

UNIVERSITE TOULOUSE III PAUL SABATIER
FACULTE DES SCIENCES PHARMACEUTIQUES

ANNEE : 2013

THESES 2013 TOU3 2111

THESE

POUR LE DIPLOME D'ETAT DE DOCTEUR EN PHARMACIE

Présentée et soutenue publiquement
par

Pierre ORLIAC

LA PHARMACIE D'OFFICINE A L'ERE DE LA DEMATERIALISATION

13 décembre 2013

Directeur de thèse : Professeur Florence TABOULET

JURY

Président : Pr Florence TABOULET
1er assesseur : Dr Blandine JUILLARD-CONDAT
2ème assesseur : Dr Dominique BOURGOIS
3ème assesseur : Dr Philippe LATRY
4ème assesseur : M Sylvain IEMFRE
5ème assesseur : Dr Bernard CHAMPANET

REMERCIEMENTS

A Madame le professeur Florence Taboulet

Professeur de Droit et Economie de la santé à l'Université Paul Sabatier Toulouse III,

J'ai eu la chance de pouvoir suivre votre enseignement tout au long de mes études, en filière officine comme en filière industrielle, ce qui me permet d'avoir une large connaissance des problématiques liées à la législation des produits de santé. Votre enseignement m'a également permis de connaître l'étendue de mes devoirs professionnels ainsi que les règles à respecter, ce qui me permet d'assumer mon rôle et de m'épanouir en tant que professionnel de santé. Je vous remercie d'avoir accepté de diriger mon travail ainsi que pour votre patience et votre disponibilité qui m'ont permis de traiter ce sujet extrêmement vaste mais passionnant. Votre enthousiasme et la confiance que vous m'avez témoignée tout au long de la rédaction de mon manuscrit ont été la source de ma motivation à accomplir ce long travail. Soyez assurée de ma plus sincère reconnaissance ainsi que de mon profond respect devant vos qualités professionnelles et humaines.

A Madame Blandine Juillard-Condat

Pharmacien, maître de conférences des universités, praticien hospitalier,

Je vous remercie très sincèrement d'avoir accepté de juger mon travail. Soyez assurée de ma profonde reconnaissance.

A Madame Dominique Bourgois

Pharmacien, responsable du pôle sécurité des patients, politique des produits de santé et biologie médicale, Direction de la santé publique de l'agence régionale de santé de Midi-Pyrénées,

Par le développement et la coordination de projets régionaux, les agences régionales de santé permettent de tisser la toile de l'e-santé en France. En veillant attentivement à la qualité des sites internet de vente en ligne de médicaments, elles préservent également la sécurité de ce nouveau mode de dispensation qui me fascine. Je vous remercie vivement d'avoir accepté de participer au jury de ma thèse.

A Monsieur Philippe Latry

Médecin chef de service système d'information de la direction du service médical d'Aquitaine (CNAMTS),

Je suis très honoré de vous compter parmi les membres de ce jury et vous remercie de l'intérêt que vous avez porté à mon travail.

A Monsieur Sylvain Iemfre

Directeur de la direction des technologies en santé du conseil national de l'ordre des pharmaciens,

Au cours de la rédaction de cette thèse, j'ai pris conscience que le développement des technologies en santé constituait une opportunité unique d'affirmer la légitimité du pharmacien en tant que professionnel de santé. Vos travaux n'y sont bien sûr pas étrangers. Je suis très honoré que vous ayez accepté de juger mon travail et vous prie de croire en ma sincère admiration.

A Monsieur Bernard Champanet

Pharmacien, président du syndicat des pharmaciens du Tarn,

Je vous remercie d'avoir accepté de participer au jury de ma thèse. Soyez assuré de ma plus sincère considération.

A Madame Marie-Line Bonnefous, pharmacien, qui m'a accueilli au sein de la pharmacie Gambetta à Cahors où est né mon souhait de devenir pharmacien dès mon stage en entreprise au collège. C'est également au sein de votre équipe que j'ai eu la chance d'accomplir mes premiers stages officinaux au cours desquels j'ai réellement concrétisé ce désir en m'initiant à la pratique officinale.

Aux pharmaciens qui m'ont accueilli à bras ouverts au cours de mes stages et mes remplacements : **Madame Odette Pradines** de la pharmacie Inter-Santé (Cahors), **Madame Karine Arfi** de la pharmacie Saint-Etienne (Toulouse), **Monsieur Pierre Laffourcade** de la pharmacie Laffourcade (Toulouse) et **Monsieur André Rouayroux** de la pharmacie Wilson (Toulouse).

A Madame Christine Libon et Madame Claire Issac de l'Institut de Recherche Pierre Fabre qui m'ont accueilli au sein du service d'immunologie de l'IRPF. Je suis admiratif de votre dévouement et de votre passion dans l'accomplissement de cette étape fondamentale de la genèse d'un médicament qu'est la recherche.

Au personnel de la faculté des sciences pharmaceutiques de Toulouse et tout particulièrement à **Monsieur le professeur Raymond Bastide**, pharmacien hospitalier et à **Monsieur le professeur Philippe Courrière**, pharmacien, sans lesquels je ne serais certainement pas arrivé jusque là.

A tous les professeurs de la faculté qui m'ont tant appris et particulièrement **Monsieur Chatelain** qui a fait naître en moi une passion pour la botanique et le jardinage, **Madame Sallerin**, **Madame Martin** et **Monsieur Sècheresse** pour l'enseignement des cours de communication.

A mes parents, mes sœurs et toute ma famille qui m'ont soutenu tout au long de mon long parcours universitaire.

A Gabrielle, qui me guide et illumine ma vie chaque jour ainsi qu'à sa famille pour son soutien.

A tous mes amis et particulièrement **Madame Sandrine Cohen**, pharmacien, **Madame Marie Lopez**, préparatrice en pharmacie, **Monsieur Thibault Faure**, préparateur en pharmacie et **Monsieur Louïc Henriët**, pharmacien, qui m'ont tant aidé lors de mes premiers pas au comptoir officinal.

A la vallée du Lot et du Célé pour ses paysages et ses brochets.

TABLE DES MATIERES

Introduction	8
Chronologie de l'e-santé en France	11
Partie A : Le traitement automatisé de données à l'officine	14
Chapitre 1 : Fondement	15
A.1.1. Le secret médical	17
A.1.1.1 Sources de droit	17
A.1.1.2 Dérogations légales au secret médical	19
A.1.2. Principes fondamentaux	19
A.1.2.1 Principe de finalité	20
A.1.2.2 Principes d'exactitude et de pertinence des données	21
A.1.2.3 Principes de confidentialité et de sécurité des données	22
A.1.3. Droits des patients au regard des données traitées	24
A.1.3.1 Droit d'information et droit d'accès	24
A.1.3.2 Droit au consentement et droit à l'oubli	26
A.1.3.3 Droits d'opposition et de rectification	27
A.1.3.4 Cas particulier des personnes mineures et sous tutelle	27
Chapitre 2 : La genèse de données électroniques	28
A.2.1. Le poste de travail informatique officinal	29
A.2.1.1 Configuration matérielle	29
A.2.1.1.a Les périphériques informatiques	31
A.2.1.1.b Les mémoires informatiques	34
A.2.1.2 Les logiciels de gestion d'officine	35
A.2.1.2.a La certification des logiciels d'aide à la dispensation	36
A.2.1.2.b Les fichiers des logiciels de gestion d'officine	36
A.2.1.2.c Principales fonctions des logiciels de gestion d'officine	38
A.2.2. Le système électronique de saisie de l'assurance maladie	42
A.2.2.1 Contexte règlementaire	42
A.2.2.2 Les cartes à puce électronique	43
A.2.2.2.a Standards de conception	44
A.2.2.2.b La carte Vitale 2 et ses données personnelles	46
A.2.2.2.c Les cartes de la famille CPS et leurs « données métier »	48
A.2.2.3 Lecture et mise à jour des cartes à puce	51
A.2.2.3.a Procédures d'agrément et d'homologation des interfaces	51
A.2.2.3.b Les lecteurs de cartes à puce	52
A.2.2.3.c Les fournitures logicielles d'interfaçage	53
A.2.2.3.d Les bornes de mise à jour des cartes Vitale	55
A.2.2.4 La numérisation des pièces justificatives	55
A.2.2.4.a Champs d'application	56
A.2.2.4.b Contraintes techniques	57
A.2.3. L'identification des personnes et de l'officine	58
A.2.3.1 L'identification de l'officine	58
A.2.3.2 L'identification des professionnels de santé	59
A.2.3.2.a Le répertoire partagé des professionnels de santé	59
A.2.3.2.b Le référentiel des acteurs santé sociaux	61
A.2.3.3 L'identification des patients	61
A.2.3.3.a Le numéro d'inscription au répertoire des personnes physiques	62
A.2.3.3.b Le numéro d'adhérent à un organisme complémentaire	63
A.2.3.3.c L'identifiant national de santé	63
A.2.3.3.d Le numéro de dossier pharmaceutique	67
A.2.4. L'identification des produits de santé	69
A.2.4.1 La codification des produits de santé	69
A.2.4.2 Le marquage du conditionnement extérieur	71
A.2.4.3 La suppression de la vignette pharmaceutique	75

Chapitre 3 : L'hébergement et la transmission de données électroniques	79
A.3.1. L'hébergement de données de santé	79
A.3.1.1 Statut juridique de l'hébergeur	80
A.3.1.2 Stockage, sauvegarde et archivage	81
A.3.1.3 Supports de données dématérialisées	83
A.3.1.3.a Le disque dur interne d'un ordinateur	83
A.3.1.3.b Les médias amovibles classiques	83
A.3.1.3.c Les serveurs de stockage de données	85
A.3.2. Les réseaux informatiques à l'officine	85
A.3.2.1 Le réseau informatique local	86
A.3.2.2 Le réseau internet	87
A.3.2.2.a Modalités d'accès et sous-traitance	88
A.3.2.2.b Les protocoles réseaux	88
A.3.2.3 Le réseau SESAM-Vitale	90
A.3.2.3.a Modalités d'accès	90
A.3.2.3.b Modalités de télétransmission	91
A.3.3. L'interopérabilité des systèmes informatisés de santé	91
A.3.3.1 Intérêts de la structuration et du codage des données de santé	92
A.3.3.2 Interopérabilités sémantique et syntaxique	93
A.3.3.3 L'interopérabilité technique	94
A.3.4. La sécurité du système informatique officinal	95
A.3.4.1 La démarche de sécurisation du système informatique officinal	95
A.3.4.2 Mise en œuvre d'une politique de sécurité	96
A.3.5. La sécurité des échanges dématérialisés	101
A.3.5.1 Confidentialité et chiffrement	102
A.3.5.1.a Méthodes de chiffrement symétrique	103
A.3.5.1.b Méthodes de chiffrement asymétrique	105
A.3.5.1.c Chiffrement hybride et clé de session	107
A.3.5.1.d Fonctions de hachage et codes d'authentification de message	107
A.3.5.2 Identification et authentification électroniques	110
A.3.5.3 La signature électronique	111
A.3.5.4 Les certificats électroniques	113
A.3.5.4.a La gestion des certificats électroniques	114
A.3.5.4.b Structure et fonctions des certificats émis par l'ASIP Santé	116
A.3.5.4.c Fonctions de sécurité offertes par la carte CPS3	120
A.3.5.4.d Capacités cryptographiques de la carte Vitale 2	122
Partie B : La dématérialisation au quotidien du pharmacien d'officine	126
Chapitre 1 : Les échanges dématérialisés avec l'assurance maladie	127
B.1.1. La modernisation du système de facturation des produits de santé	127
B.1.1.1 Contexte réglementaire	127
B.1.1.2 Contexte technique	129
B.1.2. La dématérialisation des feuilles de soins	130
B.1.2.1 La préparation des factures électroniques	132
B.1.2.2 La mise en forme des factures et des lots	134
B.1.3. La numérisation des pièces justificatives	138
B.1.3.1 Constitution d'un dossier de pièces justificatives	139
B.1.3.2 Mise en lot des dossiers de pièces justificatives	139
B.1.4. Les flux de télétransmission	141
B.1.4.1 Les flux de facturation et de pièces justificatives	141
B.1.4.1.a Constitution et sécurisation des flux	141
B.1.4.1.b L'adressage des flux	142
B.1.4.2 Autres flux de télétransmission	144
B.1.4.2.a Les flux d'administration du système SESAM-Vitale	144
B.1.4.2.b Les flux retour	144

Chapitre 2 : L'aide à la dispensation et au suivi thérapeutique des patients	145
B.2.1. La dématérialisation des registres comptables	146
B.2.1.1 L'ordonnancier électronique	146
B.2.1.2 Le registre spécial des stupéfiants	146
B.2.2. Le dossier de suivi pharmaco-thérapeutique (DSPT)	147
B.2.2.1 Principales fonctions du DSPT	148
B.2.2.1.a Gestion du dossier du patient	149
B.2.2.1.b Gestion des délivrances	150
B.2.2.2 L'opinion pharmaceutique	151
B.2.2.2.a Définition et objectifs	151
B.2.2.2.b Mise en œuvre de l'opinion pharmaceutique	152
B.2.2.2.c Communication de l'opinion pharmaceutique	153
B.2.3. Le dossier pharmaceutique	154
B.2.3.1 Présentation et objectifs	155
B.2.3.2 Les étapes clés de la vie d'un dossier pharmaceutique	156
B.2.3.2.a La création d'un dossier pharmaceutique	157
B.2.3.2.b L'alimentation du dossier pharmaceutique	157
B.2.3.2.c La consultation du dossier pharmaceutique	158
B.2.3.2.d L'édition et la clôture du dossier pharmaceutique	158
B.2.3.3 L'articulation du dossier pharmaceutique avec le DMP et le Web-Médecin	159
B.2.3.4 Le réseau du dossier pharmaceutique : vecteur d'alertes sanitaires et de retraits de lots	161
B.2.3.4.a La diffusion d'alertes sanitaires	162
B.2.3.4.b Les rappels et retraits de lots de médicaments	162
B.2.3.5 La sécurisation du dossier pharmaceutique	166
B.2.3.5.a L'identification de l'officine	166
B.2.3.5.b Constitution et sécurisation des flux de données	167
B.2.3.5.c La sécurité de l'hébergeur	167
B.2.3.5.d La traçabilité des échanges	168
B.2.4. Le partage de données entre professionnels de santé	168
B.2.4.1 La télécopie	168
B.2.4.2 Les messageries sécurisées de santé	169
B.2.5. Le e-pharmacien au cœur des orientations stratégiques de santé	171
B.2.5.1 Les nouvelles missions du pharmacien d'officine	172
B.2.5.2 La vente en ligne de médicaments par les officines en France	177
B.2.5.2.a Bonnes pratiques liées au commerce électronique de médicaments	178
B.2.5.2.b Médicaments faisant l'objet du commerce électronique	178
B.2.5.2.c Identification administrative du site de l'officine	179
B.2.5.2.d Règles techniques de conception	180
B.2.5.2.e L'e-dispensation	181
Chapitre 3 : L'e-prescription : perspective d'avenir majeure pour l'e-santé en France	183
B.3.1. L'ordonnance médicale en France	184
B.3.1.1 Statut juridique	184
B.3.1.2 Les différents types d'ordonnances	185
B.3.1.3 Rôles de l'ordonnance vis à vis de ses destinataires	187
B.3.1.3.a Outil de coopération interdisciplinaire	187
B.3.1.3.b Pièce justificative de prise en charge par l'assurance maladie	188
B.3.1.3.c Support d'information pour les patients	189
B.3.2. Etat des lieux du déploiement de l'e-prescription en Europe	190
B.3.2.1 Place de la France dans la course européenne à l'e-santé	190
B.3.2.2 Les clés du succès des politiques d'e-santé étrangères	191
B.3.2.2.a Le statut juridique de la signature électronique	192
B.3.2.2.b Le respect des droits des patients	192
B.3.2.2.c Le développement d'une infrastructure adaptée	193
B.3.2.3 Le projet epSOS : un terrain fertile à l'échelle d'un continent	196
B.3.2.4 Le projet européen Palante	198

B.3.3. Les enjeux de l'e-prescription	198
B.3.3.1 Les atouts économiques et écologiques d'une simplification administrative	199
B.3.3.2 Les bénéfices en matière de santé publique	199
B.3.3.3 Favoriser la coopération entre professionnels de santé	200
B.3.4. Comment déployer l'e-prescription en France ?	201
B.3.4.1 En anticipant les besoins d'interopérabilité	202
<i>B.3.4.1.a L'interopérabilité sémantique</i>	202
<i>B.3.4.1.b Interopérabilités syntaxique et technique</i>	203
B.3.4.2 En concevant un outil adapté aux besoins et aux infrastructures	204
B.3.4.3 En considérant les limites de la dématérialisation de l'ordonnance	208
<i>B.3.4.3.a Le support de délivrance du pharmacien</i>	208
<i>B.3.4.3.b Le plan thérapeutique du patient</i>	210
B.3.4.4 En fédérant les professionnels de santé autour d'un projet commun	212
Conclusion	213
Bibliographie	215
Annexes	222

INTRODUCTION

A l'heure où les réseaux sociaux tendent à estomper la frontière entre informations privées et publiques, assurer la confidentialité des données relatives à la santé des personnes au sein des systèmes d'information de santé demeure plus que jamais une condition incontournable de toute politique d'e-santé. Si la société numérique fascine au moins autant qu'elle inquiète, les systèmes d'information proposent de répondre aux besoins croissants de leurs usagers en matière de dématérialisation, de portabilité et d'accessibilité aux informations.

Outre l'ordinateur personnel qui demeure l'outil informatique le plus couramment employé, de nouveaux systèmes (*smartphones*, tablettes...) voient le jour et de nouveaux moyens d'accès à internet se développent. En dix ans, la proportion des ménages français disposant d'un accès à internet à leur domicile est ainsi passée de 11% à 64%, tendant à estomper la fracture numérique constatée jusqu'alors¹. Parallèlement, l'utilisation de l'internet mobile connaît un essor considérable ces dernières années puisque 40 % des internautes ont déjà surfé en 2012 sur Internet via leur téléphone portable contre seulement 10 % en 2007². Le développement des techniques d'acquisition et de transfert de données rend ainsi la dématérialisation accessible à tout un chacun. Rendre immatériel quelque chose, c'est-à-dire le dépouiller de sa matière concrète³ devient ainsi un geste quotidien ; mais comment expliquer un tel engouement pour la généralisation des échanges dématérialisés aussi bien entre personnes, qu'entre personnes et administration et/ou entreprises, ou encore entre entreprises ?

La convergence des moyens de communication permettant de véhiculer tous types de médias (voix, images, données...) via des réseaux de télécommunication toujours plus performants couplée à la relative facilité d'usage de ces systèmes, rendent les échanges dématérialisés incontournables. Le développement des systèmes d'information, c'est à dire « de moyens destinés à élaborer, traiter, stocker ou transmettre des informations faisant l'objet d'échanges par voie électronique entre autorités administratives et usagers ainsi qu'entre autorités administratives » a ainsi permis de constituer le socle de notre système d'administration en ligne (1). Déclarer ses impôts sur le revenu en ligne ou encore effectuer un paiement par carte bancaire plutôt que par chèque ou espèce sont devenus coutumiers des Français.

Par ailleurs, toute démarche de dématérialisation des échanges présente des bénéfices directs tant sur le plan économique (gain de temps et de productivité, pérennisation des infrastructures) qu'écologique en réduisant la consommation de papier et les rejets de polluants (gaz toxiques, produits chimiques...) de manière considérable. D'autres bénéfices plus spécifiques sont en revanche propres à chaque système. La dématérialisation des données et des échanges au sein des systèmes d'information de santé n'a ainsi de raison d'être que si elle facilite l'exercice des professionnels de santé au bénéfice de la santé publique en offrant une meilleure qualité des soins et du suivi de chaque patient (2).

Le développement fulgurant des nouvelles technologies de l'information et de la communication permet aujourd'hui de générer de nombreux types de données numériques, parfois en quantités astronomiques. Le secteur de la santé est d'ailleurs massivement producteur et utilisateur de ces informations.

¹ Insee, enquête « *Technologies de l'information et de la communication* », avril 2010.

² Insee, enquête « *Technologies de l'information et de la communication* », 2007 à 2012.

³ Dictionnaire Larousse : définition du verbe « dématérialiser ».

La première partie de cette thèse s'intéresse donc aux opérations de traitement automatisé des données personnelles relatives aux patients dans l'exercice officinal. Compte tenu de la sensibilité de ces données, leur traitement automatisé par les pharmaciens d'officine doit être réalisé selon des règles garantissant les droits fondamentaux des patients à cet égard. Les principales finalités du traitement automatisé de telles données à l'officine doivent ainsi permettre d'améliorer la sécurité de la dispensation et le suivi pharmaco-thérapeutique des patients tout en facilitant les échanges dématérialisés avec l'assurance maladie. Les droits des patients à l'égard du traitement de leurs données sont donc assortis de devoirs incombant notamment les professionnels de santé d'en préserver la confidentialité, en vertu du principe de secret médical.

La présentation des différents outils dont disposent les pharmaciens pour réaliser le recueil d'informations et la genèse de données électroniques permet de se rendre compte de la place grandissante des nouvelles technologies dans leur exercice quotidien. Si le module d'aide à la dispensation des logiciels de gestion d'officine, élément central du système informatique officinal, est bien connu des officinaux, d'autres permettant la dématérialisation des feuilles de soins, l'accès au dossier pharmaceutique et la numérisation des ordonnances ont enrichi le panel d'outils informatiques susceptibles d'intervenir dans la prise en charge de tout patient d'une pharmacie d'officine française.

Si la dématérialisation promet un gain de place colossal lié à l'archivage des documents, l'hébergement de données électroniques doit cependant en préserver l'intégrité et la confidentialité à tout prix. Entre les données sauvegardées localement à l'officine, celles échangées entre professionnels de santé et celles télétransmises via le dossier pharmaceutique ou les flux de facturation, cet impératif de confidentialité impose donc la mise en œuvre de moyens de sécurité locaux et d'autres, sécurisant leur transmission au sein des réseaux télématiques. Si confidentielles que soient les données de santé, elles sont donc le plus souvent amenées à être communiquées à des tiers autorisés, avec le consentement et dans l'intérêt du patient. Faire circuler ainsi ces données médicales personnelles, c'est-à-dire des informations concernant « *une personne physique identifiée ou identifiable* »⁴ n'est cependant pas dénué de risques (3). Comme nous le verrons, des moyens de sécurité utilisant des techniques cryptographiques sont mis en œuvre pour préserver ce secret médical partagé lors de la transmission électronique de données. Ces techniques sont cependant remises en question depuis quelques semaines avec les récentes révélations d'Edward Snowden sur l'existence d'un programme secret américain mis en œuvre par la *National Security Agency* visant à espionner les flux de données électroniques, y compris cryptés, circulant sur les réseaux mondiaux. La sécurité des échanges au sein des systèmes d'information de santé français étant assurée par ces mécanismes en partie élaborés par cette agence américaine, il est tout à fait légitime de s'interroger sur leur réelle confidentialité.

La deuxième partie de cette thèse décrit comment la dématérialisation s'inscrit dans l'exercice quotidien du pharmacien d'officine. Compte tenu de la généralisation de la numérisation des ordonnances à l'officine, cette partie présente tout d'abord les échanges dématérialisés des pharmaciens avec les organismes d'assurance maladie, puis l'ensemble des outils permettant l'aide à la dispensation et au suivi thérapeutique de chaque patient. Une présentation du panel d'outils numériques dont disposent les pharmaciens d'officine permet ainsi de mettre en évidence les nombreux bénéfices offerts par l'informatisation locale des dossiers des patients, le dossier pharmaceutique en ligne et les messageries sécurisées de santé.

⁴ Telles qu'elles sont définies par la directive européenne 95/46/CE sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Considérant les nouvelles missions offertes aux pharmaciens d'officine par la loi du 21 juillet 2009 portant réforme de l'hôpital et relative aux patients dite loi HPST et l'avenant numéro 1 à la convention nationale régissant les rapports entre les pharmaciens et l'assurance maladie, cette partie propose également une réflexion sur les bénéfices potentiels de la dématérialisation et du développement des nouvelles technologies dans l'accomplissement de ces nouvelles missions et notamment s'agissant du suivi thérapeutique des patients et de l'épanouissement du "e-pharmacien correspondant". Nous étudierons par ailleurs les modalités d'application de l'arrêté du 20 juin 2013 autorisant la vente de certains médicaments par le site internet d'une officine française autorisée ainsi que les règles et les bonnes pratiques liées à ce nouveau mode de dispensation.

Enfin, dans la continuité de la numérisation des ordonnances à l'officine, la dématérialisation de la prescription à la source et de sa transmission grâce à un système d'e-prescription constitue l'une des principales orientations stratégiques de notre système d'e-santé. L'étude des systèmes d'e-prescription opérationnels à l'étranger permet de situer la place de la France dans la course européenne à l'e-santé et de prendre la mesure des efforts à fournir pour améliorer notre système compte tenu de ses contraintes techniques et juridiques. Afin de nourrir les réflexions actuelles sur le déploiement d'un tel projet au cœur duquel les pharmaciens se situeraient, cette partie propose certaines suggestions pour la conception d'un outil d'e-prescription interopérable avec les systèmes existants et adapté à l'exercice quotidien des professionnels de santé, tout en considérant les limites de la dématérialisation de l'ordonnance.

Dans le sillage des leaders européens en matière d'e-santé, le développement d'un service d'e-prescription, véritable passerelle électronique entre prescripteurs et pharmaciens, en France, pourrait constituer l'opportunité tant attendue de finaliser et généraliser le dossier médical personnel (DMP), tout en valorisant le succès du dossier pharmaceutique et le travail accompli sur les messageries sécurisées de santé (MSSanté), parachevant ainsi notre système d'e-santé.

Si l'essor des nouvelles technologies de l'information et de la communication (NTIC ou TIC) a révolutionné les pratiques professionnelles de nombreux secteurs d'activité, celui de la santé a su tirer profit de ces innovations au bénéfice de la santé publique. Elles regroupent les techniques utilisées dans le traitement et la transmission des informations, principalement dans le domaine de l'informatique, d'internet et des télécommunications. Entre la première communication d'un électrocardiogramme par téléphone en 1905 et la première opération de télé-chirurgie entre Strasbourg et New-York en 2001, s'est écoulé près d'un siècle au cours duquel de nouveaux moyens de saisir et communiquer l'information sont nés, tendant à abolir le temps et les distances.

On entend par **e-santé** « *l'application des TIC à l'ensemble des activités en rapport avec la santé* » (Commission européenne (4)) et/ou « *la fourniture de soins à distance* » (Organisation mondiale de la santé (5)). Cette large définition de l'e-santé lui attribue ainsi de nombreux domaines d'application tels que le suivi d'une maladie chronique, les dossiers médicaux informatisés, l'information et la prévention sur la santé, l'aide au handicap ou la télémédecine...

Le développement de logiciels métiers spécifiques à chaque catégorie de professionnel de santé a tout d'abord permis l'archivage de données relatives aux patients (informations administratives, civiles, cliniques, diagnostics, examens complémentaires...), l'aide à l'élaboration et à la dispensation de prescriptions, puis la dématérialisation et la télétransmission des feuilles de soins au format électronique (FSE). Les professionnels de santé disposent aujourd'hui de logiciels très performants reposant notamment sur l'utilisation de bases de données médicamenteuses dont la qualité est certifiée par la Haute Autorité de santé, sécurisant les actes de prescription et de dispensation.

En 1993, la création conjointe du groupement d'intérêt économique autour du système électronique de saisie de l'assurance maladie chargé de porter le projet SESAM-Vitale (GIE SESAM-Vitale) et du groupement d'intérêt public « carte de professionnel de santé » (GIP-CPS) chargé de promouvoir la sécurité des échanges électroniques du secteur de santé, va permettre l'aboutissement des expérimentations menées dès 1983 sur la carte de santé à mémoire électronique voulue par Monsieur Pierre Bérégovoy, alors ministre des affaires sociales et de la solidarité. Le GIE SESAM-Vitale propose alors d'élaborer un nouveau support de carte d'assurance maladie sous forme d'une carte à puce électronique en répondant aux exigences d'identification et de sécurité posées par le traitement des données de santé : l'ébauche de la carte Vitale est née. Cinq cent cinquante mille cartes sont ainsi diffusées pour expérimentation sur quatre sites expérimentaux en 1993 pour finalement équiper 40 millions de bénéficiaires de l'assurance maladie un an plus tard. Afin d'être utilisée simultanément avec la carte Vitale pour générer des feuilles de soins électroniques, la première version de la carte CPS dédiée aux professionnels de santé voit le jour.

« L'ordonnance Juppé » du 24 avril 1996 rendant obligatoire la télétransmission des FSE par les professionnels de santé d'ici la fin de l'année 1998, la France s'engage alors sur un long chemin vers la modernisation de son système de santé. Utilisées conjointement, la carte Vitale et la carte CPS constituent ainsi les véritables clés d'entrée des systèmes d'information en santé.

Même si dans un premier temps la qualité du réseau internet français ne permettait pas une transmission de données très « volumineuses », l'échange confraternel d'informations permet

le rapprochement des différents partenaires impliqués dans la prise en charge globale du patient. En 2004, la société ATOS WORLDLINE remplace CEGETEL-RSS en tant qu'opérateur réseau pour la transmission des feuilles de soins électroniques via le réseau SESAM-Vitale. La même année, l'article 34 de la loi n° 2004-810 introduit la possibilité de prescrire des soins ou des médicaments par courriel sous certaines conditions, ouvrant ainsi la porte à la transmission de prescriptions par voie électronique.

Afin de nourrir cet élan vers la constitution d'un véritable « toile » de données de santé dématérialisées, le ministère de la santé en collaboration avec l'assurance maladie et la caisse des dépôts et consignations constituent en avril 2005 le groupement d'intérêt public dédié au dossier médical personnel (GIP-DMP) afin de mettre en œuvre le projet du DMP créé par la loi du 13 août 2004. L'objectif du GIP-DMP est de finaliser ce projet d'ici la fin de l'année 2007, afin de permettre le partage entre professionnels de santé désignés, des données médicales des patients qui le souhaitent. Les filiales SANTEOS (Atos Origin) et Extelia (La Poste) se voient attribuer le rôle d'hébergeur du DMP le 10 mars 2010 et les premiers dossiers seront finalement créés à partir de janvier 2011.

Par ailleurs, le décret du 9 février 2006 organise la création d'une base de données de l'ensemble des actes médicaux et paramédicaux pris en charge par l'assurance maladie ainsi que le relevé des prescriptions médicales et des arrêts de travail des douze derniers mois. Ce nouvel outil baptisé « web-médecin » est accessible par les médecins avec le consentement des patients sur le site AMELI.fr. Cependant, pour le Conseil national de l'ordre des médecins, l'articulation de ces systèmes pose problème puisque l'accès au web-médecin peut être librement refusé par le patient tandis que le refus de donner accès au DMP sera susceptible d'entraîner une modulation des taux de prise en charge des actes par l'assurance maladie.

Le projet de dossier pharmaceutique lancé en 2006 par l'ordre des pharmaciens se concrétise le 2 décembre 2008 lorsque la Commission nationale de l'informatique et des libertés (CNIL) donne un avis favorable à sa généralisation dans toutes les officines du territoire suite à une expérimentation d'un an et demi dans plusieurs départements. Il est créé par le pharmacien après recueil du consentement du patient, et n'est consultable qu'en présence de ce dernier. La sécurisation de la transmission des données et l'hébergement du dossier pharmaceutique ont été confiés à un hébergeur unique indépendant : le groupement d'intérêt économique SANTEOS (GIE-SANTEOS). Voué à fusionner avec le DMP, le dossier pharmaceutique permettra d'enrichir celui-ci de l'historique des produits de santé, prescrits ou non, facturés et remis au patient à l'issue d'un processus de dispensation.

Le décret n°2007-960 du 15 mai 2007 relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique prévoit par ailleurs une obligation pour les professionnels de santé souhaitant accéder à des informations médicales à caractère personnel sur support informatique ou de leur transmission par voie électronique, d'utiliser leur carte CPS d'ici trois ans. Le ministère de la santé et des sports autorise par l'arrêté du 6 février 2009 la création par le GIP-CPS d'un répertoire partagé des professionnels de santé (RPPS), véritable annuaire des professionnels de santé. Le GIP-DMP et le GIP-CPS disparaissent en novembre 2009 pour laisser place au groupement d'intérêt public de l'Agence des systèmes d'information partagés de santé GIP-ASIP Santé le 15 septembre 2009. L'Agence nationale des systèmes d'information partagés de santé (ASIP Santé) est notamment en charge de concrétiser le projet DMP, de la gestion des cartes CPS et plus généralement, de promouvoir le développement de l'e-santé en France.

Début 2010, l'expérimentation de la numérisation des ordonnances par les pharmaciens en vue de les transmettre à l'assurance maladie sous forme de CD-ROM débute dans sept départements et près d'une centaine d'officines. Les résultats encourageants et la bonne adhésion des pharmaciens, poussent l'assurance maladie soutenue par les syndicats de pharmaciens à étendre cette expérimentation à l'ensemble du territoire. L'avenant conventionnel n°3 du 14 novembre 2011 de la convention pharmaceutique généralise la dématérialisation des ordonnances à l'ensemble des pharmacies françaises et l'expérimentation de la télétransmission est lancée.

Le déploiement progressif du dossier pharmaceutique et du DMP se déroule parallèlement au développement des logiciels métiers des professionnels concernés afin d'en optimiser l'interopérabilité et l'utilisation en pratique. Afin de recentrer le DMP sur le patient et assouvir son besoin d'information, l'ASIP Santé lui propose un accès autonome via un service web en ligne auprès duquel il s'authentifie à l'aide d'un identifiant assorti d'un mot de passe, remis par le médecin au moment de la création du dossier. Compte tenu de l'incertitude qui pèse actuellement sur la confidentialité des données personnelles circulant sur internet, proposer aux patients de s'impliquer dans ces systèmes afin qu'ils n'en soient plus spectateurs semble incontournable pour gagner leur confiance.

A partir de juin 2011, l'ASIP Santé équipe les professionnels de santé d'une nouvelle version de la carte CPS (version 3) enrichie de nouvelles fonctionnalités. Un an plus tard, près de 70% des médecins libéraux et hospitaliers, 99 % des pharmaciens, 85% des dentistes et 80 % des sages-femmes sont équipés, soit environ 850 000 cartes CPS3 distribuées pour le moment. Comme nous le verrons, la carte CPS constitue un élément fondamental de la sécurisation des échanges dématérialisés permettant notamment de préserver la confidentialité et l'intégrité des données échangées. Le site internet de l'assurance maladie, AMELI.fr, évolue également et s'enrichit de nouvelles fonctions en permettant la dématérialisation des premiers arrêts de travail et de la procédure de choix du médecin traitant. Les conventions régissant les rapports entre l'assurance, les pharmaciens d'une part et les médecins d'autre part, prévoient enfin de dématérialiser progressivement les prescriptions à la source en développant un système d'e-prescription, conformément aux recommandations de l'inspection générale des affaires sociales.

L'évolution des performances des outils informatiques et des réseaux offrent ainsi de nombreuses perspectives pour la dématérialisation des échanges au sein des systèmes d'information de santé. En marge des réflexions menées sur l'e-prescription, les nouvelles missions du « pharmacien correspondant » prévues par la loi HPST pourraient permettre de définir de nouvelles orientations stratégiques pour la dématérialisation des échanges entre professionnels de santé ainsi qu'entre professionnels de santé et patients.

Partie A : LE TRAITEMENT AUTOMATISE DE DONNEES A L'OFFICINE

La généralisation de l'équipement informatique des professionnels de santé leur permet de bénéficier de fonctions étendues de gestion automatisée de données nécessaires à leur activité. Qu'il s'agisse d'informations confidentielles relatives à un patient ou d'un simple registre comptable, l'outil informatique leur permet d'automatiser de nombreuses tâches encore réalisées « manuellement » il y'a quelques décennies telles que la gestion des dossiers des patients, des stocks et des ventes de produits ou la facturation des actes et des produits de santé.

L'informatique ne dispense pas pour autant les professionnels de santé d'assumer leurs devoirs déontologiques et en particulier de respect du secret médical. Cet outil doit donc être un atout dans la prise en charge du patient en se conformant à certains principes fondamentaux garants de son emploi à bon escient. En effet, les données de santé, parce qu'elles relèvent de l'intimité de la vie privée des personnes, sont des données sensibles devant faire l'objet d'une protection particulière. A ce titre, elles bénéficient d'un statut particulier imposant le respect de règles de sécurité garantes de leur confidentialité. En sa qualité d'autorité de protection des données, la CNIL, en étroite collaboration avec les acteurs des systèmes informatisés de santé, contribue ainsi aux nombreux chantiers dans le domaine de l'e-santé. Le recueil, l'hébergement, la transmission de ces données sont autant d'étapes critiques de leur traitement qu'il est ainsi nécessaire de réaliser conformément aux règles définies, pour les finalités prévues et dans le respect des droits des patients.

La dématérialisation des documents à l'officine s'inscrit dans la démarche de modernisation et d'efficacité du système de santé français portée par le ministère de la santé en collaboration avec l'assurance maladie et les ordres de professionnels de santé. Si l'objectif est d'assurer un allègement administratif ainsi qu'un gain de temps consacré à chaque patient, l'informatique permet également de rapprocher les professionnels de santé afin de garantir l'efficacité et la cohérence de son parcours de santé.

Le large panel d'outils informatiques à la disposition des professionnels de santé permet de dématérialiser chaque jour un peu plus. Qu'il s'agisse de la gestion de l'activité économique de l'officine, des relations avec l'assurance maladie ou de la dispensation des produits de santé, l'informatique permet d'assister le pharmacien dans son exercice quotidien.

Si la dématérialisation des documents à l'officine promet de nombreux bénéfices, une attention toute particulière doit être portée à la sécurité et à l'intégrité des données électroniques enregistrées et échangées par les différents systèmes afin d'en préserver la qualité et la confidentialité.

Chapitre 1 : FONDEMENT

L'utilisation néfaste de données personnelles aux heures les plus sombres de l'histoire française a permis de prendre conscience de la nécessité d'instaurer un cadre juridique précis autour de leur recueil et de leurs finalités. C'est avec une volonté d'organiser la gestion de ces données que l'Etat français élaborait différents modèles d'organisation visant à centraliser différents répertoires utiles aux administrations. Le projet SAFARI porté par l'INSEE à partir de 1971 visait à centraliser l'ensemble des données personnelles (professionnelles, militaires, médicales, fiscales...) sous forme d'un seul fichier identifié par l'usage du NIRNIPP (numéro d'inscription au répertoire national d'identification des personnes physiques) ou NIR. Cette perspective d'une administration toute-puissante, perçue comme une entrave aux libertés individuelles fit scandale suite à la parution de l'article du journal « *Le Monde* » du 21 mars 1974 intitulé « *Safari ou la chasse aux Français* ». Le Gouvernement du Président Valéry Giscard d'Estaing tout juste élu, prend alors conscience de l'urgence de clarifier le périmètre et les modalités de traitement des données recueillies auprès des Français et reprend le projet de création d'une autorité administrative indépendante et transparente régissant les modalités du traitement des données personnelles.

Ce projet aboutit à la **loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés** et à la création de la Commission nationale de l'informatique et des libertés (CNIL) chargée de veiller à ce que l'informatique soit « *au service de chaque citoyen* » et « *ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques*⁵ ».

Afin de mieux appréhender le processus de traitement des données personnelles et ses finalités, il est important de définir et préciser la portée de ces données.

Les **données personnelles** sont définies par l'article 2 de la loi informatique et libertés comme « *toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.* » Cet article précise également qu'un **fichier de données à caractère personnel** correspond à « *tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés.* »

Le **traitement des données à caractère personnel** consiste en « *toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.* » Lorsque le responsable du traitement a recours à un système informatisé (un ordinateur par exemple), on parle de **traitement automatisé des données à caractère personnel**.

Les **données à caractère personnel relatives à la santé des personnes**, les opinions politiques, religieuses, les origines raciales, ethniques ou encore les données bancaires sont considérées comme des **données sensibles**⁶ dont le traitement est en principe interdit⁷.

⁵ Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, article 1.

⁶ Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

⁷ Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, article 8.

Cependant, pour des raisons pratiques, la loi informatique et libertés prévoit certaines dérogations limitatives autorisant leur traitement sous certaines conditions.

Par son avis sur les données de santé dématérialisées du 19 octobre 2012, la conférence nationale de santé présente les données de santé comme l'ensemble des informations sur l'état de santé et les maladies d'un individu ou d'une population donnée mais aussi sur des éléments qui peuvent déterminer l'état de santé et les maladies (facteurs de risques médicaux, biologiques ou génétiques, comportements de santé, consommation des soins, positions sociales, conditions de travail, conditions de vie, environnement physique de l'habitat...) (6).

Le code de la santé publique prévoit cependant qu'elles se limitent aux « *données recueillies ou produites à l'occasion des activités de prévention, de diagnostic ou de soins*⁸ » mais encore, aux « *informations formalisées (...) ou ayant fait l'objet d'échanges écrits entre professionnels de santé, notamment des résultats d'examen, comptes rendus de consultation, d'intervention, d'exploration ou d'hospitalisation, des protocoles et prescriptions thérapeutiques mis en œuvre, feuilles de surveillance, correspondances entre professionnels de santé, à l'exception des informations mentionnant qu'elles ont été recueillies auprès de tiers n'intervenant pas dans la prise en charge thérapeutique* »⁹.

Comme tout responsable du traitement de données personnelles, les professionnels de santé sont tenus de déclarer leurs fichiers de données à la CNIL¹⁰. Cependant, l'article 24 de la loi informatique et libertés permet à certaines professions comme celles de la santé (médicales et paramédicales) de bénéficier d'une formalité allégée consistant en une déclaration de conformité de leur traitement à une norme simplifiée élaborée par la CNIL et disponible sur son site internet. Pour les pharmaciens, il s'agit de la déclaration simplifiée n° 52¹¹ (ou norme simplifiée relative aux traitements automatisés de données à caractère personnel mise en œuvre par les pharmaciens à des fins de gestion de la pharmacie) adoptée le 8 juin 2006, réalisable en ligne sur le site de la CNIL. C'est autour de ces normes simplifiées que s'articulent les devoirs des professionnels de santé ainsi que les droits des patients autour du traitement de leurs données de santé.

La norme simplifiée n° 52 reposant sur les grands principes du traitement automatisé de données à caractère personnel prévus par la loi informatique et libertés, définit le périmètre des informations susceptibles d'être recueillies à l'officine, leurs destinataires ainsi que les modalités de leur traitement, d'accès et de sécurité.

La CNIL travaille ainsi en collaboration avec de nombreux organismes et institutions¹² chargés d'assurer les modalités de traitement et de protection de ces données hautement sensibles.

⁸ Article L.1111-8 du code de la santé publique.

⁹ Article L.1111-7 du code de la santé publique.

¹⁰ L'article 226-16 du code pénal prévoit que le non-accomplissement de cette formalité auprès de la CNIL soit sanctionné de cinq ans d'emprisonnement et 300 000 euros d'amende.

¹¹ Cette norme simplifiée ne concerne en revanche pas le traitement automatisé des données du dossier pharmaceutique faisant l'objet d'une procédure particulière.

¹² On distingue notamment le Comité consultatif sur le traitement de l'information en matière de recherche dans le domaine de la santé, l'Agence des systèmes d'information partagés de santé, l'Institut des données de santé, les comités de protection des personnes, le Conseil national de l'information statistique, et la Commission d'accès aux documents administratifs.

A.1.1. LE SECRET MEDICAL

Une particularité des professions de santé, par rapport à d'autres professions soumises à une obligation de secret est qu'elle produit des informations spécifiques, portant sur ce que le professionnel a compris de l'état de santé d'un patient (7). Au-delà d'une obligation légale, le respect de la confidentialité de ces informations constitue l'un des piliers porteurs de la relation de confiance établie entre tout professionnel de santé et ses patients.

En France et en Europe, les informations médicales personnelles sont considérées comme des données sensibles, protégées par un corpus juridique qui évolue à mesure que grandissent la société numérique, l'exigence de transparence qui traverse le domaine de la santé, et la notion de « secret médical partagé ». Reconnues comme faisant partie intégrante de la personnalité de l'individu par le groupe européen d'éthique, les données de santé appartiennent à la vie privée, domaine protégé par l'article 9 alinéa 1 du code civil ainsi que par l'article 8 de la convention de sauvegarde des droits de l'Homme et des libertés fondamentales (8).

La garantie de la confidentialité des données de santé doit donc se traduire par le respect de règles définies pour encadrer leur traitement. Le développement des systèmes d'information couplé à l'essor de nouvelles technologies tendent ainsi à favoriser la sécurité des données mais multiplient la complexité des moyens à mettre en œuvre pour assurer cette confidentialité.

A.1.1.1 SOURCES DE DROIT

Si la question de la confidentialité des informations médicales connues par les professionnels de santé ne date pas d'hier, ce n'est qu'en 1810 que le code pénal introduit une réglementation autour du secret professionnel en positionnant les professionnels de santé en première ligne.

C'est maintenant l'article 226-13 du nouveau code pénal qui prévoit que « *la révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15000 euros d'amende* ». Lorsque la révélation du secret médical entraîne un préjudice pour la victime, le professionnel de santé fautif peut également être condamné à verser des indemnités de dommages et intérêts.

C'est autour de l'article L.1110-4 du code de la santé publique qui pose le principe et définit la substance du secret médical, que s'articulent les dispositions prévues par les codes de déontologie professionnels. Il prévoit que « *toute personne prise en charge par un professionnel(...) de santé (...) ait droit au respect de sa vie privée et du secret des informations la concernant* » et précise que ce secret « *s'impose à tout professionnel de santé, ainsi qu'à tous les professionnels intervenant dans le système de santé* ».

Cet article précise également que le secret médical est amené, sauf opposition du patient, à être partagé entre professionnels de santé afin de lui assurer la continuité de ses soins et lui garantir une prise en charge adaptée à ses besoins. Ainsi, « *deux ou plusieurs professionnels de santé peuvent (...), sauf opposition de la personne dûment avertie, échanger des informations relatives à une même personne prise en charge* » mais le patient « *peut refuser à tout moment que soient communiquées des informations la concernant à un ou plusieurs professionnels de santé.* »

Ce devoir de respect du secret professionnel est ainsi rappelé aux médecins, pharmaciens¹³, chirurgiens-dentistes, sages-femmes ainsi qu'aux auxiliaires médicaux, aides-soignants, auxiliaires de puériculture et ambulanciers, dans les codes de déontologie des nombreuses professions actrices du système de santé. Ils ont ainsi le devoir de mettre tous les moyens en œuvre pour garantir la confidentialité de tout ce qui leur est « *venu à la connaissance* » dans l'exercice de leur profession, « *c'est-à-dire non seulement ce qui lui a été confié, mais aussi ce qu'il a vu, entendu ou compris.* » ainsi qu'aux « *personnes qui l'assistent dans son travail* » (secrétaires, étudiants...).

La violation de l'obligation déontologique de respect du secret peut ainsi faire l'objet de sanctions disciplinaires par l'autorité représentative de la profession concernée (comme l'ordre des pharmaciens). Il peut s'agir d'un avertissement, d'un blâme, d'une interdiction temporaire d'exercer avec ou sans sursis (pour une durée maximale de 3 ans), voire d'une radiation de l'ordre.

Puisqu'il est amené à être partagé entre professionnels de santé, les dépositaires du secret médical peuvent donc s'avérer nombreux selon la complexité du parcours de santé d'un patient. Le cercle de personnes susceptibles de partager le secret médical en pharmacie est précisé par la procédure de déclaration de traitement de données de santé à caractère personnel auprès de la CNIL (norme simplifiée n°52), il s'agit (9) :

- du personnel de l'officine ;
- des professionnels de santé et membres de l'équipe de soins (dans les établissements de santé), avec l'accord de la personne concernée ;
- des agents des organismes d'assurance maladie habilités à prendre connaissance de l'identité de l'assuré, de son numéro de sécurité sociale ainsi que les codes des médicaments, produits de santé ou dispositifs médicaux délivrés ;
- du personnel habilité des organismes d'assurance maladie complémentaire destinataire de l'identité de leurs assurés, de leur numéro de sécurité sociale et, sous la forme d'une codification tarifaire globale, des médicaments délivrés ;
- des organismes de recherche dans le domaine de la santé et les organismes spécialisés dans l'évaluation des pratiques de soins.

Si le développement des systèmes informatisés de santé conduit les professionnels de santé à partager des données personnelles relatives à leurs patients entre eux, rien ne les autorise à livrer des renseignements hors des dérogations légales. Même entre eux, la discrétion est la règle puisque les limites de cette notion de «secret partagé» sont conditionnées par l'intérêt du partage de ces informations dans la prise en charge d'un patient.

L'émergence des échanges dématérialisés suggère donc des points d'attention et de vigilance nouveaux afin de mettre en œuvre des moyens de sécurité adaptés à la nature de ces données.

¹³ Articles R.4235-5 et R.4235-43 du code de la santé publique.

A.1.1.2 DEROGATIONS LEGALES AU SECRET MEDICAL

Condition incontournable de tout processus de traitement automatisé de données de santé, le principe intangible du respect du secret médical peut néanmoins faire l'objet de dérogations légales dans certaines circonstances particulières. En effet, l'article 226-14 du code pénal porte directement dérogation au précédent en prévoyant que « *l'article 226-13 n'est pas applicable dans les cas où la loi impose ou autorise la révélation du secret. En outre, il n'est pas applicable :*

1° A celui qui informe les autorités judiciaires, médicales ou administratives de privations ou de sévices, y compris lorsqu'il s'agit d'atteintes ou mutilations sexuelles, dont il a eu connaissance et qui ont été infligées à un mineur ou à une personne qui n'est pas en mesure de se protéger en raison de son âge ou de son incapacité physique ou psychique ;

2° Au médecin qui, avec l'accord de la victime, porte à la connaissance du procureur de la République les sévices ou privations qu'il a constatés, sur le plan physique ou psychique, dans l'exercice de sa profession et qui lui permettent de présumer que des violences physiques, sexuelles ou psychiques de toute nature ont été commises. Lorsque la victime est un mineur ou une personne qui n'est pas en mesure de se protéger en raison de son âge ou de son incapacité physique ou psychique, son accord n'est pas nécessaire ;

3° Aux professionnels de la santé qui informent (...) du caractère dangereux pour elles-mêmes ou pour autrui des personnes qui les consultent et dont ils savent qu'elles détiennent une arme ou qu'elles ont manifesté leur intention d'en acquérir une. Le signalement aux autorités compétentes effectué dans les conditions prévues au présent article ne peut faire l'objet d'aucune sanction disciplinaire. »

Il est important de noter que le premier alinéa de cet article constitue une autorisation et non une obligation de violation du secret professionnel. Cependant, si la personne ayant connaissance de ce secret décide de ne pas le divulguer, il s'engage selon l'article 223-6 du code pénal à mettre tous les moyens en œuvre pour « *empêcher (...) sans risque pour lui ou pour les tiers, soit un crime, soit un délit contre l'intégrité corporelle de la personne* » sous peine d'être puni de cinq ans d'emprisonnement et de 75000 euros d'amende. Il en est de même pour « *quiconque s'abstient volontairement de porter à une personne en péril l'assistance que, sans risque pour lui ou pour les tiers, il pouvait lui prêter soit par son action personnelle, soit en provoquant un secours* ».

Enfin, comme nous le verrons, l'article L.1110-4 du code de la santé publique prévoit que ce secret puisse être révélé sous certaines conditions aux ayants-droits d'une personne décédée.

A.1.2. PRINCIPES FONDAMENTAUX

Afin de protéger la vie privée des personnes dont les données à caractère personnel font l'objet d'un traitement, il est nécessaire d'assurer la sécurité et la confidentialité de leurs données. La confidentialité est définie comme « *la protection des communications ou des données stockées contre l'interception et la lecture par des personnes non autorisées* »¹⁴, il s'agit du principe fondamental sur lequel repose la confiance dans l'utilisation des systèmes d'information (10).

¹⁴ Règlement (CE) N°460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information, article 4.

Le pharmacien est responsable des traitements des données à caractère personnel mis en œuvre au sein de l'officine et doit à ce titre, se conformer aux exigences de la loi informatique et libertés. Les grands principes liés au traitement des données par les pharmaciens d'officine énoncés dans la norme de déclaration simplifiée n°52 permettent ainsi de définir les modalités de leur recueil, des moyens mis en œuvre pour en assurer la confidentialité ainsi que les finalités de leur traitement.

A.1.2.1 PRINCIPE DE FINALITE

La collecte des données personnelles doit se dérouler de manière loyale et licite, pour un usage déterminé et légitime¹⁵, « *directement auprès de la personne concernée et ne peuvent être traitées que pour les fins en vue desquelles elles ont été recueillies* »¹⁶. Le traitement des données de santé à caractère personnel au sein d'une pharmacie d'officine doit en faciliter la gestion administrative ainsi que la dispensation des produits de santé et l'analyse statistique des ventes grâce à :

- la tenue de l'ordonnancier et des registres pour les produits dont la délivrance est soumise à un enregistrement obligatoire ;
- la gestion du dossier de suivi pharmaco-thérapeutique (DSPT) du patient ;
- l'élaboration et la transmission de courriers à d'autres professionnels de santé et notamment l'opinion pharmaceutique ;
- l'élaboration et la télétransmission des factures électroniques et subrogatoires ;
- l'édition d'un bordereau récapitulatif des caisses ;
- la gestion des règlements ;
- la réalisation d'études statistiques à partir d'informations anonymisées et la participation à des études épidémiologiques (9).

Le code de la santé publique interdit par ailleurs la constitution et l'utilisation à des fins de prospection ou de promotion commerciale, de fichiers composés à partir de données issues directement ou indirectement des prescriptions médicales ou des données personnelles de santé (même rendues anonymes à l'égard des patients), dès lors que ces fichiers permettent d'identifier directement ou indirectement le professionnel prescripteur. Par exemple, la mise en place d'un fichier de patients par un professionnel de santé exerçant à titre libéral doit lui permettre de gérer ses dossiers médicaux, d'éditer des feuilles de soins, de gérer les rendez-vous. Ce fichier ne peut pas être utilisé à des fins de prospection commerciale ou de communication politique sous peine de sanctions (de deux à cinq ans d'emprisonnement et de 75 000 à 300 000 euros d'amende)¹⁷.

¹⁵ Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, article 6.

¹⁶ Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, article 33.

¹⁷ Articles L.4113-7 et L.4163-9 du code de la santé publique et article 226-21 du code pénal.

A.1.2.2 PRINCIPES D'EXACTITUDE ET DE PERTINENCE DES DONNEES

Tout pharmacien doit vérifier l'**exactitude des informations** qu'il recueille (celles-ci doivent être « *exactes, complètes et, si nécessaire, mises à jour* » et rectifiées ou effacées en cas d'inexactitude) ainsi que leur **pertinence** au regard des finalités pour lesquelles elles sont collectées (elles sont « *adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs* »¹⁸). Par exemple, l'enregistrement de la nationalité d'un patient dans le fichier du cabinet médical ou encore dans le fichier clients d'une pharmacie n'est pas pertinent. L'enregistrement des informations relatives aux habitudes de vie d'un patient peut en revanche être admis dans la mesure où ces informations sont nécessaires au diagnostic et aux soins.

La norme simplifiée n°52 de la CNIL prévoit ainsi une liste d'informations utiles à l'exercice de la pharmacie d'officine (hors dossier pharmaceutique) susceptibles d'être recueillies auprès des patients dont :

- **L'identité du patient** : nom, prénom, sexe, adresse, numéro de téléphone ;
- **Son numéro de sécurité sociale et les modalités de prise en charge** : régime d'assurance maladie, validité des droits... pour l'édition et la télétransmission des feuilles de soins électroniques aux organismes du régime obligatoire d'assurance maladie dont dépend le patient ;
- **Son adhésion éventuelle à un organisme d'assurance maladie complémentaire** : numéro d'adhérent et taux de prise en charge pour la prise en charge complémentaire éventuelle de produits de santé ;
- **Ses Données de santé** :
 - Médicaments, produits de santé ou dispositifs médicaux dispensés, posologie, date de l'ordonnance et durée de la prescription ;
 - Modalités particulières de prise en charge médicale : hospitalisation à domicile, prise en charge dans un réseau de santé ;
 - Renseignements d'ordre biologique, physiologique et pathologique propres à influencer la réaction du patient aux médicaments ;
 - Historique des médicaments dispensés, traitements en cours, médecins traitants ;
 - Informations relatives à la profession dans la stricte limite où elles sont nécessaires à la dispensation.
- **Des informations relatives aux habitudes de vie du patient**, le nom et, le cas échéant, les coordonnées des proches mandatés pour le retrait des produits délivrés et leur lien avec le patient peuvent être collectées avec son accord et dans la stricte limite où elles sont nécessaires à la dispensation.

¹⁸ Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, article 6.

Enfin, les informations relatives au médecin prescripteur (nom, adresse, numéro d'identification, spécialité, situation conventionnelle) consulté par le patient peuvent également être collectées.

A.1.2.3 PRINCIPES DE CONFIDENTIALITE ET DE SECURITE DES DONNEES

L'écrit sur support électronique confère les mêmes droits que l'écrit sur support papier puisqu'ils ont la « *même force probante* »¹⁹ et qu'ils sont tous deux admis comme « *preuve (...), sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité.* »²⁰

L'écrit électronique oblige donc les responsables du traitement des données à « *adopter des mesures de sécurité physiques (sécurité des locaux), logiques (sécurité des systèmes d'information) et adaptées à la nature des données et aux risques présentés par le traitement. Le non-respect de l'obligation de sécurité est sanctionné de 5 ans d'emprisonnement et de 300 000 € d'amende* »²¹. Cette obligation de moyen en matière de sécurité des données est d'ailleurs réitérée par la loi informatique et libertés afin « *d'empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès* »²². Lorsque le responsable d'un traitement de données confie cette opération à un organisme sous-traitant en vertu de l'article 35 de la loi informatique et libertés, un contrat liant les deux parties rappelle les obligations incombant à ce dernier en matière de protection de la sécurité et de la confidentialité des données.

Afin d'en garantir la sécurité dans le domaine de la santé, le principe d'une réglementation autour de la conservation sur support informatique ainsi qu'à la transmission électronique de données de santé fut adopté par décret en Conseil d'Etat après avis public et motivé de la CNIL²³. Cette réglementation issue du décret n° 2007-960 du 15 mai 2007 relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique dit « décret de confidentialité » est transposée dans le code de la santé publique par 3 articles :

• **L'article R.1110-1** prévoit que tout acteur du système de santé souhaitant conserver ou transmettre électroniquement des données de santé est soumis au respect de référentiels décrivant :

- les mesures de sécurisation physique des matériels et des locaux ainsi que les dispositions prises pour la sauvegarde des fichiers ;
- les modalités d'accès aux traitements, dont les mesures d'identification et de vérification de la qualité des utilisateurs, et de recours à des dispositifs d'accès sécurisés ;
- les dispositifs de contrôle des identifications et habilitations et les procédures de traçabilité des accès aux informations médicales, ainsi que l'histoire des connexions ;

¹⁹ Article 1316-3 du code civil.

²⁰ Article 1316-1 du code civil.

²¹ Article 226-17 du code pénal.

²² Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, article 34.

²³ Article L.1110-4 du code de la santé publique.

- les mesures mises en œuvre pour garantir la confidentialité des informations échangées par voie électronique, le cas échéant, par le recours à un chiffrement en tout ou partie de ces informations.

• **L'article R.1110-2** impose au responsable du traitement, de veiller au respect du référentiel et doit notamment contrôler l'identification et la légitimité des professionnels pour l'accès aux données traitées. Il établit pour cela une liste nominative mise à disposition des patients, préalablement informés des dispositions prises pour garantir la conformité au référentiel.

• **L'article R.1110-3** prévoit enfin que tout professionnel de santé souhaitant accéder à des informations médicales personnelles ou les partager par voie électronique doit obligatoirement utiliser sa carte CPS, les certificats électroniques inclus dans la carte remise à tout professionnel de santé assurant des fonctions de chiffrement des données, d'authentification et de signature électronique.

Par ailleurs, l'ordonnance n° 2005-1516 du 8 décembre 2005 s'inscrit dans la trajectoire du Gouvernement en matière de simplification des démarches des usagers et de facilitation de l'accès de ces derniers aux services publics. Elle prévoit ainsi, l'établissement d'un référentiel général de sécurité (RGS (1)) afin de fixer les règles que doivent respecter certaines fonctions contribuant à la sécurité des systèmes d'information.

Ce référentiel élaboré conjointement par l'Agence nationale de sécurité des systèmes d'information et la direction générale de la modernisation de l'Etat « *fixe les règles auxquelles les systèmes d'information mis en place par les autorités administratives doivent se conformer pour assurer la sécurité des informations échangées, et notamment leur confidentialité et leur intégrité, ainsi que la disponibilité et l'intégrité de ces systèmes et l'identification de leurs utilisateurs...* »²⁴. Comme nous le verrons, les fonctions de sécurité d'authentification, de chiffrement et de signature électroniques au moyen de certificats électroniques sont ainsi mises en œuvre afin d'assurer la confidentialité des données au sein des systèmes d'information de santé, conformément à ce référentiel.

Un enjeu tel que la sécurisation des systèmes d'information de santé pourrait conduire à la mise en œuvre de règles de sécurité si draconiennes qu'elles ne pourraient réellement être appliquées. Il s'agit donc de trouver le meilleur compromis entre l'effort sécuritaire et l'impact sur la pratique professionnelle de la mise en œuvre de tels moyens de sécurisation. C'est pourquoi le référentiel général de sécurité propose trois niveaux de sécurité aux exigences croissantes pour chaque fonction de sécurité selon les moyens mis en œuvre (1) :

- un niveau élémentaire (*) où une clé cryptographique peut être stockée sous forme logicielle ;
- un niveau standard (**) où la clé est stockée sur un support cryptographique physique comme une « puce électronique » ;
- un niveau renforcé (***) où la clé est également stockée sur un support cryptographique physique et qui est le seul permettant d'élaborer une signature présumée fiable.

²⁴ Décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

Le référentiel général de sécurité et ses annexes permettent ainsi de définir les moyens nécessaires à la mise en œuvre des fonctions de sécurité du système SESAM-Vitale. Compte tenu du caractère hautement confidentiel des données de santé, l'Agence nationale de sécurité des systèmes d'information et l'ASIP Santé certifient respectivement que **la carte Vitale et la carte CPS 3** disposent de caractéristiques techniques permettant la mise en œuvre du niveau de sécurité renforcé (***) (11) (12).

A.1.3. DROITS DES PATIENTS AU REGARD DES DONNEES TRAITEES

Le ministère chargé de la santé a fait de l'année 2011 l'année des patients et de leurs droits afin de renforcer l'effectivité de leurs droits, d'améliorer leur information et de promouvoir leur place dans le système de santé. Le « droit à l'intimité de la vie privée »²⁵ vise ainsi à renforcer la garantie des droits individuels des citoyens tels que le respect du secret relatif à la santé, du secret de la résidence et du domicile ou encore le droit à l'image... Tout patient autorisant un professionnel de santé à procéder au traitement de ses données personnelles dispose ainsi de droits leur permettant d'en prendre connaissance, de les modifier ou les retirer à tout moment. Ces droits fondamentaux doivent garantir à tout patient une parfaite liberté de choix quant à l'utilisation de ses données.

A.1.3.1 DROIT D'INFORMATION ET DROIT D'ACCES

Toute personne doit être informée de la collecte et du traitement de ses données à caractère personnel. Le responsable du traitement doit informer les personnes concernées de son identité, de la finalité du traitement poursuivi, du caractère obligatoire ou facultatif des réponses, des conséquences en l'absence de réponse, des destinataires des données, des droits reconnus de la personne et d'éventuels transferts de données vers un pays hors de l'Union européenne²⁶.

La loi du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé a profondément modifié les modalités d'accès aux dossiers médicaux. Puisque « *toute personne a le droit d'être informée sur son état de santé* »²⁷, chacun peut accéder directement à son dossier médical et aux informations de santé le concernant.

Tout professionnel de santé, dans la limite de ses compétences et dans le respect des règles déontologiques, doit au patient une information claire, délivrée oralement au cours d'un entretien individuel de manière adaptée et compréhensible par le patient sur l'affection dont il souffre, ses symptômes, ses conséquences mais également les investigations, traitements et actions de prévention envisagés et les risques qui y sont associés²⁸. Seules l'urgence ou l'impossibilité d'informer le patient peuvent donc dispenser un professionnel de santé de lui délivrer les informations relatives à son état de santé. Chaque patient peut en outre exprimer la volonté d'être laissé dans l'ignorance d'un diagnostic sauf s'il existe un risque de transmission pour son entourage. Selon une enquête du collectif interassociatif sur la santé (CISS) réalisée en mars 2013, 85% des personnes interrogées considèrent être bien informées sur leur état de santé, leurs soins et leurs traitements (13).

²⁵ Article 9 du code civil.

²⁶ Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, article 32.

²⁷ Articles L.1111-2 et L.1111-7 du code de la santé publique.

²⁸ Des recommandations de bonnes pratiques sur la délivrance de l'information sont établies par la Haute Autorité de santé et homologuées par arrêté du ministre chargé de la santé.

Toute personne justifiant de son identité a donc le droit d'accéder et d'obtenir l'intégralité de ses données à caractère personnel auprès du responsable du traitement²⁹. Ainsi, « *toute personne a accès à l'ensemble des informations concernant sa santé détenues, à quelque titre que ce soit, par des professionnels et établissements de santé* »³⁰. Symbole de la « loi Kouchner » du 4 mars 2002, ce droit est plus ou moins connu des patients mais également des professionnels de santé selon une étude menée par TNS Sofres (14) présentée le 4 mars 2011, 9 ans jour pour jour après son application. Par ailleurs, si le patient a ouvert un dossier médical personnel, il a la possibilité d'accéder directement sur internet, depuis son ordinateur, au contenu de son DMP ainsi qu'au journal des opérations effectuées sur celui-ci.

Qu'elles soient sur support papier ou électronique, les données de santé peuvent être communiquées à la personne concernée soit directement soit par l'intermédiaire d'un professionnel de santé qu'elle désigne³¹. La communication doit être réalisée dans un langage clair (par exemple, par l'indication de la signification des codes utilisés). L'accès aux données se fait, au choix du demandeur, soit par consultation sur place avec éventuellement remise de copies, soit par l'envoi des documents aux frais du demandeur (si possible en recommandé avec accusé de réception) (annexe 1).

La communication des informations doit être faite au plus tard dans les huit jours suivant la demande. Si les informations remontent à plus de cinq ans à partir de la date à laquelle elles ont été constituées, ce délai est porté à deux mois. Préalablement à toute communication, le destinataire de la demande doit vérifier l'identité du demandeur (ou la qualité de médecin de la personne désignée comme intermédiaire).

Les ayants droits d'une personne décédée, sauf volonté contraire exprimée par l'intéressé de son vivant, peuvent accéder à certaines informations du dossier médical afin de connaître les causes de décès, défendre la mémoire du défunt ou faire valoir leurs droits. Ils doivent préciser le motif de la demande d'accès et les professionnels de santé doivent quant à eux s'assurer de l'identité et de la qualité d'ayant droit du demandeur, du motif de la demande et de l'absence d'opposition du défunt (15).

Enfin, « *les professionnels de santé (...) doivent, avant l'exécution d'un acte, informer le patient de son coût et des conditions de son remboursement par les régimes obligatoires d'assurance maladie* »³². Dans ce domaine, la convention nationale organisant les rapports entre les pharmaciens titulaires d'officine et l'assurance maladie rappelle que « *le pharmacien reporte sur l'original de l'ordonnance et, le cas échéant, sur son duplicata lors de la première délivrance les mentions (...) permettant de garantir aux assurés sociaux une bonne information sur le coût des produits de santé qui leur sont délivrés.* »³³. Malgré ces dispositions, seulement 48% des personnes interrogées par le CISS estiment être bien informées sur le prix et les taux de remboursement (13).

Enfin, l'arrêté du 26 mars 2003 relatif à l'information du consommateur sur les prix des médicaments non remboursables dans les officines oblige les pharmaciens à indiquer clairement le prix par un étiquetage sur le conditionnement pour les produits non exposés au public et par un affichage lisible et visible par le client, pour ceux qui sont exposés.

²⁹ Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, article 39.

³⁰ Informations des usagers du système de santé et expression de leur volonté (articles R.1111-1 à R.1111-8 du code de la santé publique).

³¹ Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, article 43.

³² Article L.1111-3 du code de la santé publique.

³³ Arrêté du 4 mai 2012 portant approbation de la convention nationale organisant les rapports entre les pharmaciens titulaires d'officine et l'assurance maladie, article 36.5.2.

A.1.3.2 DROIT AU CONSENTEMENT ET DROIT A L'OUBLI

Le consentement consiste pour le patient à prendre les décisions concernant sa santé : il a la liberté d'accepter, de refuser ou d'interrompre tout acte ou traitement proposé par un professionnel de santé. Pour que des informations puissent être considérées comme confiées à un professionnel de santé celui doit recueillir « *son consentement exprès, par tout moyen, y compris sous forme dématérialisée* ³⁴ ». En pratique le recueil de ce consentement est généralement matérialisé par la remise de la carte Vitale du patient au professionnel de santé l'autorisant indirectement à télétransmettre des feuilles de soins électroniques.

C'est l'article L.1111-4 du code de la santé publique qui définit les grands principes du consentement des malades. Ainsi, « *le médecin doit respecter la volonté de la personne après l'avoir informée des conséquences de ses choix. Si la volonté de la personne de refuser ou d'interrompre tout traitement met sa vie en danger, le médecin doit tout mettre en œuvre pour la convaincre d'accepter les soins indispensables* ». Il précise « *qu'aucun acte médical ni aucun traitement ne peut être pratiqué sans le consentement libre et éclairé de la personne et ce consentement peut être retiré à tout moment. Lorsque la personne est hors d'état d'exprimer sa volonté, aucune intervention ou investigation ne peut être réalisée, sauf urgence ou impossibilité, sans que la personne de confiance, la famille, ou à défaut, un de ses proches ait été consulté. Ce consentement exprès du patient peut être obtenu par voie électronique.* »

La conférence nationale de santé constituée de 113 membres représentant les acteurs du système de santé français permet d'exprimer leurs points de vue sur les politiques de santé et relaie les demandes et les besoins de la population en termes d'état de santé, et d'accès au système de santé. Elle relève que depuis de nombreuses années, des organisations de soins ou des professionnels de santé collectent ou échangent des données de santé sans que jamais le consentement des patients n'ait été recueilli (6). L'article 7 de la loi informatique et libertés oblige pourtant les professionnels de santé à obtenir l'accord du patient pour la création et la transmission d'un fichier de données médicales d'un patient. Dans ces conditions, l'ASIP Santé met à disposition un modèle de note d'information relative au consentement à l'hébergement de données de santé à caractère personnel et au DMP, destiné aux offreurs de soins faisant héberger leur système d'information par un tiers (annexe 2). Si le consentement du patient est obligatoire pour la création et la consultation de son DMP³⁵ ou de son dossier pharmaceutique³⁶, il n'est en revanche pas requis pour la création de son historique de remboursements (web-médecin) établi par l'assurance maladie. Seule la consultation de cet historique requiert le consentement de la personne concernée³⁷.

Afin de limiter la durée de conservation des données de santé au strict nécessaire, la loi informatique et libertés introduit enfin le principe d'un « **droit à l'oubli** » précisant que les données personnelles « *sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées* »³⁸.

³⁴ Article L.1110-4 du code de la santé publique.

³⁵ Article L.1111-15 du code de la santé publique.

³⁶ Article L.1111-23 du code de la santé publique.

³⁷ Article L.162-4-3 du code de la sécurité sociale.

³⁸ Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, article 6.

A.1.3.3 DROITS D'OPPOSITION ET DE RECTIFICATION

Sauf obligation légale, « toute personne physique a le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement »³⁹. De même, « toute personne physique justifiant de son identité peut exiger du responsable d'un traitement que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou effacées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite »⁴⁰.

Les personnes dont les données sont traitées par un professionnel de santé sont informées (par un document affiché dans les locaux d'exercice ou remis en main propre), de l'identité du responsable du traitement, de sa finalité, des destinataires des informations et des modalités pratiques d'exercice de leurs droits d'accès, d'opposition, de rectification des informations qui les concernent. Cette affichette informative (annexe 3) est mise à la disposition de différents corps de métiers du système de santé (cabinets médicaux, paramédicaux et dentaires, lieux de soins, opticiens, pharmacies, services hospitaliers, laboratoires d'analyses...) par la CNIL dans son « guide pour les professionnels de santé ».

A.1.3.4 CAS PARTICULIER DES PERSONNES MINEURES ET SOUS TUTELLE

Le code de la santé publique prévoit des dispositions particulières en matière d'information, de recueil du consentement et de secret médical des patients mineurs. De manière générale, les droits des personnes mineures et de celles majeures protégées à l'information sur leur état de santé et le consentement aux soins, sont exercés par les titulaires de l'autorité parentale pour les mineurs et par le tuteur pour les majeurs sous tutelle⁴¹. Cependant, des nuances sont apportées à ce principe dans le sens où ces usagers au statut particulier ont le droit, en vue de participer aux décisions qui les concernent, à une information adaptée respectivement à leur degré de maturité et à leur capacité de discernement. Ainsi, un mineur peut s'opposer à ce qu'un médecin communique au titulaire de l'autorité parentale des informations qui le concernent. Le médecin fait alors mention écrite de cette opposition⁴².

Selon l'article L.1111-5 CSP : « le médecin peut se dispenser d'obtenir le consentement du ou des titulaires de l'autorité parentale sur les décisions médicales à prendre lorsque le traitement ou l'intervention s'impose pour sauvegarder la santé d'une personne mineure, dans le cas où cette dernière s'oppose expressément à la consultation du ou des titulaires de l'autorité parentale afin de garder le secret sur son état de santé. Toutefois, le médecin doit dans un premier temps s'efforcer d'obtenir le consentement du mineur à cette consultation. Dans le cas où le mineur maintient son opposition, le médecin peut mettre en œuvre le traitement ou l'intervention. Dans ce cas, le mineur se fait accompagner d'une personne majeure de son choix ».

³⁹ Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, article 38.

⁴⁰ Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, article 40.

⁴¹ Conformément aux articles L.1111-2, L.1111-4 et L.1111-7 du code de la santé publique.

⁴² Article R.1111-6 du code de la santé publique.

Chapitre 2 : LA GENESE DE DONNEES ELECTRONIQUES

Du fait de sa proximité et de sa disponibilité le pharmacien est un interlocuteur privilégié des patients afin d'évoquer leur santé. L'accueil de tout patient au comptoir d'une officine, quelle que soit sa requête, suggère ainsi l'établissement d'un dialogue, clé de voûte d'une relation de confiance indispensable avec son pharmacien. La multiplication des outils informatiques assistant ce dernier dans l'exercice de son art ne doit cependant pas détourner son attention du patient et de ses maux. Cet entretien personnalisé permet tout d'abord au pharmacien de prendre connaissance du motif de sa venue (plainte, dispensation de produits de santé, information, conseil...), d'informations relatives à son état de santé (données physiologiques, pathologiques, biologiques, cliniques...) ou à d'autres traitements (traitements en cours, allergies, contre-indications...).

Parfois muni de documents complémentaires ou de correspondances utiles à la dispensation (analyses biologiques, protocoles thérapeutiques, carnets de suivi...), tout patient peut ainsi bénéficier d'une analyse précise de sa requête par un professionnel de santé compétent. Dans ce domaine, l'utilisation de logiciels spécialisés (logiciels de gestion d'officine ou LGO) permet de créer un dossier de suivi pharmaco-thérapeutique pour chaque patient tout en assistant le pharmacien dans la recherche d'incompatibilités liées à une dispensation. Alors que les dossiers médicaux ou l'ordonnancier au format papier permettent depuis longtemps de disposer d'un historique des prestations servies à chaque patient, l'émergence des NTIC a rendu ces données disponibles rapidement et n'importe où sur le territoire via le dossier pharmaceutique.

Si l'identification précise du patient est fortement recommandée lors de toute dispensation, elle n'est obligatoire que lors de la dispensation de produits de santé inscrits sur la liste des substances vénéneuses. Dans ce cas, le pharmacien enregistre le nom et l'adresse du malade, ou le nom et l'adresse du détenteur du ou des animaux, ou la mention « usage professionnel ».

Par ailleurs, la prise en charge de dépenses de santé par les organismes d'assurance maladie impose le recueil de données administratives afin de rapprocher une dispensation et ses données de facturation. Le nom, et le prénom du bénéficiaire ainsi que la date de la prestation, l'identification de la caisse de l'assuré ainsi que son « numéro de sécurité sociale » ou NIR sont autant de données devant être collectées à partir de supports de natures variées. Dans le cas idéal, tout patient muni d'une carte Vitale est identifié par le système informatique officinal au moyen de son identifiant national de santé (INS) calculé par le logiciel du pharmacien. Les données administratives utiles à la dispensation et la facturation de produits de santé sont ainsi lues à partir de la carte et exploitées par le logiciel. De nombreux supports d'identification des bénéficiaires de l'assurance maladie au format papier peuvent également être présentés (attestation de droits, carte de mutuelle...).

Si les informations contenues dans ces documents peuvent être ajoutées « manuellement », par saisie informatique au dossier informatisé de chaque patient, la généralisation des scanners en officine permet désormais de les numériser si besoin. En effet, les récentes avancées en matière de dématérialisation permettent aujourd'hui aux pharmaciens de numériser les ordonnances au moment de la dispensation afin de s'affranchir de l'envoi des duplicatas aux organismes d'assurance maladie concernés. Couplée à la télétransmission des factures au format électronique, la télétransmission de pièces justificatives numériques a récemment permis de franchir un pas décisif dans la modernisation de notre système de santé.

Par ailleurs, l'utilisation d'un logiciel d'aide à la dispensation et du dossier pharmaceutique disponible via internet permet de bénéficier d'un niveau d'information de plus en plus élevé au fur et à mesure des dispensations.

Nous verrons enfin que l'évolution des moyens d'identification et des techniques de marquage des produits de santé constitue une composante fondamentale de leur dispensation, de leur facturation et de leur traçabilité.

A.2.1. LE POSTE DE TRAVAIL INFORMATIQUE OFFICINAL

Comme tous les secteurs de l'économie, la pharmacie a été marquée au cours des vingt dernières années par la révolution de l'informatique. Compte tenu de l'incertitude qui pèse sur l'applicabilité des cadres juridiques aux nouveaux systèmes d'e-santé, les préoccupations relatives à la confidentialité des données de santé peuvent constituer un obstacle à la généralisation de l'usage des NTIC. Une enquête visant à évaluer l'impact de ces technologies sur les conditions de travail, menée par le centre d'analyse stratégique et la direction générale du travail, révèle que les pharmacies font parties des PME françaises les mieux équipées et donc armées pour assurer le traitement de données de santé en toute sécurité (16).

Lui promettant gain de temps et efficience, l'ordinateur est ainsi devenu en quelques années un outil de travail incontournable de tout pharmacien. En automatisant de nombreuses tâches, l'évolution des technologies de l'informatique doit leur permettre d'accroître et d'optimiser le temps accordé à chaque patient, pourvu qu'ils en maîtrisent parfaitement l'utilisation. Mais la réalité est parfois toute autre. Le manque de formation ou la méconnaissance de l'outil informatique peuvent perturber le professionnel de santé dans l'accomplissement de sa mission première, monopolisant son attention au détriment de la qualité de l'acte. Il est donc primordial que tous adhèrent à la démarche de modernisation du système de soins afin que leurs patients puissent bénéficier des avantages des NTIC au cours de leur prise en charge.

L'installation et la mise en service du système informatique officinal est généralement laissée à des sociétés de services et d'ingénierie informatique (SSII). Considérant le coût d'une telle installation, le pharmacien ne doit pas se tromper dans le choix de cette société et doit pour cela évaluer (17) :

- la pérennité de l'entreprise ;
- la qualité du contrat de maintenance et son coût ;
- la qualité de la formation et son coût ;
- les capacités d'évolution et d'interopérabilité du matériel et des logiciels ;
- la garantie de certification des logiciels proposés.

A.2.1.1 CONFIGURATION MATERIELLE

Afin d'optimiser l'utilisation de son système informatique, tout pharmacien s'efforce d'adopter une organisation logique du matériel sur son lieu de travail. Leur mission première de dispensation étant principalement réalisée au comptoir de l'officine, celui-ci correspond donc à son poste de travail. Selon ses besoins, toute officine peut disposer, d'un ou plusieurs postes informatiques organisés et interconnectés de manière logique.

Avec la tendance actuelle d'« explosion des comptoirs » des pharmacies d'officine, le poste de travail du pharmacien est configuré de façon à le rendre aussi autonome que possible dans son travail. Il comporte ainsi tous les outils nécessaires au bon déroulement des ventes et des délivrances d'ordonnances (tampons, tiroir-caisse...) mais également une panoplie d'outils informatiques réunis en un même poste de travail. Directement intégré au comptoir de l'officine chaque poste permet ainsi d'effectuer la majeure partie de l'acte de dispensation en présence du patient.

Chaque poste informatique comporte généralement :

- un ordinateur composé d'une unité centrale et d'un moniteur souvent encastrés dans le comptoir afin d'optimiser leur rangement et l'accueil des patients ;
- des périphériques d'entrée : clavier, souris, lecteurs de codes barre et scanner ;
- un périphérique de sortie : imprimante utilisable par tout logiciel installé dans le système informatique : traitement de texte, bons de promis, impression du ticket vitale et des feuilles de soins papier...
- un lecteur de cartes à puce électronique permettant d'accéder aux ressources du système SESAM-Vitale en toute sécurité au moyen de la carte Vitale du patient et de la carte CPS du pharmacien.



Figure 1 : Le poste de travail informatique officinal.

A.2.1.1.a Les périphériques informatiques

Afin d'assurer la transmission des données entre l'ordinateur et chaque périphérique, chacun d'eux est relié à la carte mère de l'unité centrale par l'intermédiaire de connecteurs ou ports, véritables portes d'entrée du système informatique, souvent associés à un « code couleurs ».

Les ports les plus couramment utilisés sont :

- Les ports PS/2 (*Personal System/2*) permettent de connecter une souris et un clavier ;
- Les ports USB permettent de connecter par exemple un lecteur SESAM-Vitale, un scanner, une imprimante, une clé USB, une souris ou un clavier...
- Les ports « Firewire » permettent de connecter un disque dur externe, par exemple ;
- Les ports « audio » associés à la carte son permettent de connecter un microphone ou des enceintes ;
- Le port parallèle permet de connecter certains anciens modèles d'imprimantes ;
- Le connecteur LAN de la carte réseau branchée sur la carte mère permet de connecter un câble réseau de type RJ45 afin de relier l'ordinateur à un réseau ;
- Le port série permet de connecter certains matériels (manettes de jeu...)
- Le port VGA de la carte graphique connectée à la carte mère permet de relier l'écran (moniteur) à l'unité centrale.

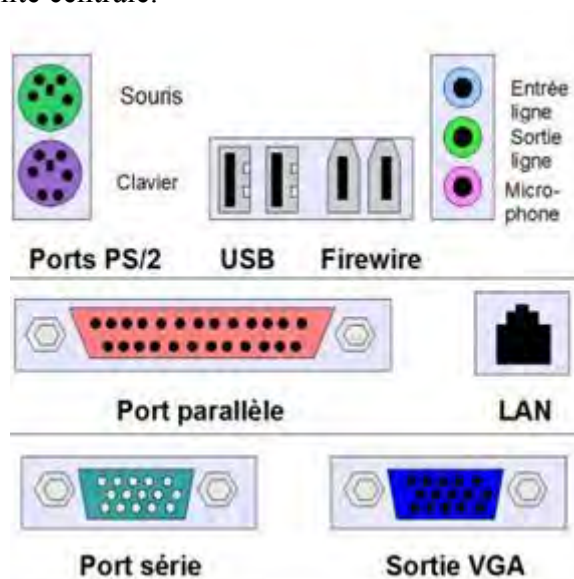


Figure 2 : Principaux connecteurs de périphériques de l'unité centrale d'un ordinateur.

Si le système informatique officinal offre au pharmacien d'incroyables capacités d'analyse et de stockage, il ne faut pas perdre de vue que toute base de données, pour être efficace, doit être alimentée. Qu'ils s'agisse de données de santé ou non, les professionnels de santé ont actuellement à leur disposition de nombreux outils permettant d'alimenter les fichiers de leurs logiciels professionnels.

Même si le poids de fichiers informatiques composés de données textuelles est réduit, le développement des techniques d'acquisition d'images de qualité toujours plus fine implique

l'utilisation de moyens de stockage et de transmission des données électroniques performants. Il est ainsi possible de distinguer différents outils d'acquisition selon la nature des données de la source, qu'il s'agisse de texte, d'images ou encore de code-barres.

- **Le clavier** est le principal périphérique permettant à son utilisateur d'entrer des données textuelles sous forme électronique dans un système informatique. Il est composé de touches alphabétiques, numériques et des touches de fonction dont la disposition est variable selon le pays (en France on parle de clavier AZERTY). A chaque pression d'une touche du clavier, un signal électrique spécifique est transmis à un micro-contrôleur, qui envoie un code à l'ordinateur décrivant le caractère correspondant à la touche.

Des jeux de caractères comme la table ASCII⁴³ ont été définis affectant à chacun de ces octets un caractère alphanumérique (A-z, 0-9) ou un caractère de ponctuation ou encore un caractère non-imprimable dit de contrôle : la tabulation, le retour à la ligne... Ainsi pour transcrire le français (avec ses majuscules) il faut compter deux fois 26 lettres, environ 35 caractères spéciaux (lettres accentués...), les dix digits (0-9), et au moins une vingtaine de caractères de ponctuation (dont l'espace), soit plus de 120 caractères.

- **La souris** est un dispositif de pointage pour ordinateur. Ce petit boîtier est composé de plusieurs boutons et d'une molette dans la plupart des cas. Elle permet de pointer, sélectionner et déplacer des éléments affichés à l'écran mais encore de faire défiler l'écran ou une liste. Elle permet également l'exécution de programmes ou de fonctions spéciales en cliquant sur les boutons dont les fonctions prédéfinies sont paramétrables. Concrètement, la souris d'ordinateur permet la saisie de données en sélectionnant et validant une valeur d'un menu déroulant. Elle est peu utilisée au comptoir de l'officine par les pharmaciens car l'attribution de raccourcis claviers aux logiciels de gestion d'officine par leurs éditeurs permettent d'accéder très rapidement aux différentes fonctions sans utiliser la souris.

- **Le microphone** permet à la fois de réaliser une communication vocale en temps réel avec un interlocuteur mais aussi d'enregistrer des données audio sur un support de mémoire. Particulièrement utilisé par les médecins afin d'éditer leurs comptes rendus de consultations, l'enregistrement vocal de données sur un support est retranscrit *a posteriori* par saisie et mise en forme du texte au moyen d'un logiciel de traitement de texte. D'autres systèmes permettent de dicter un texte à un ordinateur équipé d'un microphone couplé à un logiciel de reconnaissance vocale qui retranscrit fidèlement et en temps réel, les paroles de l'utilisateur dans un logiciel de traitement de texte..

- **Le scanner** est un périphérique informatique externe capable de transformer un document sur papier en image numérique. La numérisation est rendue possible grâce à des capteurs sensibles à la lumière rediffusée par les couleurs des documents. Ces capteurs, appelés capteurs CCD (*Charge Coupled Device*), sont composés de photodiodes dont la conductivité électrique dépend de l'intensité lumineuse. Si l'on numérise un document opaque, les capteurs mesurent l'intensité de la lumière réfléchie par le document tandis que pour un document transparent, les capteurs mesurent la lumière qui traverse ce document. S'il existe plusieurs méthodes, la numérisation linéaire est la plus couramment employée par les scanners de bureau. Le document est posé contre une vitre sous laquelle un miroir et une source de lumière effectuent ensemble un balayage linéaire (18).

Les photodiodes sont disposées en barrette sur toute la largeur de la surface exposée du document. En se déplaçant, la source lumineuse éclaire le document au travers de la vitre, la

⁴³ American standard code for information interchange.

lumière réfléchi par le document est renvoyée par le miroir mobile à un système optique qui analyse l'image ligne par ligne. Chaque ligne scannée est composée de points « élémentaires » ou pixels dont la position et la teinte sont analysées et mémorisées afin de reconstituer numériquement l'image au moyen d'un ordinateur. Il en existe de nombreux types selon les applications mais les scanners à « rouleaux » de nouvelle génération sont parfaitement adaptés à l'application officinale en raison de leurs dimensions réduites et leur facilité d'utilisation. Dans ce type de scanner, c'est le document, entraîné par des rouleaux, qui est mobile et défile devant la source lumineuse.

Couplés à un logiciel de reconnaissance optique de caractères ou OCR (*Optical Character Recognition*), ils permettent la traduction d'images de textes imprimés ou manuscrits en fichiers de texte informatisés éditables. Il est ainsi possible d'obtenir l'image numérique d'un texte sur format papier, analysée par le logiciel OCR qui produit un fichier texte (simple, au format traitement de texte...). Certains logiciels comportent également un système d'acquisition numérique de l'image et un système d'enrichissement du texte et de mise en page permettant de reproduire le document original aussi fidèlement que possible.

• **Les lecteurs de code-barres 1D** utilisent la propriété de la réflexion de la lumière sur une surface claire et d'absorption sur une surface foncée. Un lecteur de code-barres peut s'avérer utile pour faciliter la saisie de données dans le système informatique comme les codes médicament présents sur la vignette pharmaceutique et les conditionnements ainsi que pour la saisie du numéro d'identification du prescripteur, parfois exprimé sous forme d'un code-barres sur les ordonnances.

Lorsque le faisceau lumineux du lecteur balaye une surface qui alterne entre des espaces clairs et foncés, cela génère un signal électrique dont la variation en amplitude et en fréquence pourra être rapportée à un symbole donné et par conséquent, à une information ou à un message. La durée du signal électrique détermine l'épaisseur des éléments, puis le décodeur du lecteur convertit ce signal en caractères, qui sont ensuite transmis à l'ordinateur.

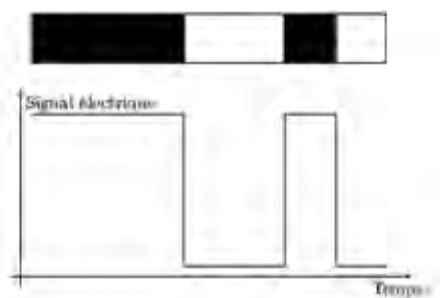


Figure 3 : Principe de lecture d'un code-barres unidimensionnel.

Il existe par exemple, les crayons pour une lecture de contact en utilisant un système de LED mais ce sont le plus souvent des lecteurs LASER à lecture omnidirectionnelle, fixes, propres à chaque comptoir et reliés directement au poste informatique qui sont utilisés à l'officine. Des lecteurs portatifs sont également utilisés dans certaines officines pour réaliser les inventaires ou la réception de marchandises.

On distingue principalement :

- Les lecteurs CCD qui sont composés de plusieurs diodes produisant un faisceau de lumière rouge diffus qui intensifie le contraste entre les barres du code. Ils se présentent sous la forme d'une douchette équipée le plus souvent d'une gâchette qui permet de déclencher le faisceau lumineux. Le signal de retour est analysé par un

capteur photographique, appelé également capteur CCD. Simples d'utilisation ils ne sont cependant capables de lire certaines symbologies uniquement s'il s'agit de modèles longue distance (long range) ;

- Les lecteurs LASER, bien que plus onéreux sont les plus volontiers utilisés au comptoir officinal. Généré par une diode LASER couplée à un système de miroir rotatif ou oscillant, le faisceau lumineux possède un large pouvoir couvrant et permet ainsi de lire aisément les différents types de codes-barres unidimensionnels. Le signal de retour est ensuite analysé par un phototransistor. Elle se présente sous forme de douchette (souvent utilisée pour réaliser les inventaires) ou de poste fixe à lecture omnidirectionnelle et offre de meilleures performances que les douchettes à diodes en permettant de lire à longue distance tous les codes-barres unidimensionnels.

• **Les lecteurs de Datamatrix ou codes 2D** sont le plus souvent équipés d'imageurs ou caméras CCD capables de scanner les Datamatrix et de les enregistrer. Cette technologie applique les mêmes principes de fonctionnement que les lecteurs CCD linéaires sauf que le signal n'est pas capturé linéairement mais décodé par capture de la représentation du code 2D au moyen d'un capteur numérique comparable à celui d'un appareil photo numérique. Les lecteurs CCD Imager, sont conçus pour décoder tout ce qu'ils trouvent dans leur fenêtre de capture et lire les codes 1D et 2D les plus courants, comme le Datamatrix. Cette image sera ensuite décodée par le logiciel du lecteur pour déterminer sa nature et son contenu. Celui-ci transfère la chaîne de caractères présents dans le Datamatrix au système informatique de l'officine qui en analyse, gère et exploite le contenu (19).

Tout comme les lecteurs 1D, il est possible de trouver de nombreux types de lecteurs en deux dimensions sur le marché comme des scanners de petite taille adaptés au travail au comptoir, logés dans le poste de dispensation auquel ils sont reliés pour la transmission des flux d'information ou d'autres, portatifs, embarquant un logiciel et adaptés au travail d'arrière-boutique qui requiert une plus grande mobilité.

Ces lecteurs sont proposés aux pharmaciens d'officine par les sociétés d'informatique officinale sous formes d'un paquet « matériel et logiciel » au prix moyen de 250 à 300 euros HT par paquet soit environ 1500 euros pour une officine de 5 comptoirs. Cependant, tous les lecteurs ne sont pas de qualité équivalente (20).

Le pharmacien doit prendre en compte différents paramètres pour orienter son choix vers le matériel le plus performant et au meilleur coût. Il est ainsi nécessaire de considérer les capacités de traitement de l'image, de décodage, les qualités optiques ainsi que l'inclusion de systèmes permettant l'interprétation d'un code-barres déformé, endommagé ou imprimés en couleurs inversées. Cependant, même si les difficultés de lecture rencontrées initialement par les pharmaciens semblent avoir été surmontées, la vitesse d'acquisition dite « agressivité » des Datamatrix, n'est toujours pas aussi élevée que celle des codes 1D malgré l'évolution des lecteurs.

A.2.1.1.b Les mémoires informatiques

Afin d'en permettre le traitement automatisé, toute donnée électronique est enregistrée dans la mémoire d'un système informatique. Le stockage de données électroniques ne se limite cependant pas au disque dur d'un ordinateur. De nombreux périphériques externes et supports amovibles de données électroniques peuvent être utilisés selon les besoins de l'utilisateur, la miniaturisation des composants électroniques permettant ainsi de stocker des quantités de données colossales dans un espace très réduit (21).

L'unité de mesure informatique est le bit⁴⁴ symbolisé « b ». Il s'agit d'une valeur binaire (0 ou 1) décrivant schématiquement un système à deux états : ouvert ou fermé. La combinaison de huit bits constitue un octet « o ». Un octet permet donc de coder 2^8 , soit 256 valeurs différentes représentées, soit sous forme d'un entier naturel entre 0 et 255 compris (en base 10), soit par la succession de huit chiffres binaires. On définit ainsi que un kilobit vaut 2^{10} bits soit 1024 bits.

Ces données s'inscrivent dans des mémoires à plus ou moins long terme selon le type de support utilisé et sont exploitées par les différents composants du système informatique. Dans le cas d'un ordinateur, la carte mère constitue le socle d'interconnexion de composants permettant le traitement des octets par un microprocesseur, afin d'être exploités par l'utilisateur à l'aide d'une interface logicielle adaptée.

La mémoire est un dispositif électrotechnique permettant de stocker des données électroniques. Pièce maîtresse d'un ordinateur, on la rencontre également dans certains supports de stockage tels que les cartes à puce ou les clés USB. La mémoire informatique désigne deux catégories de supports matériels de données selon l'utilisation qui lui est vouée.

Les mémoires volatiles sont des mémoires de travail qui s'effacent lorsque l'alimentation électrique s'arrête. Elles participent au bon fonctionnement d'un système électronique (comme un ordinateur ou une carte à puce) en stockant temporairement des données afin de les mettre à disposition du processeur. C'est par exemple le cas de la mémoire vive ou RAM (*Random Access Memory*) rapidement mise à disposition. Elle reste cependant onéreuse pour une faible capacité de stockage.

Les mémoires rémanentes ne s'effacent pas lors de la mise hors tension du système, elles jouent un véritable rôle de stockage de données à long terme. Il peut s'agir de la mémoire morte ou ROM (*Read Only memory*) qui contient des informations non modifiables et définies par le fabricant comme le système BIOS (*Basic Input Output System*) d'un ordinateur ou le masque d'une carte à puce électronique. Les mémoires de masse (disques-durs, CD, DVD, clés USB) qui sont susceptibles de contenir de très grandes quantités de données rentrent également dans cette catégorie. Tout comme certaines mémoires programmables utilisées par exemple dans les clés USB (FLASH) ou les cartes à puce électronique (EEPROM⁴⁵), ce sont des mémoires de fonctionnement lent.

A.2.1.2 LES LOGICIELS DE GESTION D'OFFICINE

Outre le système d'exploitation⁴⁶ et les logiciels destinés au grand public (traitement de texte, navigateur internet, Acrobat Reader®...), la couche logicielle de tout système informatique officinal est dotée d'un logiciel professionnel spécialisé ou logiciel de gestion d'officine. Celui-ci intègre un ensemble complet et documenté de programmes conçus pour être fournis à plusieurs utilisateurs en vue d'une même application ou d'une même fonction. Au cœur du système informatique officinal, il est utilisé par l'ensemble de l'équipe et permet d'automatiser et de coordonner de nombreuses opérations autour de la dispensation des produits de santé et de la gestion administrative et économique de l'officine.

⁴⁴ De l'anglais *binary digit*

⁴⁵ *Electrically-erasable programmable read-only memory*, mémoire morte programmable et effaçable électriquement.

⁴⁶ La liste des environnements acceptant les fournitures SESAM-Vitale étant susceptible d'évoluer, elle est de ce fait mise à jour sur le site du GIE SESAM Vitale : <http://www.SESAM-vitale.fr>.

Pour l'aider dans le choix du logiciel de gestion de son officine, le pharmacien peut se référer aux recommandations de sa SSII, de son répartiteur ou utiliser le logiciel fourni par le groupement auquel il adhère. En effet, les groupements se chargent de référencer un logiciel et d'en négocier les coûts d'achat, d'installation et de maintenance auprès des SSII mises en concurrence afin de décharger autant que possible les pharmaciens de ces préoccupations. C'est pourquoi certains groupement créent et distribuent leur propre logiciel afin de répondre au mieux aux attentes des adhérents (Logiphar® de Giphar® par exemple).

A.2.1.2.a La certification des logiciels d'aide à la dispensation

La loi relative au renforcement de la sécurité sanitaire du médicament et des produits de santé du 29 décembre 2011 rend obligatoire la certification des logiciels d'aide à la prescription (LAP) « *au plus tard le 1er janvier 2015* » et confie également à la Haute Autorité de santé un rôle de **certification des logiciels d'aide à la dispensation (LAD)**⁴⁷.

Cette procédure de certification du module d'aide à la dispensation des logiciels de gestion d'officine doit participer à l'amélioration des pratiques de dispensation officinale et garantir la conformité des logiciels à des exigences minimales en termes de sécurité et de conformité de la dispensation afin de répondre aux objectifs suivants :

- sécuriser la dispensation des produits de santé ;
- faciliter la vérification de la conformité de l'ordonnance ;
- mettre à disposition des informations et des conseils nécessaires au bon usage des médicaments dispensés.

Comme nous le verrons, l'inclusion de bases de données médicamenteuses au cœur des logiciels de gestion d'officine constitue un point essentiel de la certification des logiciels d'aide à la prescription et des logiciels d'aide à la dispensation.

A.2.1.2.b Les fichiers des logiciels de gestion d'officine

Un logiciel de gestion d'officine peut être décrit comme une plateforme permettant l'interconnexion de différentes applications intégrées dont le fonctionnement repose sur l'exploitation de fichiers organisés en véritables bases de données permettant de stocker des informations multiples de façon structurée et avec le moins de redondances possible.

La plupart des fonctionnalités proposées par les logiciels de gestion d'officine reposent ainsi sur la présence de volumineux fichiers permettant au pharmacien de disposer de nombreuses données utiles à la gestion de l'activité économique de l'officine mais aussi à la dispensation et à la facturation des produits de santé. Les principaux fichiers utilisés sont (17) :

• **Le fichier « assuré »** répertoriant l'ensemble des patients de la pharmacie qui bénéficient du tiers-payant ou de la délégation de paiement. A chaque assuré correspond une fiche électronique à laquelle les bénéficiaires sont rattachés selon leur rang. Ce fichier comprend généralement des informations :

- administratives : nom, prénom, date de naissance, NIR, adresse numéro de téléphone, régimes d'assurance maladie, crédits en cours...

⁴⁷ Article L.161-38 du code de la sécurité sociale.

- thérapeutiques : historique des délivrances, prescripteurs associés, produits avancés ou promis ;
- médicales : utiles aux dispensations de produits de santé (allergies, état physiopathologique comme une insuffisance rénale, hépatique...).

Le contenu de chaque fiche individuelle permet de constituer une importante base de données dont chaque dossier pourra être « appelé » selon des critères plus ou moins précis. Il est possible d'identifier spécifiquement chaque dossier au moyen du NIR ou de tout autre trait d'identification tels que le nom de famille, le prénom, la date de naissance... permettant d'affiner les critères de recherche.

- **Le fichier « contrats »** recense l'ensemble des contrats proposés par les organismes de prise en charge de régime obligatoire et/ou complémentaire géré par l'officine. Un ou plusieurs contrats peuvent être associés à chaque assuré bénéficiant du tiers-payant, en précisant leurs dates de validités et le numéro d'adhérent.

- **Le fichier « organismes »** répertorie les différents organismes de régimes obligatoires et complémentaires des assurés de l'officine ainsi que les contrats associés. Ce fichier est en étroite relation avec la **table de codification des organismes destinataires** contenant l'ensemble des données de codification des organismes d'assurance maladie conformément à la norme B2 utilisée pour la télétransmission des données de facturation électroniques. Chaque organisme est identifié par un triplet de codes : le code « grand régime », le numéro de « caisse gestionnaire » et le numéro de « centre gestionnaire ». A chaque triplet correspond une ligne de la table à laquelle est associée l'adresse électronique de la caisse destinataire des flux de factures électroniques.

- **Le fichier « prescripteurs »** dresse la liste de l'ensemble des praticiens prescripteurs auxquels les patients de l'officine ont recours. L'identification du prescripteur est associée à toute dispensation de produits de santé soumis à une prescription médicale. Il est identifié au moyen de son numéro RPPS et/ou ADELI et le code de sa spécialité est précisé en vue de la télétransmission SESAM Vitale. Afin de constituer un fichier efficace, les informations relatives aux prescripteurs doivent être régulièrement mises à jour et aussi complètes que possible (adresse postale ou de messagerie électronique, numéro de téléphone, fax ...).

- **Le fichier « vendeurs »** regroupe l'ensemble du personnel susceptible de dispenser des produits de santé à l'officine. Il permet ainsi d'identifier le responsable de chaque opération qu'il effectue (vente, commande, modification des stocks...) mais également d'élaborer des statistiques de ventes.

- **Le fichier « produits »** recense l'ensemble des informations relatives aux produits commercialisés par l'officine qu'il s'agisse de produits de santé ou non. Il comporte des informations détaillées sur les produits telles que les monographies (en relation avec une base de données médicamenteuse) et les fiches de produits de parapharmacie éventuellement enrichies de photos. Il en précise d'une part la forme, le prix de vente, son éventuel taux de prise en charge et permet la gestion de son réapprovisionnement, du stock et de son rangement dans l'officine d'autre part. Il permet en outre de réaliser une étude statistique précieuse afin de visualiser la rotation du stock ainsi que l'historique des achats et des ventes de ce produit sur une période donnée.

Afin d'alimenter ce fichier, un nouveau produit peut être ajouté manuellement ou automatiquement à partir des données du site d'un répartiteur pharmaceutique (« Le point »

de l'OCP par exemple) ou via les mises à jour régulières proposées par les SSII (par internet ou CD-ROM).

- **Les bases de données médicamenteuses** indexées aux logiciels d'aide à la prescription et aux logiciels d'aide à la dispensation⁴⁸ intéressent de près la Haute Autorité de santé, dont l'agrément atteste de leur qualité. Compte tenu du nombre (en perpétuelle augmentation) de médicaments sur le marché, les professionnels de santé disposent depuis bien longtemps de sources d'informations reconnues afin de les assister dans leurs prescriptions et leurs dispensations⁴⁹. Les monographies des médicaments ayant reçu une autorisation de mise sur le marché sont ainsi publiées sous forme de véritables dictionnaires et renseignent particulièrement les résumés des caractéristiques des produits (RCP) ainsi que les informations économiques publiées au Journal Officiel. En consultant le RCP de tout médicament, un professionnel de santé peut parfois lever certains doutes liés à la prescription ou à la dispensation d'un médicament compte tenu du contexte. Il peut ainsi en vérifier la composition, les indications précises, les posologies et modalités d'administration, les précautions d'emploi, les contre-indications, les interactions, les effets indésirables, les propriétés pharmacocinétiques et pharmacodynamiques.

L'informatisation de ces professions a donc logiquement conduit les éditeurs de logiciels à inclure ces informations dans leurs outils sous forme de véritable bases de données. A ce jour, quatre bases de données ont reçu l'agrément afin d'être incluses aux logiciels d'aide à la prescription et aux logiciels d'aide à la dispensation : Vidal, Thériaque, Claude Bernard et Thésorimed (22).

Disposer ainsi « en clin d'œil » d'un ensemble structuré de données exhaustives, exactes et à jour présente de nombreux avantages. Outre la mise à disposition rapide des monographies directement au comptoir de dispensation, le réel atout de cette base de données réside dans ses interactions avec les différents modules proposés par le logiciel de gestion d'officine. Comme nous le verrons, la fonction d'aide à la dispensation offerte par tout logiciel de gestion d'officine permet de confronter les données de cette base de données **entre elles et avec celles relatives à un patient** enregistrées via les différents dispositifs proposés aux pharmaciens. Cet outil ne doit cependant pas aliéner le pharmacien dans son jugement et ses choix, il s'agit de le conforter ou non dans sa décision de conclure une dispensation par la délivrance d'un médicament.

A.2.1.2.c Principales fonctions des logiciels de gestion d'officine

Les présentations et les fonctions de ces logiciels de gestion d'officine ont évolué au fil des années afin de s'adapter aux exigences et aux besoins élargis de l'équipe officinale. Ils proposent un ensemble coordonné d'outils visant à améliorer l'efficacité de la dispensation et de la facturation des produits de santé ainsi que la gestion économique et administrative de l'officine.

- **Des outils de gestion des stocks et des registres** permettent de mettre en œuvre l'ordonnancier électronique ainsi que les registres comptables électroniques obligatoires. Il permet en outre de connaître l'évolution des stocks de tous les produits vendus par l'officine et de calculer une périodicité optimale de réapprovisionnement auprès des organismes répartiteurs et des laboratoires.

⁴⁸ Par opposition aux banques documentaires destinées à être consultées sur internet comme celle de l'Agence nationale de sécurité du médicament.

⁴⁹ Le dictionnaire Vidal au format papier existe depuis 1914.

La gestion informatisée des stocks constitue pour toute officine un outil stratégique permettant d'optimiser l'approvisionnement en adéquation avec la demande. Afin de proposer un échantillon de produits de santé adapté à la demande d'une clientèle toujours plus exigeante, tout pharmacien titulaire peut solliciter l'aide de son logiciel afin de choisir le bon produit au bon moment, en bonne quantité et au bon prix tout en lui accordant le bon emplacement au sein de l'officine (23).

Les logiciels de gestion d'officine permettent aujourd'hui de réaliser un suivi rigoureux des ventes et des stocks mais demande tout de même une bonne méthodologie et un sens de l'organisation. En effet, la mise en œuvre de la gestion des stocks passe par la mise en place d'une véritable procédure d'assurance qualité nécessitant une longue préparation en amont afin de réaliser un inventaire physique précis de l'ensemble des références disponibles et de constituer un stock aussi juste que possible.

Le principal atout de la gestion informatisée des stocks est de maîtriser le volume et donc le coût du stock tout en proposant un échantillon de produits adapté (suffisant mais non excessif au regard du coût d'immobilisation du stock). Une fois l'inventaire physique réalisé, le logiciel de gestion d'officine analysera les entrées et sorties de chaque produit afin de proposer automatiquement au pharmacien les quantités d'unités à commander en tenant compte de l'état actuel du stock, de la demande actuelle, de la saisonnalité du produit...

Afin de déterminer la période optimale de réapprovisionnement d'une unité de production, les logiciels de gestion d'officine se basent sur la formule mathématique de Wilson qui considère :

- le coût de lancement d'une commande ;
- la consommation annuelle prévisionnelle ;
- le coût unitaire du produit ;
- le taux de possession du stock (24).

Le pharmacien reste bien évidemment libre de modifier ces paramètres avant la télétransmission du bon de commande électronique vers le fournisseur (répartiteur ou laboratoire). Dans ce domaine, la norme Pharma-ML est une norme de télétransmission permettant un échange direct entre le pharmacien d'officine et ses fournisseurs, et garantit l'authentification et la sécurité de cet échange. Intégrée directement aux logiciels de gestion d'officine, cette norme facilite la passation des commandes par internet tout en automatisant la gestion des stocks. Elle est reconnue par l'ensemble des fournisseurs et propose une interrogation des stocks et des prix de la base des produits de chaque fournisseur ainsi que la réception de bons de livraison valorisés. La dernière version de la norme Pharma ML (version 3) intègre les impératifs réglementaires de la traçabilité (code produit, numéro de lot et date de péremption).

Cette analyse du stock par le logiciel de gestion d'officine permet donc d'étudier facilement la rotation des produits et de réaliser des simulations de fixation des prix et de marge tout en comparant les différentes offres des fournisseurs. Le pharmacien peut ainsi bénéficier de commandes groupées, de promotions facilitant le choix de ses fournisseurs et les négociations commerciales. La justesse et la pertinence d'un stock n'est possible que si un suivi régulier du stock physique est réalisé (par exemple par zone géographique de la pharmacie). Une mise en adéquation du stock informatique et du stock réel doit donc être effectuée périodiquement afin

de limiter le nombre de « manquants » et de pointer les produits à faible rotation (évitant ainsi les périmés).

- L'ordinateur du poste de travail officinal faisant office de caisse enregistreuse informatique, permet également de réaliser une **gestion des ventes** et un **suivi des transactions financières** réalisées pour le compte de l'officine. Le **progiciel de facturation** est historiquement la première fonction proposée par les logiciels de gestion d'officine.

Lors de l'appel d'un produit (généralement par saisie de son code-barres) une ligne de facturation est ajoutée à la facture. Le pharmacien précise le nombre d'unités vendues et le progiciel calcule le montant correspondant en indiquant les éventuels taux de prise en charge. Lorsqu'une nouvelle ligne de facturation est créée, le logiciel permet la recherche en direct d'éventuelles interactions entre les différents produits saisis. A la fin du processus de facturation informatique, les différents fichiers du logiciel de gestion d'officine sont mis à jour en conséquence (mise à jour des stocks, gestion du tiers-payant, gestion des encaissements...) (3).

Il est possible de distinguer plusieurs types de facturation à l'officine (3) :

- **La facturation générique** de produits non soumis à prescription médicale (médicaments conseils, cosmétiques, phytothérapie, aromathérapie...) avec ou sans identification du client ;
- **La facturation « Pro-forma »** permet la facturation des produits inscrits sur la Liste des Produits et Prestations Remboursables (LPPR) qui nécessitent l'établissement d'une entente préalable. Il permet d'en établir le prix avant la livraison afin de réaliser les formalités nécessaires à son acquisition ;
- **La facturation réduite** permet l'édition d'un ticket de caisse simple ;
- **La facturation SESAM-Vitale**, avec identification obligatoire du patient, permet enfin la création de factures (ou feuilles de soins) destinées aux organismes d'assurance maladie en vue d'une prise en charge partielle ou totale des dépenses. Couplé à un **module de numérisation des pièces justificatives**, il permet d'apporter tous les justificatifs nécessaires à la prise en charge des produits de santé par les organismes d'assurance maladie.

Tout assuré porteur d'une carte Vitale à jour ou, à défaut, d'une attestation papier justifiant l'ouverture des droits, peut bénéficier sous certaines conditions d'une dispense d'avance des frais médicaux. L'assurance maladie rembourse les frais médicaux sur la base de **tarifs de responsabilité** et les sommes restantes, correspondant au **ticket modérateur**, sont à la charge de l'assuré mais peuvent être partiellement ou totalement prises en charge par un organisme complémentaire.

Le principe du **tiers-payant pharmaceutique**⁵⁰ dispense un assuré de régler le montant des frais remboursables par l'assurance maladie, l'avance étant réalisée par le pharmacien. Le tiers-payant peut être **partiel** lorsque l'assuré paie uniquement le ticket modérateur ou **total** lorsque l'assuré n'a aucun frais à régler.

⁵⁰ Introduit par l'article L.162-16-7 du code de la sécurité sociale.

Suite à la commission paritaire nationale du 6 juin 2012 introduisant le **dispositif « tiers-payant contre génériques »**, les pharmaciens doivent cependant réserver le tiers payant aux seuls assurés acceptant la substitution des médicaments par leur générique⁵¹.

Le suivi des factures transmises aux assurances maladies nécessite un contrôle quotidien rigoureux afin de limiter le nombre de factures rejetées par les caisses. Chaque facture étant identifiée par un numéro, le pharmacien édite la liste des factures électroniques transmises qu'il pourra mettre en parallèle avec les flux retours de l'assurance maladie notifiant l'avis de règlement ou de rejet. Cette fonction permet de corriger d'éventuelles erreurs du processus de facturation (faute de frappe, erreur administrative...) et de relancer automatiquement un avis de paiement aux organismes payeurs.

Les logiciels de gestion d'officine permettent donc de réaliser une analyse du chiffre d'affaires net par type de transaction (tiers-payant, hors tiers-payant, hors ordonnance...) et d'analyser les mouvements de trésorerie pour le mettre en parallèle avec les sommes effectivement calculées lors du comptage de chaque caisse, les différents types de règlements, les crédits...

Des outils d'analyse des ventes permettent également d'imputer directement une vente à un vendeur rendant ainsi possible des analyses statistiques au service du pharmacien titulaire afin d'analyser et faire évoluer les compétences de vente de chaque vendeur dans un domaine particulier (phytothérapie, cosmétique, compléments alimentaires...). Il permet également de réaliser un bilan journalier, mensuel ou annuel des ventes afin d'analyser les périodes les plus propices (heure de la journée, saison...) selon le type de produit et la valeur du panier moyen.

Outre ces fonctions principales indispensables à l'activité économique de toute officine, d'autres outils permettent la gestion du personnel (contrats, emplois du temps...), la mise en place de politiques de prix et de merchandising, la création de supports de communication (édition d'étiquettes, affiches)...

• **La fonction d'aide à la dispensation** vise à assister le pharmacien afin d'améliorer la qualité, la sécurité et l'efficacité de leurs dispensations. Ce module permet la détection d'incompatibilités (contre-indications, interactions, surdosage...) lors de chaque dispensation sur ordonnance ou sur conseil. Il met en parallèle le fichier du patient et les monographies de la base de données afin d'alerter le pharmacien face à toute incompatibilité entre un produit de santé et l'état de santé du patient ou d'autres spécialités d'une même dispensation ou d'une dispensation précédente. En étroite relation avec le dossier de suivi pharmaco-thérapeutique, cette fonction ne doit en aucun cas se substituer aux connaissances et aux capacités d'analyse du pharmacien, il s'agit d'un « garde-fou » assistant le pharmacien dans sa décision et permettant d'améliorer la qualité d'une dispensation et le suivi thérapeutique du patient.

La majorité des logiciels de gestion d'officine offre également certaines fonctions supplémentaires comme **l'aide à la prise d'un médicament** par le patient visant à prévenir certains risques ou accidents liés à leur mésusage. A la fin de chaque dispensation, le logiciel de gestion d'officine permet ainsi d'éditer et imprimer un « plan de prises » des médicaments permettant au patient de se remémorer à chaque instant les modalités d'application de la stratégie thérapeutique adoptée. Le contenu de ce document personnalisé est structuré selon la

⁵¹ Cette règle ne s'applique pas dès lors que le médecin prescripteur porte la mention « non substituable » sous forme manuscrite, écrite en toutes lettres et placée en face de chacune des lignes de prescription auxquelles elle s'applique.

règle des « B » : le bon médicament, à la bonne dose, au bon moment et selon la bonne voie d'administration (3).

Un **progiciel d'aide à la gestion du préparatoire** peut également permettre la prise en charge de certaines tâches liées à la fabrication des préparations magistrales ou officinales et des produits officinaux divisés conformément aux règles de bonnes pratiques de préparation.

Comme nous le verrons, les logiciels de gestion d'officine intègrent également des modules permettant d'une part l'élaboration d'opinions pharmaceutiques et du dossier de suivi pharmaco-thérapeutique et d'autre part la création et l'alimentation du dossier pharmaceutique en ligne du patient. Ces fonctions visant à mettre véritablement l'informatique au service de la dispensation des produits de santé seront étudiées plus précisément dans la deuxième partie.

A.2.2. LE SYSTEME ELECTRONIQUE DE SAISIE DE L'ASSURANCE MALADIE

Le **système électronique de saisie de l'assurance maladie (SESAM)** est un dispositif voué à développer l'automatisation et la dématérialisation de transactions entre les assurés sociaux, les professionnels de santé et les régimes obligatoires et complémentaires d'assurance maladie. Ce projet porté depuis 1993 par le GIE SESAM-Vitale qui en assure la conception et la mise en œuvre avait pour objectif initial de diminuer les coûts de gestion des feuilles de soins générées par les professionnels de santé grâce à une organisation reposant sur la saisie informatique des informations permettant le remboursement des dépenses de santé à sa source. Si la carte Vitale développée par le GIE SESAM-Vitale était initialement réservée à l'identification des patients et de leurs droits pour la facturation de soins et de produits de santé, ses applications sont désormais élargies. L'accès aux systèmes informatisés de santé est ainsi verrouillé par deux cadenas dont la carte Vitale et la carte CPS constituent les clés.

A.2.2.1 CONTEXTE REGLEMENTAIRE

L'ordonnance du 24 avril 1996 relative à la maîtrise des dépenses de santé a donné au projet toute sa légitimité et marqué son lancement en prévoyant la diffusion de cartes à puce individuelles comme support d'identification des assurés. Cette orientation stratégique, dès le lancement du programme, a fait de la France le précurseur de la généralisation à grande échelle de cette technologie dans le monde de la santé⁵². Elle oblige ainsi les professionnels, et les organismes ou établissements qui dispensent des actes ou des prestations prises en charge par l'assurance maladie à être équipés afin de pouvoir émettre, signer, traiter et recevoir les feuilles de soins électroniques (FSE)⁵³. C'est ainsi que le GIP-CPS eut pour mission de définir, émettre et gérer les cartes CPS des professionnels de santé dès 1993 afin de répondre aux exigences d'identification et de sécurité du projet SESAM-Vitale⁵⁴.

Si tout professionnel de santé a la liberté de choix de l'équipement informatique grâce auquel il établit les FSE et les télétransmet, il doit cependant utiliser des équipements agréés par le centre national de dépôt et d'agrément (CNDA) de l'assurance maladie, ou de ceux homologués par le GIE SESAM-Vitale (conformément au cahier des charges).⁵⁵

⁵² Echéance fixée au 31 décembre 1999.

⁵³ Echéance fixée au 31 décembre 1998.

⁵⁴ C'est aujourd'hui l'Agence nationale des systèmes d'information partagés de santé qui est en charge d'assurer la gestion des cartes CPS.

⁵⁵ Arrêté du 4 mai 2012 portant approbation de la convention nationale organisant les rapports entre les pharmaciens titulaires d'officine et l'assurance maladie, article 37.2.2.

Outre la télétransmission des FSE par les professionnels de santé habilités, ce système propose certaines fonctions spécifiques à certains modes d'exercice comme la dématérialisation des ordonnances, du feuillet d'accident du travail, du guide de maternité, du carnet de soins gratuits... (25) En effet, les missions du système SESAM-Vitale ont récemment été élargies afin de permettre la numérisation et la télétransmission de pièces justificatives numériques par certaines catégories de professionnels de santé parmi lesquelles les pharmaciens font figure de locomotive. Ce système en perpétuel évolution permet donc de proposer un panel de services toujours plus large qui pourrait se concrétiser davantage avec la dématérialisation de la prescription à la source.

Compte tenu du caractère hautement confidentiel des informations traitées, l'enjeu principal de ce système est de garantir l'authenticité, l'intégrité et la confidentialité des données dématérialisées. C'est ainsi que la dernière version du cahier des charges émis par le GIE SESAM-Vitale (version 1.40 addendum n°6) précise les contraintes et spécifications matérielles aux fournisseurs d'équipements agréés. Pour un fonctionnement optimal, ce système nécessite toutefois une infrastructure technique complexe, gage de sécurité et d'interopérabilité, comprenant :

- Des supports d'identité électroniques sous forme de cartes à puce électronique individuelles ainsi que leurs outils associés (lecteurs et bornes de mise à jour) ;
- Une infrastructure logicielle permettant d'accéder au contenu des cartes et d'en exploiter les données au moyen de lecteurs adaptés ;
- Des infrastructures de télécommunication et d'hébergement permettant la transmission des données et leur éventuel stockage.

A.2.2.2 LES CARTES A PUCE ELECTRONIQUE

Si les supports d'identification présentés par les patients peuvent être de nature variée (attestation papier, carte de mutuelle...), la généralisation des cartes Vitale et CPS comme support d'identification national des patients et des professionnels de santé rend la carte à puce incontournable au sein des systèmes d'information de santé. Invention française, elle est composée d'une structure (généralement en matière plastique) à laquelle un circuit imprimé (la puce) est intégré. Ce dernier contient un microprocesseur capable de traiter des données (enregistrées dans la mémoire de la carte ou non), ou limité à des circuits de mémoires non volatiles et, éventuellement associé à un composant de sécurité. Ces cartes se sont multipliées dans notre quotidien et nous sommes amenés à en utiliser différentes chaque jour (cartes de paiement, de transport en commun, carte SIM des téléphones portables...) et peuvent présenter certaines fonctions particulières comme le mode sans contact équipant certaines cartes de dernière génération.

Il est possible de distinguer deux types principaux de cartes à puce individuelles utilisées avec le système SESAM-Vitale : la carte Vitale (actuellement dans sa 2^{ème} version) et les cartes CPS des professionnels de santé (3^{ème} version). Initialement vouées à la dématérialisation du processus de facturation des produits et actes de santé pris en charge par l'assurance maladie, ces cartes n'ont cessé d'évoluer techniquement offrant de nouvelles fonctions, gages de sécurité et d'interopérabilité des systèmes. En évoluant techniquement, la carte Vitale propose ainsi de nouvelles fonctions au service des patients, des professionnels de santé et de l'assurance maladie comme la consultation du DMP, du dossier pharmaceutique et du web médecin, avec l'accord préalable du patient. La remise de sa carte Vitale au professionnel de santé matérialisant son accord pour la télétransmission des données de facturation à

l'assurance maladie n'exprime en revanche pas son consentement pour le traitement, l'hébergement de ses données et l'utilisation des dossiers médicaux partagés. Ce rôle ambigu de la carte Vitale a d'ailleurs été soulevé par la CNIL qui considère que la simple remise de la carte n'atteste pas de la réalité du consentement du patient.

La carte CPS constitue quant à elle la clé d'entrée de la e-santé d'aujourd'hui et de demain. Elle était jusqu'à présent utilisée principalement dans le cadre de la production des feuilles de soins électroniques de l'assurance maladie, mais est dorénavant inscrite, comme nous l'avons vu, comme un outil obligatoire imposé pour l'accès aux données de santé à caractère personnel, notamment dans le cadre du partage de l'information médicale. Dans ce cadre, la carte de professionnel de santé constitue un instrument essentiel du dispositif de sécurité des systèmes d'information de santé en sécurisant les échanges et le partage des données de santé afin d'en préserver la confidentialité (26).

Elle permet notamment aux professionnels de santé de :

- s'identifier et s'authentifier fortement dans un système d'information afin d'éviter une usurpation de leur identité ;
- sécuriser la télétransmission des factures électroniques ;
- créer, alimenter et consulter le DMP ou le dossier pharmaceutique de leurs patients
- réaliser des actes médicaux à distance (télémédecine) ;
- utiliser des outils de messagerie sécurisée destinées aux professionnels de santé ;
- s'identifier pour accéder à des locaux grâce à la technologie sans contact.

Ce travail collaboratif entre le GIE SESAM-Vitale et l'ASIP Santé permet aujourd'hui de proposer un service certifié visant à automatiser ou dématérialiser les échanges d'information entre les professionnels de santé et les organismes d'assurance maladie (obligatoire ou complémentaire) en toute sécurité. Ce système aura permis de réaliser 1,2 milliard de transactions sécurisées en 2011 (27).

A.2.2.2.a Standards de conception

Qu'il s'agisse de la carte Vitale 2 ou de la carte CPS3, elles sont élaborées selon des standards communs :

• **Le standard ISO 7816** qui s'organise autour de quinze normes définissant les caractéristiques des cartes à puce fonctionnant par contact électrique comme :

- les caractéristiques physiques de la carte (support) et de la puce électronique : forme, dimensions, contraintes physiques acceptables, dimensions et positions des contacts ;
- les caractéristiques électriques et les protocoles de communication avec les lecteurs;
- les moyens de sécurisation et de codage des données ;
- le format des paquets de données transmises entre la carte et le lecteur...

Ce « format de carte bancaire » (format ID1 de 85 mm par 54 mm pour une épaisseur de 0,76 mm), fait de la carte à puce un outil facilement transportable que l'on peut toujours avoir sur soi en cas de besoin. La miniaturisation des composants électroniques regroupés dans une puce de taille réduite (environ 1/20^{ème} de la surface de la carte) leur permet d'embarquer un microprocesseur de technologie réinscriptible couplé à des supports de mémoires RAM, ROM et EEPROM⁵⁶ permettant le stockage des données et le fonctionnement d'applications embarquées (28).

- **Le standard ISO 14443** décrit les spécificités du module de communication « sans contact » utilisé par de telles puces comme celle de la carte CPS3. En effet, dans un souci d'ergonomie et pour ouvrir la carte CPS à de nouveaux usages, ce nouveau mode de communication a été ajouté aux fonctionnalités de la CPS3 permettant à l'utilisateur d'utiliser sa carte sans avoir à l'insérer dans la fente d'un lecteur, réduisant de ce fait les manipulations à effectuer et l'usure du support. Elle est équipée pour cela d'un composant unique permettant le mode dual, c'est-à-dire offrant les deux modes de communication « contact » et « sans contact » grâce à une antenne noyée dans le support plastique. Ce module de transmission est conforme au protocole normalisé ISO 14443 A ou B, selon le composant embarqué, et activé dès que la carte se trouve dans le champ électromagnétique d'un lecteur sans contact (estimé à 10 cm maximum). En théorie, les fonctionnalités accessibles dans les modes contact et sans contact sont potentiellement les mêmes. Toutefois, la stratégie de migration et les contraintes liées à l'utilisation d'une telle interface impliquent certaines limitations d'usage du mode sans contact.

- **Le standard européen de sécurité IAS (pour identification, authentification, signature)⁵⁷** décrit les moyens d'identification, d'authentification et de signature électronique utilisés par de telles cartes afin de se conformer aux exigences de sécurité définies par le référentiel général de sécurité. Comme nous l'avons vu, ce référentiel définit les moyens à mettre en œuvre afin d'assurer la sécurité des échanges dématérialisés entre les usagers et l'administration selon le niveau de sécurité visé. S'agissant des données de santé, le niveau visé est le niveau renforcé « *** ». Cela se traduit en terme d'implémentation matérielle et logicielle par l'emploi de fournitures cryptographiques (crypto-processeur) permettant aux applications embarquées de procéder à l'authentification de son porteur et d'élaborer des signatures électroniques conformément à l'échelle d'évaluation du produit selon des critères communs au niveau renforcé (29) (12).

Il existe deux versions de ce standard IAS :

- les spécifications IAS Premium v1.01 (2006) auxquelles sont conformes les cartes Vitale 2 (11) ;
- les spécifications IAS ECC (2010) auxquelles sont conformes les cartes CPS3 qui proviennent de la mise en conformité pour le développement d'une carte d'identité électronique européenne (*European citizen card*) permettant l'interopérabilité des cartes au niveau européen (12).

⁵⁶ 48 Ko de mémoire EEPROM pour la carte vitale 2 (11)

⁵⁷ *Identification, authentication and electronic signature for the european citizen card*. Spécifié par le GIXEL, il s'appuie sur le standard français IAS Premium.

Ce standard offre un double avantage :

- la mise en conformité aux exigences de sécurité de niveau (***) du référentiel général de sécurité ;
- une interopérabilité des systèmes dont le fonctionnement repose sur l'utilisation de telles cartes, constituant ainsi le socle de développement de l'ensemble de l'identité et donc de l'économie numérique européenne. En effet les cartes élaborées conformément à ce standard permettent l'usage de lecteurs PC/SC dits transparents qui équipent en standard certains postes de travail ou qui sont disponibles sous forme de périphériques bon marché. Ces spécifications doivent ainsi permettre la normalisation des échanges entre la carte et le terminal et de disposer d'une offre industrielle interopérable.

A.2.2.2.b La carte Vitale 2 et ses données personnelles

Délivrée gratuitement depuis 1998 aux bénéficiaires de l'assurance maladie française de plus de seize ans, la carte Vitale est une carte électronique individuelle inter-régimes qui en identifie chaque bénéficiaire (titulaire de la carte ou de ses ayants droit, mineurs ou conjoint)⁵⁸. Quel que soit le régime, elles sont identiques et valables sur l'ensemble du territoire tout au long de la vie de son titulaire.

La première version de la carte Vitale diffusée était une carte familiale (assurés et ayants droit). Elle fut distribuée aux ayants droit de seize ans et plus à partir de 2001 et les enfants de moins de seize ans peuvent aujourd'hui être inscrits sur les cartes des deux parents à la demande de ces derniers (15). Elle fut progressivement remplacée à partir de novembre 2006 par la nouvelle carte Vitale 2 enrichie notamment de la photo de l'assurée et dont plus de vingt millions d'exemplaires ont été distribués (27). Cette évolution porte sur des caractéristiques techniques offrant de nouvelles fonctions mais aussi sur son contenu qui s'est enrichi.

Si elle est entièrement gratuite pour le bénéficiaire, son coût de production unitaire est estimé à 2,70 €. Les cartes Vitale 2 vierges produites chaque année par l'entreprise SELP à Mareuil en Dordogne sont ensuite personnalisées soit par un sous-traitant⁵⁹ soit par la Caisse nationale d'assurance maladie dans leur centre spécialisé de Cergy-Pontoise (Val-d'Oise). A ce sujet, la tentative avortée de délocalisation de la production de la carte Vitale 2 en Inde en décembre 2011 est en contradiction avec son fondement même : le besoin de sécurisation⁶⁰.

L'un des premiers avantages des cartes à puce sur leur équivalent papier consiste en l'inscription de données à la fois sur le support mais également dans la puce électronique, les rendant invisibles sans l'utilisation d'un lecteur approprié. Si la sécurisation de l'accès au contenu des cartes Vitale a parfois été remise en cause il est important de ne pas perdre de vue que cette carte, bien que dotée d'une mémoire EEPROM de 48 ko, n'est pas utilisée comme support de stockage de données de santé proprement dites, mais comme support d'identification des patients et de données administratives. Le GIE-SESAM-Vitale avait malgré tout initialement prévu un volet « santé » voué à remplacer le carnet de santé par un fichier informatique porté par la carte Vitale mais ce projet avorta en 2007 avec le lancement du projet du DMP.

⁵⁸ Article L.161-31 du code de la sécurité sociale.

⁵⁹ Société Euro P3C, filiale du groupe Crédit Mutuel.

⁶⁰ JO du 05/07/2012, Sénat, page 1426, question orale sans débat n° 1634S de Monsieur le Sénateur Bernard Cazeau.

La carte Vitale 2 contient donc des informations personnelles sur l'assuré inscrites dans sa puce électronique (48 Ko de mémoire EEPROM) et d'autres, directement lisibles, imprimées sur la carte. Le périmètre de ces informations est règlementairement défini par le décret n°2007-199 du 14 février 2007 relatif à la carte d'assurance maladie.

- **Les données visibles de la carte Vitale 2** peuvent être illustrées par le modèle de présentation de la carte fourni par l'assurance maladie permettant de visualiser la disposition des informations imprimées sur la matrice de la carte.

DONNEES VISIBLES IMPRIMEES SUR LA CARTE VITALE 2	
RECTO	VERSO
 - La date d'émission de la carte ; - Le nom et le prénom du titulaire de la carte ; - Le NIR de l'assuré ; - La photographie du porteur ; - Le numéro de série logique de la carte Vitale (utilisé pour la télétransmission des FSE) verticalement à côté de la photographie; - Un signe d'identification en relief pour les personnes malvoyantes.	 - Le numéro de série physique de la carte et un code-barres dans lequel il est encodé (utilisé en phase de production des cartes) ; - La date de fabrication.

Tableau 1 : Présentation des informations imprimées sur la matrice de la carte Vitale.

La photographie doit correspondre aux spécifications de la norme ISO/IEC 19794-5:2005 des cartes d'identité et passeports. Elle doit être récente, faite par un photographe ou dans une cabine photo agréée, en couleur, de taille 35 mm x 45 mm, sur fond clair et uni, visage centré de face et tête nue.

- **Les données inscrites dans la puce de la carte Vitale 2** ne sont pas présentées en tant que telles par la dernière version du cahier des charges SESAM-Vitale (addendum n°6 avec erratum Mars 2012) (30). En effet, seule l'organisation des volets de données inscrites dans les versions précédentes de la carte (versions 1bis et 1ter) ainsi que leurs modalités d'accès en lecture et en écriture sont mentionnées. Lors de son lancement en 2006, la carte Vitale 2 fut d'ailleurs présentée par le GIE comme une carte Vitale 1ter personnalisée par la photographie de l'assuré et certaines données spécifiques dites « données vitale 2 » (31).

Le contenu des différents volets de la carte Vitale 1ter ainsi que leurs modalités d'accès en lecture et en écriture au moyen de lecteur homologué sont présentées dans l'annexe 4. Ces données inscrites dans la puce électronique comprennent :

- les données visibles imprimées sur la carte présentées ci-dessus : nom, prénom, date de naissance et NIR de l'assuré ainsi que le numéro de série logique et la date de validité de la carte et la photo sous forme numérique.
- les données relatives aux droits aux prestations en nature au regard d'un régime de base d'assurance maladie ;
- les données relatives, le cas échéant et sous réserve de son consentement, à la situation du titulaire au regard de la protection complémentaire d'assurance maladie ;
- les données relatives au choix du médecin traitant du titulaire de la carte ;
- les données relatives à la situation du titulaire en matière d'accident du travail ou de maladies professionnelles ;
- les données relatives à l'accès aux soins en cas de séjour ou résidence dans un autre Etat membre de l'Union européenne (formulaires E111, E112 et E128) ;
- les données personnelles concernant les coordonnées d'une personne à prévenir en cas de nécessité si le titulaire de la carte y a consenti ;
- la mention indiquant que son titulaire a eu connaissance des dispositions de la réglementation sur le don d'organe ;
- des données permettant d'assurer la mise en œuvre des fonctions de signature électronique, de protéger l'accès aux informations de la carte et d'authentifier la carte en tant que carte d'assurance maladie et d'identifier son titulaire.

A.2.2.2.c Les cartes de la famille CPS et leurs « données métier »

Les cartes de la famille CPS sont des cartes d'identité professionnelle électroniques contenant les données d'identification de son porteur (identité, profession, spécialité) mais aussi sa situation d'exercice (cabinet ou établissement).

C'est l'entreprise Oberthur Technologies© qui, depuis 2011, assure la réalisation de l'actuelle version de la carte (CPS3) dans sa totalité, de la conception à la certification, en passant par la personnalisation ainsi que l'envoi aux professionnels de santé pour le compte de l'ASIP Santé. Protégée par un code confidentiel ou code porteur, la carte CPS constitue le maillon final d'une chaîne de confiance qui permet à son titulaire d'attester de son identité et de ses qualifications professionnelles (12).

La CPS3 est distribuée gratuitement et systématiquement à tout professionnel de santé (libéral et hospitalier) inscrit au tableau des quatre ordres professionnels suivants : pharmaciens, sages-femmes, chirurgiens-dentistes et médecins. Les autres professionnels non encore inclus dans le répertoire partagé des professionnels de santé peuvent en faire la demande, ce service est désormais gratuit. Cette gratuité est justifiée par le caractère obligatoire de la carte pour effectuer certaines transactions électroniques sécurisées. La 3^{ème} et dernière version en date de la CPS diffusée par l'ASIP Santé offre de nouvelles fonctionnalités et de meilleures garanties

de sécurité. On distingue différents types de cartes suivant la profession exercée et le niveau de responsabilité du porteur (32):

- La CPS pour les professions de santé réglementées par le code de la santé publique ;
- Pour les professions non réglementées par le code de la santé publique et les salariés d'une structure de soins :
 - ❖ La CDE (carte de directeur d'établissement) pour les responsables de structures de soins ;
 - ❖ La CPE (carte de personnel d'établissement) pour les personnels des établissements de soins comme les préparateurs en pharmacie. Elle est délivrée à la demande et sous la responsabilité d'un titulaire d'une CPS ou d'une CDE auquel l'activité du salarié est rattachée, par exemple pour un préparateur en pharmacie.
 - ❖ Pour les professionnels non réglementés et salariés de structures autorisées :
 - La CDA pour les responsables de structure ;
 - La CPA pour les personnels de structure.

Déclinée sous des visuels de couleurs différentes pour chaque profession concernée afin d'en faciliter l'identification visuelle, la CPS3 comporte comme la carte Vitale des informations imprimées sur son support et d'autres inscrites dans la puce électronique. A titre d'exemple, la CPS3 destinée aux pharmaciens intègre le motif visuel de l'ASIP Santé de couleur verte (rouge pour les médecins) et renseigne sur sa face l'intitulé de la carte, la qualification, le numéro d'identification du professionnel de santé (RPPS ou, le cas échéant ADELI), son nom et son prénom ainsi que la date d'expiration de la carte et son numéro de série logique (verticalement en bas à droite).



D'un point de vue électronique, les données métier sont retranscrites dans 2 zones distinctes de stockage de la puce :

- Le volet CPS2ter qui contient les données métier telles qu'elles étaient présentes dans la version précédente de la CPS : la CPS2ter dont le contenu et la structure sont conservés afin d'assurer une compatibilité totale avec les différents dispositifs ;
- Le volet IAS qui contient les données métier CPS mises à jour dont le format est adapté pour se mettre en conformité avec le RPPS.

DONNEES METIERS INSCRITES DANS LA PUCE DE LA CPS3 (12)
DONNEES RELATIVES AUX ACTIVITES DU PROFESSIONNEL DE SANTE
Données relatives à la carte elle-même - Identifiant de l'émetteur de la carte fourni par l'ASIP Santé (10 caractères numériques mentionnés sur la première ligne de la face avant de la carte) - Identifiant IAS : numéro unique de la carte attribué par l'ASIP Santé composé de 19 caractères décimaux - Catégorie de carte, dates de début et de fin de validité : 1^{er} et dernier jour de validité de la carte et du certificat associé Données relatives au porteur en tant que personne physique Civilité, nom patronymique, nom marital, prénoms, codes langues (jusqu'à 4 langues) Données relatives au porteur en tant que professionnel de santé - Type de carte : CPS, CPE... - N° d'identification nationale du porteur de la carte - Code profession et nom d'exercice - Spécialité ordinale ADELI (volet CPS2ter) et spécialité ordinale RPPS (volet IAS) Données liées aux situations d'exercice du porteur - Mode d'exercice (libéral, salarié, remplaçant), statut, et niveau de responsabilité - Tableau de pharmacien - Identification nationale ADELI pour application SESAM-Vitale - Identification nationale de la structure et raison sociale - Secteur d'activité ADELI (volet CPS2ter) et secteur d'activité RPPS (volet IAS) Données de sécurité - Code porteur et code déblocage - Certificats X.509 d'authentification et de signature (et bi-clés associés) - Certificat technique d'authentification en mode sans contact et le bi-clé correspondant (volet IAS)
DONNEES ACCESSIBLES EN MODE SANS CONTACT
Afin de se conformer aux exigences de la CNIL, seules des données non nominatives peuvent être échangées via le protocole ISO 14443. On distingue : - Le numéro de série sans contact : La carte CPS3 émet un identifiant fixe et propre à chaque carte composé du numéro de série du composant défini et inscrit par le fabricant de la puce. - L'identifiant technique (ou numéro logique IAS) : numéro unique de la carte accessible via le jeu de commandes IAS aussi bien en mode sans-contact qu'en mode contact. - Un certificat technique X.509 d'authentification en mode sans contact; - Une zone de données applicatives réservée pour le stockage de données applicatives (4096 octets) accessible uniquement via le jeu de commandes IAS, aussi bien en mode sans-contact qu'en mode contact.
DONNEES DU DOMAINE ASSURANCE MALADIE (DAM)
Les DAM sont des informations nécessaires à la facturation (situations d'exercice et de facturation) initialement présentes dans la version précédente de la carte CPS. Même si le principe de la suppression de ces informations a été voté par le GIP-CIPS en janvier 2003, elles sont maintenues dans le volet CPS2ter afin d'assurer la compatibilité avec les applications terrain existantes et ne sont accessibles qu'avec le jeu de commandes CPS2ter.

Tableau 2 : Présentation des données métier inscrites dans la puce de la carte CPS3.

A.2.2.3 LECTURE ET MISE A JOUR DES CARTES A PUCE

La lecture, l'acquisition de données ainsi que la mise en œuvre des fonctions de sécurité des cartes à puce électroniques passe par l'utilisation d'un périphérique lecteur dédié et de fournitures logicielles embarquées dans ce lecteur et dans la couche logicielle du système informatique officinal. Si les lecteurs homologués SESAM-Vitale constituent le socle de développement technique des solutions de facturation, le standard IAS offre la possibilité d'utiliser ces cartes avec des lecteurs standards.

A.2.2.3.a Procédures d'agrément et d'homologation des interfaces

En marge de la certification des modules d'aide à la dispensation et des bases de données médicamenteuses par la Haute Autorité de santé, les éditeurs de logiciels de gestion d'officine doivent aussi respecter les contraintes fixées par le GIE SESAM-Vitale pour la conception de leurs modules de facturation. Afin d'attester de la qualité de ces outils, les progiciels de facturation des logiciels de gestion d'officine ainsi que les interfaces de lecture font l'objet de procédures de qualification auprès d'autorités compétentes. **La commission de validation et d'homologation** du GIE SESAM-Vitale prononce ainsi la validation des modalités d'agrément et d'homologation⁶¹ octroyés par le centre national de dépôt et d'agrément (CNDA) qui en garantit la conformité aux référentiels correspondants.

L'agrément⁶² **SESAM-Vitale** est nécessaire pour les solutions de facturation logicielles utilisant un module progiciel de facturation ou un module de scannérisation des ordonnances (SCOR). Au 31 décembre 2012, 17 progiciels pharmaciens étaient agréés SESAM-Vitale 1.40 contre 10 fin 2011 et 80% des postes de travail des pharmaciens étaient équipés de cette version, soit près de 20 000 officines, contre 3 500 fin 2011 (33).

L'homologation⁶³ **SESAM-Vitale** concerne les autres configurations afin de s'assurer de la conformité des produits (lecteurs et terminaux de mise à jour) ou services développés par un industriel aux exigences du référentiel d'homologation⁶⁴.

L'objectif est de s'assurer de la conformité des flux transmis au travers du réseau SESAM-Vitale afin de garantir (34):

- des délais de remboursement rapides et un traitement égal de tous les assurés,
- le paiement des prestations de tiers-payant aux professionnels de santé,
- un taux de rejet minimum pour les régimes d'assurance maladie ;
- une procédure unique de référencement connue et reconnue aux éditeurs de logiciels.

La version actualisée du cahier des charges élaboré par le GIE SESAM-Vitale permet aux logiciels de facturation de prendre dorénavant en compte la liste d'opposition incrémentale, le format à 13 caractères des codes CIP et le RPPS. Au 30 Janvier 2013, 82% des pharmacies télétransmettent leur flux de facturation sous cette version logicielle. Afin de permettre aux éditeurs déjà titulaires de l'agrément SESAM-Vitale en version 1.40, d'ajouter à leur progiciel

⁶¹ <http://www.cnda-vitale.fr>

⁶² Agrément : Déclaration de conformité aux dispositions légales. Acceptation, reconnaissance, généralement de caractère officiel par une autorité (dictionnaire Larousse).

⁶³ Homologation : Reconnaissance, déclaration de conformité aux règlements en vigueur, à certaines normes (dictionnaire Larousse).

⁶⁴ Ce référentiel est mis à disposition des industriels après constitution d'un dossier.

de santé un module de télétransmission des pièces justificatives relatives aux lots de FSE, un agrément supplémentaire est nécessaire. Pour l'obtenir, l'éditeur doit signer le protocole d'agrément avec le CNDA en conformité avec le cahier des charges SCOR v2.10.

TYPE DE PROCEDURE	REFERENTIEL VALIDE CVH
Agrément des solutions de facturation	Cahier des charges SESAM-Vitale 1.40 (addendum n°6)
Agrément SCOR	Cahier des charges SCOR v2.10
Homologation Terminal Lecteur	Référentiel Terminal Lecteur v3.30
Homologation Télé-mise à jour	Référentiel Télémise à jour v3.10
Homologation Interface PC/SC	Référentiel Accès Cartes - Interface PC/SC v1.02

Tableau 3 : Correspondance entre les types de procédures d'agrément ou d'homologation et les référentiels validés.

A.2.2.3.b Les lecteurs de cartes à puce

Un lecteur homologué SESAM-Vitale est un appareil programmable élaboré conformément aux spécifications du référentiel « Terminal lecteur » du GIE SESAM-Vitale garant de son homologation⁶⁵. Il permet la lecture et l'acquisition de données inscrites dans les puces électroniques des cartes Vitale et CPS et participe à la sécurisation de la facturation des produits et prestations de santé. Il existe deux grands types de lecteurs homologués :

- Le terminal lecteur, fixe, connecté en permanence au poste de travail du professionnel de santé ;
- Le terminal lecteur applicatif complet et le terminal lecteur réduit, portatifs, utilisés par les professionnels de santé ayant un besoin de mobilité.

Les lecteurs utilisés en officine sont des lecteurs externes fixes permettant de lire simultanément la carte Vitale du patient et la CPS de son pharmacien, on parle donc de lecteur bi-fentes.

Par ailleurs, le standard IAS utilisé pour la conception des cartes Vitale 2 et CPS3 doit permettre de disposer d'une offre industrielle interopérable ainsi qu'une normalisation des échanges entre la carte et le terminal. Ce standard permet donc l'utilisation de **lecteurs dits transparents PC/SC** (*Personal computer / Smart card*) qui équipent en standard certains postes de travail ou qui sont disponibles sur le marché sous la forme de périphériques indépendants (12).

Comme nous l'avons vu, l'homologation des interfaces utilisant des lecteurs standards dits PC/SC répond aux exigences du référentiel « accès cartes – interface PC/SC v1.02 ». Il permet aux industriels de développer une solution offrant aux différentes applications de la sphère santé-social (facturation, services en ligne de l'assurance maladie...) un accès sécurisé et éventuellement distant au moyen d'un équipement standard y compris avec des systèmes d'exploitation mobiles telles que les tablettes numériques ou les *smartphones* (35).

⁶⁵ La liste des lecteurs homologués est disponible en ligne sur le site du GIE SESAM-Vitale : <https://www.SESAM-vitale.fr>

Afin de profiter pleinement des fonctions de la CPS3, leurs titulaires peuvent utiliser un lecteur à fente classique ou un lecteur muni de la fonctionnalité dite « sans contact ». Comme nous l'avons vu, les modalités de mise en œuvre de l'interface sans contact peuvent répondre indifféremment à la norme ISO14443 A ou B. Cela implique donc que ces lecteurs doivent être compatibles simultanément avec ces deux normes, le parc de cartes pouvant potentiellement être réparti entre les deux types.

L'usage de la carte dans un lecteur « **avec contact** » consiste à insérer la carte dans la fente du lecteur, puis à saisir éventuellement **un code PIN confidentiel et strictement personnel** (comme celui d'une carte bancaire)⁶⁶. Ce mode d'utilisation permet d'effectuer l'ensemble des opérations de sécurité offertes par la carte.

En mode dit « **sans contact** » avec un lecteur sans contact, certaines fonctions de la carte peuvent être effectuées sans saisie du code confidentiel. Ce mode de fonctionnement simplifie l'usage de la carte dans des contextes moins sécurisés tels que l'accès à des locaux par exemple (36).

A.2.2.3.c Les fournitures logicielles d'interfaçage

Un intergiciel ou *middleware* est un logiciel permettant à plusieurs applications informatiques de communiquer entre elles et permet d'accéder à la carte sur le poste de travail via un lecteur de cartes. Le GIE SESAM-Vitale et l'ASIP Santé mettent ainsi ces interfaces à disposition des éditeurs de logiciels de gestion d'officine afin qu'elles soient intégrées à leurs logiciels.

Les **fournitures SESAM-Vitale** regroupent ainsi l'ensemble des modules logiciels mis à disposition des éditeurs de progiciels par le GIE SESAM-Vitale sur leur plateforme de diffusion en ligne⁶⁷. Parmi ces fournitures on distingue, la **bibliothèque SESAM-Vitale** et le **logiciel lecteur**.

Si certains professionnels mobiles (visiteurs médicaux, infirmières...) utilisent parfois un dispositif de facturation sans ordinateur ou « solution intégrée FSE », les logiciels de gestion d'officine et les lecteurs SESAM-Vitale agréés intègrent également un ensemble de modules développés par le GIE ou **bibliothèque SESAM-Vitale**. Cette bibliothèque regroupe l'ensemble des modules logiciels fournis par l'assurance maladie obligatoire installés sur l'équipement informatique du professionnel de santé afin de lui permettre d'utiliser les fonctions offertes par l'infrastructure SESAM-Vitale pour réaliser et sécuriser l'ensemble des opérations aboutissant à la télétransmission des FSE et des pièces numériques. Il s'agit d'un pack logiciel comprenant (25) :

- **des modules de facturation** regroupant le module **SSV** (services SESAM-Vitale) et le logiciel lecteur pré-installé dans tous les lecteurs homologués. Ils permettent l'accès aux cartes Vitale et CPS pour la création et la sécurisation des factures électroniques ;
- **des modules de tarification : SRT** (services de réglementation et tarification) pour la tarification des prestations et **STS** (services de tarification spécifiques) pour la part complémentaire ;
- **le GALSS** (gestionnaire d'accès au lecteur santé social) chargé de gérer la communication entre le lecteur et le logiciel de gestion d'officine.

⁶⁶ Au moyen d'un clavier numérique de saisie du code porteur de la carte CPS ou PIN Pad.

⁶⁷ <https://diffusion.SESAM-vitale.fr>

Le logiciel lecteur SESAM-Vitale (dernière version EI96S v03.x) permet de lire toute carte compatible avec la norme ISO 7816 selon deux modes (25) :

- un mode « transparent » dans lequel les données ne sont pas traitées ;
- un mode « intelligent » dans lequel les données sont traitées par une application implantée dans le lecteur.

Les cartes Vitale portant un numéro de série long fabriquée à partir de juin 2012 ne seront pas lues correctement si la version du logiciel lecteur n'est pas à jour. C'est pourquoi les professionnels de santé n'étant pas équipés de la dernière version de lecteurs (version 3.X)⁶⁸ doivent procéder à une mise à jour du logiciel lecteur. Les risques potentiels d'une absence de mise à jour sont (37):

- le rejet de FSE émises avec un numéro de série erroné ;
- l'élaboration d'une FSE avec une carte réellement en opposition, mais non détectée comme telle;
- l'impossibilité de faire une FSE avec une carte correcte, mais considérée à tort comme étant en opposition.

Si le référentiel d'homologation « terminal lecteur » est classé confidentiel, le cahier des charges SESAM-Vitale permet de comprendre que le lecteur est capable d'assumer des fonctions de chiffrement de certaines données sensibles des factures électroniques. En effet, les organismes d'assurance maladie complémentaires ne doivent pas avoir connaissance des informations relatives au codage (codes affinés, codes signifiants de la classification commune des actes médicaux, codes CIP...). Pour cela, le logiciel lecteur utilise des techniques de cryptographie symétrique : 3DES en mode CBC (clé de session de 128 bits) comme nous le verrons par la suite.

L'API de lecture Vitale constitue un module logiciel offrant des fonctions de lecture de la carte Vitale. Son utilisation doit permettre à tous les acteurs du monde de la santé d'accéder aux données de la carte tout en garantissant la qualité des outils développés ainsi que la fiabilité de la lecture des données inscrites en carte. Cette API n'a pas vocation à être incluse dans les progiciels de facturation (25).

La carte CPS3 sollicite deux versions de middleware selon les modalités d'utilisation de la carte. Pour l'accès au travers du canal CPS2ter, le middleware utilisé avec les cartes CPS3 emploie la Cryptolib-CPS et l'API-CPS.

Les modalités d'accès au travers du canal IAS ECC s'appuient sur le schéma d'homologation de l'Agence nationale des titres sécurisés qui repose notamment sur l'utilisation d'un middleware commun (le middleware IAS) assurant l'interopérabilité avec les cartes issues de différents fournisseurs. C'est donc ce middleware qui doit être préférentiellement utilisé pour exploiter les fonctionnalités IAS ECC de la carte CPS3.

Quel que soit le middleware utilisé, il permet l'interfaçage entre la carte et les logiciels du professionnel de santé tels les logiciels de gestion d'officine afin d'en acquérir les données ou encore d'accéder aux fonctions de sécurité proposées par la carte.

⁶⁸ 95% des professionnels de santé étaient équipés de lecteurs en version 3.0 fin 2011 (27).

A.2.2.3.d Les bornes de mise à jour des cartes Vitale

Alors que l'actualisation des données de la carte CPS passe par un renouvellement de la carte auprès de l'ASIP Santé (38), les titulaires d'une carte Vitale doivent en effectuer une mise à jour annuelle sous peine de ne pouvoir bénéficier de la dispense d'avance de ses frais médicaux. Cette mise à jour est également nécessaire en cas de changement de situation, l'assuré dispose alors d'un mois pour effectuer la mise à jour, après information par la caisse, de la prise en compte de son changement de situation. A défaut de mise à jour, la carte est temporairement inutilisable⁶⁹. 66 millions de mises à jour en ligne des données des cartes Vitale ont été réalisées en 2012 grâce aux 41 350 bornes en libre accès dans la plupart des pharmacies, certains cabinets médicaux, établissements de santé, centres de soins, mutuelles, maisons de retraite ou lieux publics comme les mairies (39).

Cette mise à jour, en particulier pour ce qui concerne la validité des droits ou l'ouverture du droit à une exonération du ticket modérateur, est de la seule responsabilité des caisses et des assurés. Dès lors qu'il s'est équipé d'une borne de télé mise à jour, le pharmacien incite l'assuré à mettre à jour sa carte. A la suite de l'opération de mise à jour, la consultation des données de la carte est possible (40).

Ce service est accessible par un matériel homologué conformément au référentiel d'homologation « télé-mise-à-jour v3.10 » du GIE SESAM-Vitale et une connexion à un service de télécommunication adapté⁷⁰ puisqu'il s'agit de télécharger les nouvelles données via le réseau SESAM-Vitale. Le matériel de mise à jour est implanté exclusivement dans l'officine en libre accès à tout assuré social, et ne peut faire l'objet de publicité à but commercial. Le pharmacien loue le matériel de télé mise à jour dont il a le libre choix parmi les solutions homologuées par le GIE. Les caisses accordent une participation financière sous la forme d'un montant annuel couvrant le coût du service, la maintenance de l'équipement et les frais de communication téléphonique. Cette participation d'un montant de 382,72 € TTC est versée par la caisse primaire pour le compte de l'ensemble des régimes. Une seule participation par officine peut être versée (40).

A.2.2.4 LA NUMERISATION DES PIECES JUSTIFICATIVES

Le projet de numérisation de pièces justificatives par les professionnels de santé fut initié par la Caisse nationale d'assurance maladie en collaboration avec les ordres de professionnels de santé en 2011. L'objectif avoué de cette mesure de dématérialisation des documents relatifs aux patients consiste en une simplification de certaines tâches administratives afin de gagner en efficience et valoriser le temps « médical »⁷¹ ainsi accru, accordé à chaque patient, tout en facilitant le traitement des dossiers par l'assurance maladie. Comme bien souvent en matière de dématérialisation au sein des systèmes d'information de santé, les pharmaciens se sont retrouvés en première ligne et ont débuté la numérisation des ordonnances de leurs patients au cours de chaque dispensation.

L'avenant conventionnel n°3 de la convention pharmaceutique a ainsi permis de franchir une étape décisive en généralisant la dématérialisation des ordonnances à toutes les pharmacies françaises. Initié en 2011, ce projet intitulé **SCOR** est généralisé à l'ensemble du territoire

⁶⁹ Article R.161-33-6 du code de la sécurité sociale.

⁷⁰ La liste des solutions de télé-mise à jour homologuées est disponible sur le site du GIE SESAM-Vitale à l'adresse : <http://www.SESAM-vitale.fr>

⁷¹ Dans son point d'information du 1^{er} décembre 2011, la Caisse nationale d'assurance maladie évoque le temps « médical » afin de désigner le temps « pharmaceutique » alloué à chaque patient lors d'une dispensation.

depuis le 15 janvier 2013⁷². Dans l'attente de la généralisation de leur télétransmission, les ordonnances numérisées sont gravées sur CD-ROM puis transmises aux organismes d'assurance maladie par voie postale.

A.2.2.4.a Champs d'application

Si les pharmaciens ne sont pas les seuls professionnels de santé impliqués dans cette démarche, ils sont cependant au cœur du projet puisqu'il s'agit de la profession sur laquelle l'impact est le plus retentissant. Le cahier des charges relatif à la numérisation et télétransmission des pièces justificatives prévoit ainsi que les pharmaciens, les responsables de laboratoires d'analyses biologiques et médicales (LABM), les masseurs-kinésithérapeutes (MK), les infirmiers et les fournisseurs de produits de santé puissent bénéficier des fonctions de dématérialisation des pièces justificatives (41).

	Pharmaciens	LABM	MK	Infirmiers	Fournisseurs
Ordonnance normale	X	X	X	X	X
Ordonnance d'exception	X				
Feuille de soins papier (modèle CERFA sans trame)	S 3115f	S 3131	S 3129	S 3129	S 3115
Feuille de soins papier d'exception	X				
Ticket Vitale (numérisé ou reconstitué)	X				
Coupons de prévention (ex : vaccination antigrippale)	X				
Démarches de soins infirmiers prescription				S 3740	
Démarche de soins infirmiers résumé				S 3742	
Autres pièces jointes	X	X	X	X	X

Tableau 4 : Types de pièces justificatives numérisées par profession de santé (41).

La convention pharmaceutique définit la "**pièce numérique**" comme la copie numérique fidèle et durable (40) :

- **de l'ordonnance originale sur support papier**, portant les mentions obligatoires du « ticket vitale ». Comme nous l'avons vu, le ticket vitale correspond aux informations reproduites **sur l'original de l'ordonnance** permettant « *de garantir aux assurés sociaux une bonne information sur le coût des produits de santé qui leur sont délivrés* ». Son rôle ne s'arrête cependant pas là puisqu'il concerne également les informations reproduites **sur le duplicata de l'ordonnance** permettant « *aux caisses d'effectuer le rapprochement avec la feuille de soins nécessaire au règlement des produits de santé* ».

Parallèlement à la télétransmission, des FSE, le pharmacien devait jusqu'alors imprimer les informations relatives à la facturation nécessaires aux caisses d'assurance maladie sur le duplicata de l'ordonnance. Les duplicatas étaient ensuite triés et classés puis transmis aux

⁷² Décision du 15 janvier 2013 portant sur la généralisation et l'extension de la télétransmission des pièces justificatives de la facturation (SCOR).

caisses par voie postale avec un bordereau. En numérisant l'ordonnance originale, il est donc désormais possible de s'affranchir de l'envoi postal de ces duplicatas papier, remplacé par la télétransmission de l'image de l'ordonnance associée aux données de facturation correspondantes.

- **de la feuille de soins sur support papier** établie sur le modèle "cerfatisé" en vigueur et signé par l'assuré en cas d'impossibilité de produire des FSE du fait de l'absence, de la non-présentation ou de la défectuosité de la carte Vitale du patient.

Le tableau ci-dessous présente les différents types de pièces numériques transmises par les pharmaciens selon le mode de sécurisation de la télétransmission. Dans le cadre d'un renouvellement d'une prescription pour laquelle le professionnel de santé a déjà télétransmis les pièces justificatives, il peut se passer de les numériser de nouveau mais doit transmettre l'identifiant de chaque pièce transmise et ayant fait l'objet d'un accusé de réception positif.

	Flux de facturation sécurisé CD-ROM/télétransmission	Flux de facturation dégradé CD-ROM/télétransmission
Ordonnance « simple »	Ordonnance papier scannée avec ticket Vitale	Ordonnance et CERFA 3115f ⁷³ (modèle numérique sans trame)
Ordonnance d'exception	Volet 4 de l'ordonnance scanné avec ticket Vitale	Volet 4 de l'ordonnance scanné et CERFA 3115f
Ordonnance bizonne	Ordonnance papier scannée avec ticket Vitale	Ordonnance papier scannée et CERFA 3115f
En cas de renouvellement	Pas de copie numérique de l'ordonnance si elle a déjà été délivrée une première fois mais présence sur le ticket Vitale de l'identification de la prescription initiale	CERFA 3115f. Pas de copie numérique de l'ordonnance si elle a déjà été délivrée une première fois mais présence sur le ticket Vitale de l'identification de la prescription initiale

Tableau 5 : Types de pièces numériques transmises selon le mode de sécurisation des flux de facturation (40).

A.2.2.4.b Contraintes techniques

De même valeur juridique et comptable que les pièces justificatives sur support papier, les pièces justificatives numériques ouvrent donc droit à la prise en charge totale ou partielle de dépenses en produits de santé. Le pharmacien est responsable de l'établissement de la pièce numérique et de sa fidélité à la version papier au moment où il établit la facturation. La qualité de numérisation permettant d'atteindre un taux d'exploitabilité suffisant est évalué par l'assurance maladie pendant un délai de 90 jours à compter de la réception des premières pièces justificatives numériques (40).

Afin de garantir une reproduction numérique rapide et fidèle de l'ordonnance, les pharmaciens ont dû enrichir leur système informatique d'un scanner. La vitesse de numérisation (nombre de pages susceptibles d'être numérisées par minute) est variable d'un

⁷³ Le modèle CERFA 3115f sans trame ne peut être utilisé que pour les FSE en mode dégradé et ne peut en aucun cas être utilisé dans la procédure papier.

appareil à l'autre. Elle dépend à la fois de la puissance des capteurs, du format du document original et de la résolution de la capture de l'image mesurée en ppp (points par pouces). Les pharmaciens doivent donc veiller à configurer leurs scanners de façon à trouver un bon compromis entre rapidité et qualité de numérisation (41).

Le pharmacien est responsable de l'établissement de la pièce numérique et de sa fidélité à la version papier au moment où il établit la facturation. Il numérise donc chaque ordonnance à l'aide de son scanner et l'image est enregistrée sous forme d'un fichier PDF. Même si les scanners actuellement disponibles dans le commerce ont largement les capacités techniques pour permettre une numérisation de qualité, le logiciel du professionnel de santé procède à un contrôle de la taille du fichier de pièces justificatives généré au format PDF et de la qualité de la numérisation.

Le volume du fichier généré lors de la numérisation des pièces justificatives ne doit ainsi pas dépasser 250 Ko et les volumes des images générés doivent être dans les ordres de grandeur suivant (41) :

- Ordonnance (1 page) + ticket Vitale : environ 50 à 70 Ko ;
- Ordonnance (1 page) + CERFA (1 page) : environ 80 à 100 Ko ;
- CERFA (1 page) : environ 50 Ko.

Le fichier au format Adobe PDF/A-1 ainsi constitué doit contenir une image à taille réelle (sans réduction ni agrandissement) d'une définition de 200 ppp (au moins 150 ppp) en noir et blanc (et non pas en niveau de gris).

A.2.3. L'IDENTIFICATION DES PERSONNES ET DE L'OFFICINE

Afin d'échanger et partager en toute confiance, tout système de traitement automatisé de données personnelles doit permettre une identification efficace des différents partenaires intervenants dans ce processus. Identifier chacun en tant que structure, professionnel mais encore comme patient et/ou bénéficiaire de l'assurance maladie est donc devenu incontournable afin de tisser la toile des systèmes informatisés de santé.

A.2.3.1 L'IDENTIFICATION DE L'OFFICINE

Comme tout établissement de santé chaque officine doit être enregistrée auprès du fichier national d'enregistrement des établissements sanitaires et sociaux (FINESS⁷⁴) qui lui attribue deux numéros :

- Le numéro FINESS juridique utilisé pour l'élaboration des feuilles de soins électroniques et transmis aux organismes d'assurance maladie ;
- Le numéro FINESS géographique qui identifie l'officine d'un point de vue physique, est notamment utilisé pour identifier l'officine vis-à-vis du serveur hébergeant le dossier pharmaceutique.

⁷⁴ Ministère des affaires sociales et de la santé – DREES - <http://finess.sante.gouv.fr/>

A.2.3.2 L'IDENTIFICATION DES PROFESSIONNELS DE SANTE

Lors de l'inscription d'un professionnel de santé à l'ordre régissant sa profession, il fournit un ensemble d'informations personnelles attestant de son identité et de sa légitimité d'exercice de la profession dont (42) :

- Des données d'état civil : nom, prénom, date et lieu de naissance, sexe, nationalité ;
- Les coordonnées de correspondance : adresse postale, numéro de téléphone, adresse e-mail ;
- Les diplômes et compétences : numéro, date d'obtention, intitulé du diplôme, ainsi que le lieu de délivrance et le nom sous lequel le diplôme a été attribué et l'exercice de pratiques particulières (expert auprès des tribunaux ou des assurances par exemple) ;
- Les compétences linguistiques du professionnel de santé en français et en langues étrangères ;
- Les expériences professionnelles officinales (durées, nom et adresse de l'officine) ;
- Le lieu d'exercice : nom, adresses postale et électronique, numéros de téléphone et de télécopie, le numéro SIRET et la forme juridique de l'entreprise ;
- Les informations relatives à l'exercice d'autres activités pharmaceutiques (gérance de pharmacie à usage intérieur, dispensation de gaz à usage médical...) ;
- La signature manuscrite du professionnel de santé.

Les informations recueillies dans ce formulaire d'inscription font l'objet d'un traitement automatisé par l'ordre et sont destinées notamment au ministère de la santé, aux agences régionales de santé, aux caisses d'assurance maladie et à l'ASIP Santé pour l'établissement du répertoire partagé de santé (RPPS) *« dans un but de simplification des démarches administratives. Elles permettent notamment l'établissement de statistiques démographiques, la fabrication des cartes de professionnel de santé (CPS) et le traitement des adhésions aux conventions nationales de sécurité sociale »* (42).

A.2.3.2.a Le répertoire partagé des professionnels de santé

L'arrêté du 6 février 2009 portant sur la création d'un traitement de données à caractère personnel dénommé RPPS couplé à l'avis de la CNIL du 27 mars 2008 autorise la création de ce répertoire voué à remplacer progressivement l'ancien système ADELI (automatisation des listes) identifiant les professionnels de santé. Le RPPS est une base de données relative aux professionnels de santé hébergée et gérée par l'ASIP Santé dont l'INSEE, les ordres et le service de santé des armées en certifient le contenu. L'Agence exploite ainsi les données fournies par le professionnel de santé à l'ordre lors de son inscription afin de constituer ce répertoire d'identification et leur fournir une carte de professionnel de santé⁷⁵.

⁷⁵ Une déclaration préalable d'activité libérale auprès de l'assurance maladie est nécessaire pour l'obtention de la carte CPS.

Les données contenues dans le RPPS telles qu'elles sont décrites par l'article 2 de cet arrêté concernent :

- Les données d'identification du professionnel de santé : numéro RPPS, noms de famille et d'usage, prénoms, date et lieu de naissance, date de décès, nationalité actuelle, date d'acquisition de cette nationalité ;
- Les diplômes, attestations et autorisations liés à l'exercice de la profession : intitulé, date d'obtention, lieu de formation, autorité de délivrance, numéro...
- Les données d'exercice de la profession : intitulé de la profession, identité d'exercice, inscription à l'ordre, coordonnées de correspondance, dates de début et de fin des périodes pendant lesquelles le professionnel fait l'objet d'une mesure de suspension ou d'interdiction d'exercice, langues étrangères pouvant être utilisées dans le cadre de l'exercice professionnel ;
- Les qualifications, titres et exercices particuliers : intitulé, date de reconnaissance, date d'abandon ;
- Des informations relatives aux activités et aux structures d'exercice :
 - o genre d'activité, date de début et de fin de l'activité, motif de cessation d'activité ;
 - o mode d'exercice, fonction, type d'activité libérale, spécialités de concours et autres attributions, catégorie de professionnel de santé, coordonnées du professionnel de santé dans son lieu d'exercice ;
 - o structure d'exercice ou d'emploi : numéro SIRET ou FINESS, coordonnées, activité, secteur d'activité santé, catégorie juridique.
- Des informations sur la carte CPS : type de carte, numéro, période de validité, date d'opposition ;
- Des informations complémentaires contenues dans le répertoire : un annuaire des personnes habilitées à accéder au traitement, les nomenclatures nécessaires à la tenue du répertoire, des identifiants techniques, des dates liées à la gestion des historiques.

Ces données sont conservées « *jusqu'au centième anniversaire du professionnel, si ce délai est compatible avec la condition d'une durée minimale de trente ans à compter de la date de fin de capacité d'exercice, dans le cas contraire, jusqu'au trentième anniversaire de sa fin de capacité d'exercice* » (article 4).

Si chaque professionnel de santé a accès à la totalité de ses propres informations, l'ensemble des données du RPPS n'est consultable que par un cercle de personnes habilitées défini par l'article 7 de l'arrêté⁷⁶.

⁷⁶ Les services du ministère de la santé et certains services de l'Etat, les ordres des médecins, chirurgiens-dentistes, sages-femmes et pharmaciens, la CNAMTS, l'ASIP Santé, les hébergeurs de données et imprimeurs d'ordonnances, les organismes d'AMO, d'AMC...

Afin de répondre à la mission de mise à disposition de ces informations au grand public, l'ASIP Santé publie néanmoins certaines données du RPPS via un service de communication électronique accessible après envoi et validation d'une fiche de demande d'accès (par voie électronique ou postale). Le périmètre de ces informations est cependant restreint, il s'agit du numéro RPPS, des noms et prénoms d'exercice, de la profession exercée, des qualifications et titres professionnels correspondant à l'activité exercée et des coordonnées des structures d'exercice (raison sociale, adresse département, région numéro de téléphone (43)).

Enfin, « **l'annuaire du GIP-CPS** »⁷⁷ met également à disposition du grand public les informations relatives à leurs certificats électroniques d'authentification et de signature, utiles aux utilisateurs pour le déchiffrement et la vérification des signatures électroniques des professionnels de santé.

A.2.3.2.b Le référentiel des acteurs santé sociaux

Lancé en 2012, le RASS constitue le vecteur de publication du RPPS. Il met l'ensemble des données de description des professionnels de santé à disposition des utilisateurs autorisés, dans le respect des règles définies par l'arrêté RPPS, et permet également d'accéder aux données d'identification des établissements dans lesquels ils exercent (répertoire FINESS).

Concrètement, il s'agit de *Web-services* de consultation de données relatives aux personnes physiques et morales accessible par les professionnels de santé munis d'une autorisation d'accès au RPPS et d'une carte CPS garantissant son authentification forte auprès du serveur.

En valorisant les données pour différents usages (information du grand public, efficience des échanges dématérialisés, pilotage de l'offre de soin...), le RASS a vocation à devenir le socle d'urbanisation des systèmes d'information du système de santé en se substituant progressivement à l'ensemble des annuaires existants.

A.2.3.3 L'IDENTIFICATION DES PATIENTS

Afin d'associer les données de santé d'un patient au bon dossier, il est primordial de pouvoir l'identifier sans ambiguïté. L'attribution aux patients d'identifiants de santé différents dans chaque système intervenant dans leur prise en charge constituait un frein au développement du partage et de l'échange de données de santé et représentait un risque pour le patient à qui serait attribué à tort, des données mal identifiées.

Jugé trop significatif, le traditionnel numéro de sécurité sociale (NIR) utilisé par les professionnels de santé à des fins de facturation ne peut être utilisé comme identifiant national de santé. En effet, la CNIL estime qu'un identifiant de santé spécifique, non significatif, pouvait être généré à partir du NIR de la personne selon des techniques reconnues d'anonymisation.

Depuis juin 2010, un identifiant national de santé (INS) est ainsi attribué à chaque bénéficiaire de l'assurance maladie tout au long de sa vie. Il n'est ni public, ni secret, il s'agit d'une donnée personnelle protégée par la loi informatique et libertés au même titre que le nom ou le prénom (3). Comme nous le verrons, un numéro de dossier pharmaceutique (NDP) permet par ailleurs, d'associer un dossier pharmaceutique au bon patient.

⁷⁷ Disponible à l'adresse suivante : <http://annuaire.gip-cps.fr/>

A.2.3.3.a Le numéro d'inscription au répertoire des personnes physiques

Le NIR ou numéro d'inscription au répertoire national d'identification des personnes physiques (RNIPP), plus communément appelé numéro de sécurité sociale, permet l'identification des personnes inscrites au répertoire. Ce numéro composé de treize chiffres (plus une clé de contrôle de 2 chiffres) est attribué à chaque français dès sa naissance. Il se compose de sept champs de valeurs numériques assemblées de la manière suivante (15) :

Sexe	Année de naissance	Mois de naissance	Département de naissance	N° de commune ou pays de naissance	N° d'acte de naissance	Clé de contrôle ⁷⁸
1 : homme 2 : femme	00 à 99	01 à 12	01 à 95 : métropole 970 à 989 : outre-mer 99 : étranger	001 à 990	001 à 999	01 à 97

Tableau 6 : Structure du numéro d'inscription au répertoire des personnes physiques.

Si les caractéristiques du NIR garantissent une identification fiable⁷⁹, unique et pérenne de chaque individu inscrit au répertoire (un seul numéro est attribué à chaque individu tout au long de sa vie), il est cependant **signifiant**. En effet, il est possible de déduire le sexe, le mois, l'année, le département et la commune de naissance en France ou l'indication d'une naissance à l'étranger par simple lecture de la suite de chiffres. La loi informatique et libertés soumet donc à autorisation l'utilisation de ce numéro qui fut utilisé, dès son origine, dans le secteur de la sécurité sociale. La CNIL a donc admis qu'il soit enregistré dans l'ensemble des fichiers des professionnels et organismes en relation avec le système de santé tels que (15):

- les acteurs du système de protection sociale ;
- les employeurs ;
- le pôle emploi pour le paiement des cotisations sociales des chômeurs et le maintien de leurs droits sociaux ;
- les organismes d'assurance maladie obligatoires et complémentaires ;
- les professionnels et les établissements de santé pour permettre la prise en charge totale ou partielle des frais de maladie...

Le décret du 12 septembre 1996 relatif à l'autorisation d'utilisation du NIRPP et à l'institution d'un répertoire national inter-régimes des bénéficiaires de l'assurance maladie autorise les professionnels de santé à utiliser le NIR dans le cadre de leurs relations avec la sécurité sociale à des fins de facturation. Ils ne sont cependant pas autorisés à utiliser ce numéro comme identifiant du dossier médical du patient. En effet, dans une recommandation du 20 février 2007 (44) prise à l'issue d'une série d'auditions, la CNIL a exclu l'utilisation du NIR comme identifiant de santé.

⁷⁸ Il s'agit du complément à 97 du reste de la division du numéro à 13 chiffres (NIR) par 97. Pour la calculer, il faut le nombre formé par les 13 premiers chiffres du NIR et le diviser par 97. La clé correspond à la différence (soustraction) entre 97 et le reste de cette division.

⁷⁹ Le NIR est certifié par l'INSEE à partir des données d'état civil transmises par les mairies.

A.2.3.3.b Le numéro d'adhérent à un organisme complémentaire

Si le NIR doit être employé uniquement à des fins de facturation de prestation ou produits de santé, il n'est pas suffisant pour permettre la facturation d'une éventuelle part à un organisme d'assurance maladie complémentaire (AMC). Les patients bénéficiant d'une mutuelle sont identifiés dans leurs systèmes au moyen d'un numéro d'adhérent unique ou partagé avec d'éventuels ayants-droits. Chaque numéro d'adhérent est ainsi associé au contrat souscrit par l'assuré précisant ses modalités de prise en charge.

Si la traditionnelle carte de mutuelle en papier constitue le support de droits AMC le plus répandu, l'inclusion de ces informations dans une carte à puce électronique fournie par la mutuelle ou encore, dans la carte Vitale pour certains régimes (MGEN, MGPTT, MGP, CMU-C...), facilite grandement le travail des professionnels de santé. En effet, en automatisant l'acquisition de ces données administratives, les pharmaciens ne perdent plus de temps à déchiffrer les cartes de mutuelles d'aspects hétérogènes et dont le contenu n'est pas parfaitement normalisé. Ce gain de temps et de concentration au bénéfice du patient, constitue un parfait exemple des bénéfices attendus de la dématérialisation des données et particulièrement administratives, au sein des systèmes d'information de santé.

A.2.3.3.c L'identifiant national de santé

L'identifiant national de santé (INS) introduit par la loi n° 2007-127 du 30 janvier 2007 est un identifiant unique attribué à chaque bénéficiaire de l'assurance maladie « *à des fins de coordination et de qualité des soins, pour la conservation, l'hébergement et la transmission des informations de santé ainsi que pour l'ouverture et la tenue du DMP* »⁸⁰. Son rôle est d'associer sans ambiguïté les données de santé d'un patient au bon dossier en limitant les risques de doublons⁸¹ et de collisions⁸² d'identités.

En application de l'avis de la CNIL du 20 février 2007, **l'INS est une donnée personnelle mais qui n'est pas une donnée de santé**. Il s'agit d'une donnée administrative qui constitue un moyen d'identito-vigilance ne donnant aucune information sur la santé de la personne et n'est donc pas soumis aux règles spécifiques des données de santé. Cela implique que l'INS n'est pas soumis aux dispositions du décret de confidentialité de 2007 qui, comme nous l'avons vu précédemment, rend l'usage de la carte CPS obligatoire. Il peut être diffusé à d'autres personnes que des professionnels de santé impliqués dans la prise en charge du patient. Le consentement exprès du patient n'est pas requis pour l'obtenir mais il garde cependant son droit d'opposition à l'utilisation de l'INS.

Il s'agit enfin d'une donnée sensible⁸³ dont l'utilisation en dehors des finalités prévues par l'article L.1111-8-1 du code de la santé publique peut faire l'objet de sanctions pénales (cinq ans d'emprisonnement et de 300 000 euros d'amende)⁸⁴. L'INS est donc une donnée personnelle strictement privée mais non confidentielle (45).

⁸⁰ Article L.1111-8-1 du code de la santé publique.

⁸¹ Doublon : une même personne se voit attribuer plusieurs INS-C.

⁸² Collision : un même INS-C est attribué à plus d'une personne.

⁸³ Le groupe de travail instauré par l'article 29 de la directive 95/46/CE confirme le caractère sensible d'un identifiant dédié à la santé dans son avis du 15 février 2007.

⁸⁴ Par l'article 226-16 du code pénal.

Les caractéristiques de l'INS doivent en faire un identifiant (46):

- **unique et durable** : un seul INS est attribué par assuré et il est valable tout au long de sa vie ;

- **fiable** : il est généré à partir du NIR ;

- **non significatif** : sa connaissance ne doit pas permettre de déduire des informations personnelles ;

- **non prédictible** : la connaissance du NIR ou des traits d'identité de la personne ne permettent pas la déduction de l'INS. De même, la connaissance de l'INS ne doit pas permettre de remonter au NIR de la personne.

La mise en œuvre de l'identifiant national de santé est prévue en deux étapes successives : un INS calculé (INS-C) actuellement utilisé, puis un INS aléatoire (INS-A) en cours d'élaboration.

- **L'INS-C** est un identifiant transitoire permettant d'ores et déjà l'identification des patients et facilite ainsi le déploiement d'échanges ou le partage de données de santé dans le cadre de projets régionaux ou nationaux. L'INS-C est composé de 20 chiffres et de 2 chiffres correspondant au code de détection d'erreur.

Il est calculé par le logiciel du professionnel de santé ou de tout système d'information de santé (établissement de santé, réseau, ...) à partir d'informations lues dans la carte Vitale du patient (NIR, prénom et date de naissance) auxquelles un algorithme de calcul est appliqué⁸⁵. L'ASIP Santé a élaboré et publié le référentiel d'identification des patients – volet INS-C, contenant le dossier de conception de l'INS-C ainsi que les spécifications de l'algorithme de calcul, téléchargeable à partir du site de l'ASIP Santé.

Les objectifs affichés de l'INS-C sont les suivants (45):

- **une intégration aisée** dans les outils des professionnels de santé : comme nous le verrons, l'algorithme de hachage SHA-256 étant public, les implémentations sont donc disponibles et facilement intégrables ;

- **faire de l'INS-C un identifiant non significatif** : le résultat de la fonction de hachage (empreinte) étant insignifiant par nature ;

- **pouvoir attribuer un INS-C à un maximum de personnes** : les traits nécessaires au calcul de l'INS-C ne peuvent l'être qu'avec des cartes disposant d'une zone *mapping* en version 1ter à minima (annexe 4). Avec la généralisation des cartes Vitales 2 actuelles, la quasi-totalité des assurés peuvent donc aujourd'hui bénéficier d'un INS-C ;

- **présenter un faible taux de doublons** liés à la modification des traits utilisés pour le calcul de l'INS-C. Ainsi en cas de modification ou correction des champs « prénom », « NIR » et « date de naissance », un assuré peut se voir attribuer un nouvel INS-C. Le choix de ces traits n'est donc pas le fruit du hasard puisqu'il s'agit de valeurs peu susceptibles de

⁸⁵ L'algorithme de hachage SHA-2 (256 bits).

changer dans le temps contrairement au nom d'usage⁸⁶ ou au numéro de série de la carte Vitale. En effet, ce dernier n'a pas été retenu dans le calcul de l'INS-C puisqu'il change si la carte est renouvelée mais également car un ayant-droit inscrit dans plusieurs cartes Vitale se verrait attribuer autant d'INS-C que de cartes sur lesquelles il figure. C'est notamment le cas des 12,5 millions de mineurs de moins de seize ans et des familles nombreuses.

- **présenter une faible probabilité de collisions** évaluée par l'ASIP Santé à 0,024 % pour un INS-C de 20 chiffres après génération de 66 millions d'INS-C. Elle est de 0,046 % pour 137 millions d'INS-C.

L'INS-C du patient peut être conservé dans le logiciel et peut également être transmis à un autre professionnel qui n'est pas en contact direct avec le patient comme par exemple, un laboratoire d'analyse (45).

Le calcul de l'INS-C d'un bénéficiaire de l'assurance maladie est conditionné par la capacité d'un logiciel à lire les données du bénéficiaire à partir de la carte Vitale : champs NIR individuel, champ prénom et champ date de naissance. Seuls les logiciels agréés SESAM-Vitale (cahier des charges en version 1.40 *a minima*), solutions intégrées homologuées SESAM-Vitale (référentiel V3.x *a minima*) et logiciels référencés comme intégrant le composant API de lecture Vitale, permettent la lecture systématique de ces champs (Cf. annexe 4).

- **L'INS-A**, non disponible actuellement, serait généré aléatoirement et attribué par un système central dès la création du NIR. Le terme aléatoire signifie qu'il n'y a pas de lien mathématique ou algorithmique entre les données concernant un patient et son INS-A. Il serait accessible via un télé-service national aux professionnels de santé et aux établissements après lecture de la carte Vitale du patient. Il serait composé de 10 chiffres aléatoires attribués par le système central de gestion des INS-A et de 2 chiffres correspondant au code de détection d'erreur (15).

Dans l'attente de l'utilisation de l'INS-A, il est nécessaire de considérer certains risques liés à l'identification des patients au moyen de l'INS-C :

- **Le risque de doublons** est lié à une modification des valeurs des champs « prénom », « NIR » et « date de naissance » acquises à partir de la carte Vitale. Si l'on peut imaginer que les cas d'une demande de modification du prénom ou de la date de naissance inscrits dans une carte Vitale restent marginaux, environ trente mille modifications de NIR sur les cent millions de NIR du répertoire sont effectuées chaque année.

En cas de doublon, une personne se voit attribuer plusieurs INS-C et donc potentiellement plusieurs dossiers médicaux, le professionnel de santé ayant alors accès à une vue partielle des données de santé de son patient en cas de difficulté de rapprochement.

- **Le risque de collisions** d'INS-C à 20 chiffres est extrêmement faible (estimé, comme nous l'avons vu, à 0,024% pour 68 millions d'INS-C en circulation). Un même INS-C est alors référencé avec les données de santé de deux personnes différentes.

⁸⁶ Le nom de famille (patronymique) n'a pas été retenu car il n'est disponible dans la carte vitale que pour le porteur de la carte.

Les conséquences d'une collision peuvent être de nature différente selon l'usage qui est fait de l'INS-C :

- Le rapprochement d'informations de santé de deux personnes différentes si le seul critère utilisé est l'INS-C ;
- L'attribution d'informations de santé incorrectes dans le mauvais dossier si l'usage de l'INS-C n'est pas complété par un contrôle d'identito-vigilance (cohérence du nom, cohérence du contenu du dossier, ...).

• **Les risques liés à l'algorithme de calcul** sont dus au caractère public de l'algorithme SHA-256 et de l'absence d'éléments aléatoires dans le calcul de l'INS-C. En effet, afin de donner le même résultat dans tous les systèmes utilisés, l'INS-C est par nature prévisible. Le caractère public de l'algorithme SHA-256 fait de l'INS-C une donnée privée et non une donnée secrète. Les spécifications relatives à l'algorithme de calcul de l'INS-C s'appuyant sur les travaux de l'Agence nationale de sécurité des systèmes d'information, sont disponibles dans le dossier de conception de l'INS-C disponible sur le site de l'ASIP Santé.

Le processus d'élaboration de l'INS-C est donc le suivant (47) (48) :

- Lecture et acquisition des valeurs des champs « prénom », « date de naissance », « NIR » de la carte Vitale et normalisation des données (caractères, champs) ;
- Association sans séparateur des trois champs dans l'ordre suivant : prénom, date de naissance, NIR, l'ensemble constituant « la graine » ;
- Calcul de l'empreinte de 256 bits de la chaîne de caractères de la « graine » au moyen de la fonction de hachage SHA-256 conformément au référentiel général de sécurité ;
- Conversion de l'empreinte au format numérique en base 10 (chiffres de 0 à 9) permettant d'obtenir une chaîne de 20 chiffres ;
- Calcul de l'INS-C en associant la chaîne de 20 chiffres obtenue à une clé de contrôle de 2 chiffres calculée selon les mêmes modalités que celle du NIR (méthode du complément à 97).

Comme nous le verrons, l'algorithme de hachage (SHA-256) appliqué à la « graine » n'est pas réversible et il est *a priori* impossible de remonter à cette « graine » d'informations à partir de l'empreinte générée. Cependant, l'élaboration d'une table de correspondance entre les triplets (NIR, prénom, date de naissance) et l'INS-C en appliquant l'algorithme à toutes les valeurs possibles du triplet pourrait permettre d'en révéler le secret. L'élaboration d'une telle table solliciterait cependant des moyens colossaux permettant de stocker les 9000 To de données nécessaires. Un ordinateur de bureau classique mettrait ainsi 89 ans à élaborer une telle table. L'intérêt de la mise en œuvre de tels moyens ne présente *a priori* aucun intérêt puisque le calcul de l'INS-C ne tient pas compte du nom de famille de la personne concernée (45).

• **L'utilisation frauduleuse d'une carte** appartenant à un tiers pourrait lui permettre d'accéder à des prestations de santé ou prendre connaissance d'informations confidentielles à son sujet. En effet, en l'absence d'authentification du porteur d'une carte Vitale par saisie d'un code, il est parfois difficile pour les professionnels de santé de vérifier l'identité du porteur d'une carte Vitale sur la base de la seule photographie.

	NIR	INS-C	INS-A
Taux de collisions	Nul	Extrêmement faible Moins de 0.06% de risque de trouver 1 collision parmi 100 millions d'INS-C	Nul
Taux de doublons	Nul	Très faible Uniquement lié aux changements de traits d'Etat Civil (NIR, prénoms, date de naissance)	Nul
Signifiant	Oui	Oui	Non
Prévisible	Oui	Oui	Non
Saisissable	Oui	Oui Saisie difficile en raison de la taille de 22 caractères au total.	Oui

Tableau 7 : Comparaison des caractéristiques du NIR, de l'INS-C et de l'INS-A (45).

A.2.3.3.d Le numéro de dossier pharmaceutique

Afin d'associer sans risque d'erreur un patient au bon dossier pharmaceutique, le décret n° 2008-1326 du 15 décembre 2008 relatif au dossier pharmaceutique précise que ce dernier est provisoirement identifié par un numéro de dossier pharmaceutique (NDP) en l'attente de la mise en œuvre de l'INS-A. Tout comme l'INS-C, le NDP est généré automatiquement par le logiciel de gestion d'officine à partir d'informations lues dans la carte Vitale d'un patient. Il est cependant calculé par une combinaison différente d'informations puisqu'il utilise à la fois le nom, le prénom, la date et le rang de naissance de l'assuré, mais encore, le numéro de série de la carte Vitale.

Comme pour l'INS-C, ces informations sont normalisées, le NDP est calculé selon un algorithme de hachage puis complété d'une clé à 14 chiffres obtenue par l'application d'une fonction de hachage aux trois chiffres du code commune de naissance contenu dans le NIR de l'assuré, ainsi qu'aux trois chiffres suivants codant le rang de naissance. Cette clé permet, en cas de changement de carte, de relier automatiquement le nouveau NDP de l'assuré à son précédent NDP⁸⁷.

Données lues à partir de la carte Vitale	TYPE D'IDENTIFIANT	
	INS-C	NDP
Nom		X
Prénom	X	X
Date de naissance	X	X
NIR	X	
Rang de naissance		X
Numéro de série		X
Algorithme	SHA-2	SHA-2

Tableau 8 : Comparaison des paramètres de calcul de l'INS-C et du numéro de dossier pharmaceutique (NDP) à partir des données de la carte Vitale.

⁸⁷ Délibération n°2008-487 du 2 décembre 2008 portant autorisation des traitements de données personnelles permettant la mise en œuvre généralisée du dossier pharmaceutique.

Le NDP est donc susceptible de changer lorsque certains éléments de la carte Vitale sont modifiés :

- lors d'un remplacement de carte Vitale ou lorsqu'un ayant-droit de plus de seize ans bénéficie nouvellement de sa propre carte Vitale, ou lors d'une modification du rang gémellaire de l'assuré ;

- lors d'une modification de l'identité du patient (mariage, divorce, modification d'état civil...).

Afin de prévenir les risques de doublons et de collisions, chaque dossier pharmaceutique est identifié par un numéro propre, invariable dans le temps et connu de l'hébergeur seul : le NDPi (NDP interne). Une table de correspondance détenue par l'hébergeur permet alors le rapprochement des différents NDP d'un même patient avec le NDPi de son dossier pharmaceutique. Cette correspondance a lieu lors de l'envoi de la requête de connexion au serveur et permet de mettre en évidence :

- **Les doublons** liés à la variabilité du NDP lors de modifications d'informations inscrites dans la carte Vitale, conduisant un patient à avoir plusieurs NDP. Dans ce cas, l'objectif de la table de correspondance est de rapprocher les différents NDP au NDPi unique du dossier pharmaceutique. La clé à 14 chiffres constituant le NDP permet ainsi le rattachement automatique des NDP à leur NDPi sans intervention du pharmacien.

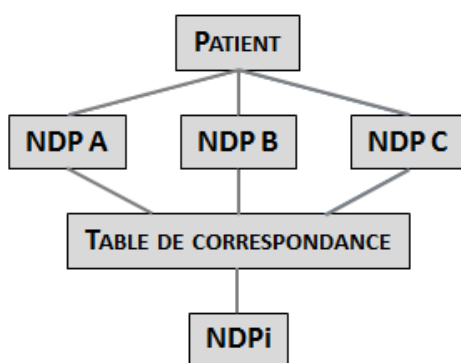


Figure 4: Dossier pharmaceutique et risque de doublons.

- **Les collisions**, lorsque le NDP d'un patient correspond à plusieurs NDPi et donc plusieurs dossiers. Le système de clé à 14 chiffres permet ainsi de déterminer avec précision quel NDPi correspond au NDP du patient :

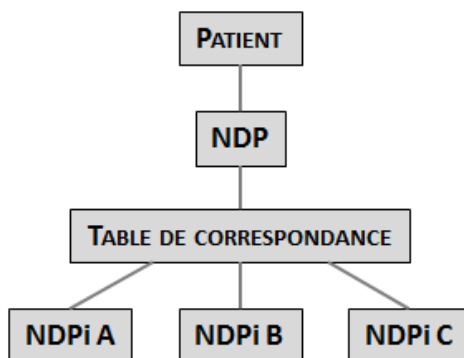


Figure 5: Dossier pharmaceutique et risque de collisions.

A.2.4. L'IDENTIFICATION DES PRODUITS DE SANTE

Au-delà de l'obligation réglementaire pour tout pharmacien titulaire d'une officine de tenir certains registres à jour, l'évolution récente du marquage des produits de santé avec la disparition programmée de la vignette pharmaceutique doit permettre de répondre à des exigences précises de sécurité et de traçabilité de ces produits. Outre les avantages logistiques garants d'une bonne organisation des stocks, l'identification des produits de santé joue un rôle crucial dans leur dispensation puisqu'elle contribue à la codification de la prestation servie à l'assuré dans toute officine et conditionne donc la rémunération du pharmacien.

Anciennement EAN.UCC⁸⁸, c'est l'organisation internationale GS1 qui est en charge de mettre au point, diffuser et promouvoir les langages technologiques communs aux entreprises, fondés sur des standards d'échange d'informations éprouvés, reconnus et adaptés aux besoins de chacun des intervenants de la chaîne d'approvisionnement (49). GS1 France définit ainsi les standards d'élaboration des codes retrouvés sur les produits en France et notamment pour les codes-barres.

Il est important de distinguer codification et symbolisation. En effet, l'attribution d'un numéro d'identification à un produit et l'apposition physique d'un code-barres sur ledit produit sont deux opérations distinctes. Le choix du type de code-barres dépend notamment de la surface disponible et du type d'information à symboliser.

A.2.4.1 LA CODIFICATION DES PRODUITS DE SANTE

Toute présentation d'une **spécialité pharmaceutique** est identifiée par un code unique dit **CIP** (code identifiant de présentation) mentionné dans la décision d'octroi d'autorisation de mise sur le marché. Ces codes sont élaborés par l'Agence nationale de sécurité du médicament en relation avec le club inter pharmaceutique⁸⁹ conformément à une convention datant de 2007. Les **produits de santé sans autorisation de mise sur le marché** (dispositifs médicaux, réactifs de laboratoires, produits de diététique, de cosmétique et parapharmaceutiques) sont quant à eux regroupés dans la codification **ACL** (association de codification logistique). Ce travail collaboratif a permis l'élaboration d'un dispositif de codification garant d'une identification efficace des produits de santé. Ils peuvent être retranscrits de façons différentes à la fois sur le conditionnement extérieur et le cas échéant, sur la vignette pharmaceutique des produits de santé (50).

Jusqu'il y a peu, le code CIP comprenait 7 chiffres (code CIP 7), mais ce système de numérotation était menacé d'épuisement, la quantité de codes encore disponibles se réduisant inexorablement. Suite à l'arrêté du 19 décembre 2012 relatif aux caractéristiques de la vignette pharmaceutique, le code CIP à 13 chiffres devint le code de référence des échanges au sein de la chaîne de distribution pharmaceutique et la vignette est amenée à disparaître au profit du marquage unique du conditionnement extérieur. Les évolutions de la codification ACL sont menées parallèlement à celles mises en œuvre sur le médicament, ACL ayant signé un accord avec GS1 afin de faire évoluer la codification ACL des produits de santé de 7 à 13 caractères selon le standard international (51).

Par ailleurs, les produits de santé inscrits sur la liste des produits et prestations (LPP) remboursables par l'assurance maladie sont quant à eux codifiés par un code spécifique ou

⁸⁸ *EAN international uniform code council.*

⁸⁹ Association créée en 1964 afin de faciliter les échanges entre les différents acteurs de la chaîne du médicament, dont les missions s'exercent dans les domaines de la codification et de la normalisation, mais aussi dans celui des bases de données.

code LPP à sept caractères alphanumériques. Cette codification concerne notamment certains dispositifs médicaux, articles de pansements, orthèses... dont la liste des codes est consultable en ligne sur le site de l'assurance maladie⁹⁰.

Afin de se rapprocher du standard international GTIN⁹¹, le club inter pharmaceutique a passé un accord avec GS1 France pour l'introduction d'un préfixe spécifique (3400) permettant au CIP13 de se rapprocher d'une structure standard internationale. Les produits non soumis à une autorisation de mise sur le marché peuvent quant à eux être identifiés selon une structure GTIN ou en utilisant un code ACL. Le préfixe attribué par GS1 France à ACL et réservé à l'identification de ces produits est le 3401⁹² (50). Le tableau ci-dessous permet de comprendre la structure des codes CIP et ACL à 13 caractères.

STRUCTURES COMPAREES DES CODES CIP ET ACL A 13 CARACTERES	
340PXYYYYYYYYZ Les 4 premiers chiffres 340P constituent un préfixe attribué par GS1 qui permet de dissocier les médicaments à usage humain (code 3400, P=0) sous la codification CIP, des dispositifs médicaux et autres produits de santé (code 3401, P=1) sous la codification ACL.	
↓	↓
3400XYYYYYYYYZ	3401XYYYYYYYYZ
CODE CIP 13	CODE ACL 13
3400XYYYYYYYYZ 1 ≤ X ≤ 5 : Homéopathie X = 9 : Allopathie ↓	3401XYYYYYYYYZ X = 0 : Dispositifs médicaux X = 1 : Vétérinaire X = 3 : Cosmétique X = 2 : Diététique X = 4 : Parapharmacie ↓
3400XYYYYYYYYZ	3401XYYYYYYYYZ
Y = Anciens codes CIP7 et ACL7 ⁹³	
3400XYYYYYYYYZ	3401XYYYYYYYYZ
0 ≤ Z ≤ 9 : Clé de contrôle de cohérence calculée en fonction des autres caractères du code. Elle permet d'accroître la fiabilité de la saisie (manuelle ou par lecteur optique)	

Tableau 9 : Comparaison des structures des codes CIP13 et ACL13 (51) (52).

⁹⁰ <http://www.ameli.fr/>

⁹¹ Le GTIN (*global trade item number*) est un code international de numérotation des articles à 13 chiffres du système GS1. Composé du préfixe entreprise GS1, de la référence article et du caractère de contrôle, il permet d'identifier toute unité commerciale, les produits-services ou les consignations et les unités logistiques.

⁹² Les produits à usage vétérinaire ont également opté pour ce nouveau type de marquage au niveau international. Le code du produit suit une structure GTIN selon les standards GS1 avec un préfixe attribué à l'entreprise propriétaire de la marque commerciale qui va ensuite gérer le code produit.

⁹³ Depuis le 1er janvier 2011 ce code n'a plus de lien avec le CIP7 et l'ACL7.

Toute spécialité pharmaceutique est donc identifiable par un code qui lui est spécifique mais qui ne permet en revanche pas de distinguer une boîte parmi les autres de cette même spécialité. L'évolution du marquage des produits de santé au cours des vingt dernières années a permis de répondre à la fois à des besoins d'identification et de traçabilité, mais encore, de faciliter la facturation et le remboursement des produits de santé par l'assurance maladie. Pour cela, deux dispositifs coexistent actuellement :

- **des informations imprimées sur le conditionnement extérieur** permettant de garantir l'identification, la traçabilité et la sécurité d'emploi de toute spécialité pharmaceutique qu'elle soit remboursable ou non, grâce, respectivement, au code CIP ou ACL à 13 chiffres, au numéro de lot et à la date de péremption ;

- **la vignette pharmaceutique** accolée au conditionnement extérieur des spécialités pharmaceutiques remboursables, renseignant des données d'identification (CIP 13) et des données relatives à la facturation et la prise en charge (prix, tarif forfaitaire de responsabilité). Seuls les progiciels de facturation répondant aux contraintes du cahier des charges SESAM-Vitale 1.40 (addendum 4 au minimum) sont capables d'exploiter ces codes à 13 chiffres (53).

Qu'il s'agisse de la vignette pharmaceutique ou du conditionnement extérieur, ces informations sont retranscrites « en clair » et sous forme codée sur le support. L'évolution des moyens utilisés pour le marquage des produits de santé est ainsi étroitement liée aux modifications de leur codification (passage de codes CIP et ACL de 7 à 13 caractères) et aux obligations réglementaires en matière de traçabilité (inscription du numéro de lot et de la date de péremption).

Afin de mieux percevoir l'intérêt des modifications du marquage des produits de santé, la compréhension des caractéristiques techniques des différentes symbologies de code-barres permet de saisir l'intérêt du remplacement du traditionnel code unidimensionnel par le Datamatrix.

A.2.4.2 LE MARQUAGE DU CONDITIONNEMENT EXTERIEUR

Tout produit fabriqué industriellement comporte de nos jours un code-barres sur son emballage permettant avant tout son identification. Véritable outil de gestion mis au service de l'efficacité, de la sécurité et de la traçabilité, le code-barres repose sur un fonctionnement simple, clair et standardisé. Il ne s'agit pas d'une étiquette comme les autres, mais d'un véritable code international structuré et hiérarchisé qui peut être lu partout dans le monde. Chaque jour les industriels marquent leurs produits d'un code-barres tandis que les distributeurs équipent leurs magasins de lecteurs optiques. Grâce à cette identification automatique des produits, le passage en caisse est accéléré et les erreurs de saisie sont réduites (54). Les produits de santé issus de l'industrie pharmaceutique ne dérogent pas à cette règle. Ils sont marqués selon des modalités bien précises dont la compréhension permet de recueillir de nombreuses informations uniquement par décodage d'un simple code. On les retrouve selon le cas sur la vignette pharmaceutique et/ou sur le conditionnement extérieur du produit et peuvent être représentés selon plusieurs symbologies reconnues par GS1.

Lorsque l'AFSSAPS (aujourd'hui Agence nationale de sécurité du médicament) a retenu le principe d'évolution du code CIP de 7 à 13 caractères en 2007⁹⁴, elle valide également l'évolution du marquage des médicaments. Le code CIP 13 doit désormais figurer

⁹⁴ Avis aux titulaires d'autorisation de mise sur le marché de médicaments à usage humain et aux pharmaciens responsables des établissements pharmaceutiques, JORF n°64 du 16 mars 2007, texte n° 107, page 4950.

sur le conditionnement extérieur dans un code graphique à deux dimensions (GS1 Datamatrix) renseignant⁹⁵ :

- la mention : " Médicament autorisé n° " suivie du numéro de l'autorisation de mise sur le marché (CIP13) ;
- le numéro du lot de fabrication ;
- la date de péremption (55).



Figure 6: Le conditionnement extérieur des médicaments : données de traçabilité.

Cette nouvelle génération de codes-barres bidimensionnels (2D) permet d'encoder une grande quantité d'informations, jusqu'à cent fois supérieures qu'un code-barres 1D classique, pour un coût réduit. Ils offrent aux fabricants la possibilité de stocker jusqu'à 2335 caractères alphanumériques ou 3116 caractères numériques sur une surface très réduite (jusqu'à moins de 1 mm²). Il nécessite toutefois un matériel de lecture optique spécifique, capable de lire également les codes-barres 1D, de même qu'un module logiciel d'intégration dans le système d'information (20).

Il existe de nombreux standards définis par GS1 permettant d'élaborer un code 2D mais le standard retenu pour le conditionnement extérieur des médicaments est le Datamatrix ECC200 tel que défini dans la norme ISO/CEI 16022:2006⁹⁶. Il se rapproche visuellement du QR code⁹⁷ lu par des applications sur *smartphone* au quotidien. De forme carrée ou rectangulaire, le Datamatrix est composé d'un cadre et d'une matrice composée de lignes et de colonnes. Cette représentation constitue un quadrillage ordonné de points noirs et de points blancs délimités par des motifs de repérage, les axes horizontaux et verticaux. Chaque colonne et ligne est composée de modules (carrés ou ronds) noirs (bit =1) ou blancs (bit=0).

Le Data matrix ECC200 est reconnaissable à l'œil humain par son module blanc dans l'angle supérieur droit. Ces couleurs peuvent cependant être inversées.



⁹⁵ Article R.5121-138 du code de la santé publique.

⁹⁶ Disponible sur le site de l'AFNOR (association française de normalisation) : www.afnor.org

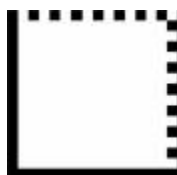
⁹⁷ Quick response code ou code à réponse rapide

Le choix de la taille de la matrice est réalisé en fonction de la quantité de données à encoder mais aussi de leur nature (numérique ou alphanumérique). Le Datamatrix ECC200 se différencie des autres types de codes en particulier par son niveau de sécurisation. Le système de correction d'erreur utilise la méthode de Reed-Solomon⁹⁸ qui est largement utilisée dans de nombreux secteurs d'activité industrielle.

Il peut être imprimé dans différentes tailles selon le nombre de caractères, la technologie de marquage et le support de marquage. A module identique, le Datamatrix rectangulaire permet une impression sur une zone plus étroite en hauteur qu'en largeur et représente donc une solution lorsqu'il existe des contraintes de place sur l'étui. Toutefois, la forme rectangulaire, plus facile à imprimer en ligne, offre moins de possibilités que la forme carrée en cas d'augmentation de la quantité de données à marquer.



Le cadre graphique de la matrice est déterminé par deux éléments formant un « L » plein (*Finder pattern*) et un « L » en pointillés (*Alternating pattern*).



Ce cadre permet l'identification de la position du marquage ainsi que son orientation dans l'espace et permet une lecture omnidirectionnelle du Datamatrix. La lecture est indépendante de la position du code par rapport au lecteur et peut donc être lu dans n'importe quel sens. D'une largeur d'un module, il est toujours le même pour une taille de Datamatrix précise quelque soit les données encodées. Une zone de silence (*quiet zone*) d'au moins un module de large est requise sur les 4 côtés de la matrice afin de permettre son identification (50).

S'ils peuvent encoder jusqu'à 2 335 caractères alphanumériques ou 3 116 caractères numériques, les Datamatrix utilisés pour le marquage des produits de santé ne codent pas plus de 124 caractères, ce qui est suffisant pour en assurer l'identification et la traçabilité (56).

La taille étant définie par le nombre de lignes et le nombre de colonnes représentées (de 10x10 à 144x144 pour les Datamatrix carrés et de 12x36 à 16x48 pour les Datamatrix rectangulaires), les Datamatrix de petite taille (inférieure à 16x16) et de grande taille (supérieure à 36x36) ne sont pas utilisés pour le marquage des produits de santé car leur capacité de codage n'est pas adaptée à la quantité de données codées (50).

⁹⁸ Système d'encodage complémentaire des données permettant d'assurer la lecture et la récupération de ces données en cas de détérioration du symbole (50).

FORME	Dimensions du Datamatrix (lignes x colonnes)	Capacité maximale de codage	
		Caractères Numériques	Caractères Alphanumériques
CARREE	18x18	36	25
	20x20	44	31
	22x22	60	43
	24x24	72	53
	26x26	88	64
	32x32	124	91
RECTANGULAIRE	12x36	44	31
	16x36	64	46
	16x48	98	72

Tableau 10 : Capacités de codage des codes Datamatrix selon leur forme et leurs dimensions (50)

Les modules du Datamatrix sont regroupés en zones de deux types : des zones de données et des zones de Reed-Solomon. Ces dernières permettent la redondance des données et servent à la vérification de la cohérence et au recalcul en cas d'incohérence. Le nombre de zones varie en fonction de la taille du Datamatrix.

Les données codées dans un Datamatrix ECC200 répondent à la structure GS1-128 permettant d'encoder des chaînes d'éléments en utilisant des identifiants de données (ID) ou AI (*application identifier*) afin de répondre à l'obligation de renseigner le numéro de lot et la date de péremption en complément de l'identification du produit par son code CIP ou ACL.

Les spécifications techniques internationales de GS1 recommandent d'imprimer en clair les informations contenues dans le code à proximité de celui-ci, notamment pour faciliter la recherche des informations si le code s'avérait illisible, les informations dématérialisées dans le Datamatrix devant être strictement identiques aux informations en clair.

Il est ainsi possible de schématiser la structure des données d'un tel code (50):



(01)03123451234569(17)100201(10)X245

FNC101031234512345691710020110X245

FNC1 : Préfixe indiquant au lecteur et au logiciel associé qu'il s'agit de la syntaxe EAN-GS1 128. Ce caractère est exploité par le lecteur mais n'est pas transmis, il indique au lecteur que l'ensemble des données imprimées suivent une structure standardisée. Le FNC1 n'apparaît pas en clair, il s'agit simplement d'une valeur spécifique de reconnaissance par les lecteurs.

Les Identifiants de données (ID) ou *Application identifiants* (AI) : Chaque information encodée dans le code Datamatrix est précédée d'un identifiant (ID ou AI) qui permet de savoir avec certitude la nature de la donnée qui suit. Ils peuvent donc prendre plusieurs valeurs différentes :

AI (01) suivi du **code produit (CIP13)**. L'AI (01) indique au lecteur et à la base de données que l'information imprimée est le code CIP 13 sur 14 caractères (il est précédé du chiffre 0).

AI (17) suivi de la **date de péremption** au format AAMMJJ (A = année, M = mois, J = jour). Si la date de péremption imprimée en clair sur l'emballage n'indique pas de jour précis (05 2014 par exemple), les caractères JJ prennent dans ce cas les valeurs 00 et on considère que la date de péremption correspond avec le dernier jour du mois.

AI (10) suivi du **numéro de lot** de taille variable (jusqu'à 20 caractères alphanumériques).

Pour faciliter l'adéquation entre l'information codée et en clair, il est recommandé d'éviter les caractères de ponctuation (-, /, etc...). Si ceux-ci sont utilisés pour le marquage en clair, il faut que les caractères imprimés dans le code-barres soient les mêmes que les caractères en clair pour assurer la cohérence de l'information et fiabiliser les contrôles.

Il est enfin important de noter que le Datamatrix ne livre aucune information sur le prix, ce rôle étant pour le moment assumé par la vignette pharmaceutique. D'autres identifiants de données existent et pourraient être ajoutés s'il se révèle utile de mentionner d'autres données dans le Datamatrix.

A.2.4.3 LA SUPPRESSION DE LA VIGNETTE PHARMACEUTIQUE

Prévue par l'article R.161-50 du code de la sécurité sociale, la vignette pharmaceutique constitue le support des informations destinées à la prise en charge des médicaments inscrits sur la liste des spécialités remboursables par les régimes d'assurance maladie. Ces caractéristiques sont définies par l'arrêté du 21 février 1996 qui précise que celle-ci :

- **doit être de forme rectangulaire** dont les dimensions sont comprises entre 2 x 1,2 cm et 5,5 x 3,5 cm ;
- doit présenter des **informations imprimées en noir** ;
- **est de couleur différente selon le taux de prise en charge** par les régimes obligatoires d'assurance maladie, défini après évaluation du service médical rendu (SMR) :
 - **100 %** pour les médicaments portant une **vignette blanche entourée d'un liseré vert** (reconnus comme irremplaçables et particulièrement onéreux) ;
 - **65 %** pour les médicaments à **vignette blanche** (SMR majeur ou important) et dans le cas d'affections graves ;
 - **30 %** pour les médicaments à **vignette bleue**, les médicaments homéopathiques et certaines préparations magistrales (médicaments à SMR modéré) ;
 - **15 %** pour les médicaments à **vignette orange** (médicaments à SMR faible).

- **comporte une partie supérieure avec un code-barres unidimensionnel** centré horizontalement, représenté selon la symbologie « code 128 », et dont le contenu est exprimé « en clair » en dessous de celui-ci. Il s'agit d'un assemblage de lignes parallèles d'épaisseur variable et d'espaces permettant de créer différentes combinaisons d'éléments correspondants aux différents caractères de la table des caractères. Cette symbologie fut choisi lors du passage aux codes à 13 chiffres afin de tenter de répondre au mieux aux contraintes de taille de la vignette pharmaceutique imposées par l'ajout de 6 chiffres supplémentaires, tout en codant une quantité d'informations plus importantes (ont été ajoutées le taux de prise en charge, le prix et le tarif forfaitaire de responsabilité). Il présente une structure numérique extrêmement efficace permettant de produire des codes-barres très denses capables d'inclure 103 caractères et propose trois jeux de caractères (majuscules, minuscules, numériques) (50). Chaque caractère est composé de trois barres et trois espaces (57).

Le contenu du code-barres 1D de la vignette pharmaceutique d'une boîte d'un médicament peut être interprété de la manière suivante :



4 34009 35966838 000195 00
R CIP13 PRIX TFR

R : taux de remboursement

R=2 : 30% ; R=4 : 65%
R=5 : 100% ; R=9 : 15%

00: prix < TFR
01: prix > TFR

- **renseigne dans sa partie inférieure, la dénomination** sous laquelle le médicament figure sur la liste des spécialités pharmaceutiques remboursables ainsi que la mention « Vignette » (ou « Vign. » voire « V. ») ainsi que le prix limite de vente au public exprimé en euros⁹⁹. Les informations sont reportées en clair sous le code-barres afin de permettre une saisie manuelle en cas de difficulté de lecture.



Figure 7: Vignette pharmaceutique et données de traçabilités : une cohabitation éphémère mais nécessaire.

⁹⁹ Pour les spécialités pharmaceutiques remboursables pour lesquelles la participation de l'assuré est supprimée, le mot « *Vignette » doit être suivi par un rectangle barré par ses diagonales. Pour les spécialités figurant dans un groupe générique et dont le prix limite de vente au public est strictement supérieur au TFR, la partie inférieure comporte sur une même ligne le prix de vente au public et le TFR (mention « Forf. » en euros).

Les premières réflexions concernant la suppression de la vignette pharmaceutique furent engagées dès 1999 suite à la réforme sur la marge des pharmaciens. L'introduction d'un forfait à la boîte ouvrait ainsi la voie à un système dans lequel la rémunération du pharmacien pouvait s'affranchir du prix du médicament.

Une seconde tentative fut menée en 2004 à l'occasion de la baisse du taux de remboursement des spécialités homéopathiques. Dans un contexte de montée en charge des médicaments génériques, les pharmaciens s'étaient alors opposés à cette suppression, mettant en avant le rôle d'information des patients sur le prix du médicament offert par la vignette (20). Cette seconde tentative échoua donc, tout comme celle émanant de la Caisse nationale d'assurance maladie en 2005. Ce n'est que lors de l'introduction du Datamatrix et du passage du code CIP de 7 à 13 caractères en septembre 2008¹⁰⁰ que la date arrêtée pour la fin programmée de la vignette pharmaceutique fut initialement portée au 1^{er} janvier 2011 puis au 31 décembre 2012¹⁰¹, pour être finalement reportée au 30 juin 2013¹⁰² (20).

L'avis du ministère des affaires sociales et de la santé aux fabricants et distributeurs de spécialités pharmaceutiques du 29 janvier 2013 précise que cet ultime report au 30 juin doit permettre de « *finaliser les discussions sur les implications pratiques, le principe étant acquis, de la suppression de la vignette pharmaceutique* ». Le système cible consiste en l'utilisation du Datamatrix comme identifiant unique et non détachable, du médicament. Faute de pouvoir loger à la fois le Datamatrix et la vignette détachable sur le conditionnement de leurs produits, le laboratoire Boiron a été autorisé à supprimer cette dernière et apposer directement le code-barres sur l'étiquette du produit (20).

Tout comme l'était la vignette automobile, la vignette pharmaceutique est un élément familier de la vie quotidienne des Français. Elle permet de communiquer le code CIP de toute spécialité facturée à un assuré lorsqu'elle est collée sur une feuille de soins papier en cas d'impossibilité de générer une feuille de soins au format électronique.

Le décret N°97-480 du 13 mars 1997 supprimant l'obligation pour les pharmaciens de coller les vignettes des produits de santé sur les feuilles de soins dès lors que leur image électronique est télétransmise aux organismes d'assurance maladie a ainsi signé « l'arrêt de mort » de la vignette pharmaceutique puisqu'il permet désormais de télétransmettre ce code et les données de facturation aux caisses sous forme électronique. Dans ce cas, le pharmacien estampille la vignette¹⁰³ afin d'éviter une réutilisation frauduleuse de ce dispositif (40). Ainsi, en cas d'impossibilité de générer une FSE, le pharmacien peut sans difficulté imprimer ces codes sur la feuille de soins papier comme c'est déjà le cas pour les produits relevant de la liste des produits et prestations remboursables.

Mais qu'en est-il de l'information des patients sur le prix et la prise en charge de ces spécialités, assurée par la vignette ?

La connaissance par les patients du prix des médicaments pris en charge par les organismes d'assurance maladie est très importante. Les assurés bénéficiant systématiquement du tiers-payant pharmaceutique n'ont parfois aucune idée du coût de leur traitement pour l'assurance maladie et semblent bien souvent peu conscients de leurs dépenses en matière de santé¹⁰⁴. Les

¹⁰⁰ Arrêté du 25 septembre 2008 relatif aux caractéristiques de la vignette pharmaceutique.

¹⁰¹ Arrêté du 7 décembre 2010 relatif aux caractéristiques de la vignette pharmaceutique.

¹⁰² Arrêté du 19 décembre 2012 relatif aux caractéristiques de la vignette pharmaceutique.

¹⁰³ Article R.161-51 du code de la sécurité sociale.

¹⁰⁴ Selon une étude de l'IFOP d'octobre 2011, intitulée « *Les Français et le système de santé* », 78% des Français ne connaissent pas le budget qu'ils consacrent à leur santé (<http://www.ifop.com/>).

prix des médicaments non remboursables étant libres, l'information sur le prix est donc capitale dans les cas d'automédication. Une enquête récente de l'UFC-Que-Choisir¹⁰⁵ montre qu'il reste de nombreux progrès à faire en matière d'information des patients sur les prix puisque dans neuf pharmacies sur dix, l'affiche devant préciser que « le prix des médicaments non remboursables est libre » est absente.

La problématique est différente pour les médicaments remboursables puisque la vignette porte à la fois le prix de vente au public (et éventuellement le tarif forfaitaire de responsabilité) ainsi que le taux de prise en charge selon un code couleur. La suppression de la vignette pose donc la question du sort à réserver à ces informations dans un contexte parfois difficilement compréhensible du grand public. Une récente étude¹⁰⁶ montre d'ailleurs le faible niveau de compréhension du système des prix et de prise en charge par la population générale puisque 34 % des personnes interrogées ignorent par exemple, que la couleur de la vignette renseigne sur le niveau de prise en charge.

Une bonne connaissance du prix des médicaments remboursables doit contribuer à sensibiliser les bénéficiaires de l'assurance maladie, sur le coût de leurs dépenses de santé pour la collectivité. Le principe de responsabilisation pourrait en effet être un vecteur de modération de la consommation médicale des patients. Dans ce domaine, le « ticket vitale » consiste à éditer une « facture » récapitulative des produits dispensés imprimée au dos de l'ordonnance remise au patient à la fin de la dispensation. Il détaille ainsi généralement des données d'identification de la pharmacie et du patient, les médicaments délivrés, leurs prix et leurs taux de prise en charge ainsi que la somme totale due et la répartition entre la part prise en charge par l'assurance maladie obligatoire, celle prise en charge par l'assurance maladie complémentaire et celle restant à la charge de l'assuré.

Dans son rapport sur les modalités de mise en œuvre de la suppression de la vignette pharmaceutique, l'inspection générale des affaires sociales émet certaines recommandations relatives à la mise en œuvre d'un système de remplacement à la vignette (20).

Ces recommandations consistent notamment à :

- supprimer la vignette au profit du Datamatrix comportant aujourd'hui le CIP13 et demain, un identifiant européen unique et ne plus faire porter par la boîte le prix et les conditions de prise en charge ;
- valoriser le ticket vitale en une facture informative obligatoire au contenu normalisé ;
- substituer le code couleurs des vignettes par une mention repérable du caractère remboursable ou non du médicament ;
- substituer l'étiquetage du prix des médicaments non remboursables par une facture détaillée obligatoire au format normalisé ;
- indiquer le niveau de SMR sur le conditionnement extérieur ou la notice ;
- créer une base de données à destination du public permettant de connaître les principales caractéristiques des médicaments.

¹⁰⁵ Automédication : Contre les maux diagnostiqués, l'UFC-Que Choisir propose son antidote ; mars 2012 ; une synthèse de l'étude a été publiée dans le numéro 502, d'avril 2012, du mensuel Que Choisir, pp. 28-30.

¹⁰⁶ Le produit de santé, entre croyances et réalité. Etude réalisée par des étudiants du master marketing de la santé de l'université Pierre et Marie Curie, 15 mai 2012 (<http://www.upmc.fr/>).

Chapitre 3 : L'HEBERGEMENT ET LA TRANSMISSION DE DONNEES ELECTRONIQUES

Si la dématérialisation des documents promet un gain de place considérable lié à l'archivage, les données électroniques ainsi générées nécessitent toutefois un support de stockage matériel bien réel. Les données recueillies à l'officine sont ainsi généralement vouées à être sauvegardées sur un support informatique afin d'en permettre un traitement ultérieur. Le stockage de ces données de santé, particulièrement sensibles, fait l'objet d'une activité d'hébergement règlementée et devant répondre à de nombreuses exigences de sécurité. Cette activité peut être réalisée par le professionnel de santé lui-même ou confiée à un hébergeur tiers agréé de données.

Par ailleurs, l'ensemble des données recueillies dans le cadre de l'utilisation de dossiers médicaux en ligne partagés (dossier pharmaceutique, dossier médical personnel...) sont quant à elles systématiquement conservées par un hébergeur tiers agréé auquel les pharmaciens peuvent accéder sur l'ensemble du territoire. La transmission de données électroniques entre deux entités (personnes ou serveurs) repose sur l'utilisation d'une infrastructure de télécommunication réseau d'étendue variable (locale ou étendue).

Hébergement et transmission de données sont donc bien souvent indissociables, mais pour interagir et se comprendre les différents systèmes doivent partager des outils sémantiques et techniques communs. L'interopérabilité des systèmes constitue ainsi une composante fondamentale du développement de tout système d'information et particulièrement dans le domaine de la santé où l'expression de termes médicaux précis doit être parfaitement interprétable et exploitable par les différents systèmes.

Compte tenu de la sensibilité des données de santé, garantir leur confidentialité, leur intégrité ainsi que l'authentification des correspondants lors d'une transmission ou d'un hébergement sont des paramètres devenus incontournables pour gagner la confiance des utilisateurs envers ces systèmes. La sécurité des données électroniques hébergées ou transmises électroniquement passe donc à la fois par des mesures organisationnelles et l'utilisation de techniques cryptographiques notamment proposées par l'infrastructure technique du système SESAM-Vitale et l'ASIP Santé.

Alors que tout devient donnée numérique, le monde entier prend conscience des enjeux liés à leur exploitation avec la récente révélation de l'existence d'un programme secret américain intitulé *Prism* qui serait destiné à la surveillance de contenus électroniques transitant sur les serveurs des plus grands groupes informatiques mondiaux. Il apparaît donc désormais nécessaire de renforcer la confiance des patients et des professionnels de santé pour l'utilisation de services en ligne tels que le dossier pharmaceutique ou le DMP.

A.3.1. L'HEBERGEMENT DE DONNEES DE SANTE

Quel qu'en soit le support, la conservation de données personnelles par un tiers autorisé correspond à une activité d'hébergement. Celui-ci peut consister en l'association d'un traitement et d'archivage des données, d'un simple archivage ou de la fourniture d'un site de sauvegarde. Les données enregistrées chaque jour par les systèmes informatiques des professionnels de santé constituent ainsi de larges bases de données sensibles. Conformément à l'article 34 de la loi informatique et libertés, *« le responsable du traitement doit mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données archivées contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisé, notamment lorsque le traitement comporte des*

transmissions de données dans un réseau ainsi que contre toute autre forme de traitement illicite ».

Avec l'émergence fulgurante du « *cloud computing* », les professionnels de santé pourraient être tentés d'utiliser la panoplie d'outils destinés au grand public tels que *Dropbox* ou *Google Drive* pour archiver les données relatives à leurs patients, puisqu'ils ont de plus en plus tendance à solliciter ces systèmes quotidiennement pour héberger leurs propres données. Compte tenu de l'incertitude actuelle qui pèse sur la réelle confidentialité des données transitant sur les serveurs de ces groupes informatiques, cette pratique pourrait être hautement périlleuse (58).

A.3.1.1 STATUT JURIDIQUE DE L'HEBERGEUR

L'article L.1111-8 du code de la santé publique définit le statut d'un hébergeur de données de santé comme une « *personne physique ou morale agréée* » auprès desquelles « *les professionnels de santé ou les établissements de santé ou la personne concernée peuvent déposer des données de santé à caractère personnel, recueillies ou produites à l'occasion des activités de prévention, de diagnostic ou de soins* ».

Si les professionnels de santé peuvent choisir de conserver eux-mêmes les données de santé de leurs patients ils ont également la possibilité de les confier à un hébergeur tiers, agréé pour cette activité. Dans les deux cas, cette activité fait l'objet d'un contrat et doit être réalisée conformément aux dispositions de la loi informatique et libertés.

Lorsque les professionnels de santé ou les établissements de santé hébergent des données de santé par leurs propres moyens, ils ne sont alors pas tenus de recueillir le consentement exprès de l'intéressé pour conserver ces données « *dès lors que l'accès aux données détenues est limité au professionnel de santé ou à l'établissement de santé qui les a déposées, ainsi qu'à la personne concernée* ». Le patient peut néanmoins faire valoir son droit d'opposition au traitement et son droit d'accès aux données de santé à caractère personnel.

Lorsqu'un professionnel de santé confie l'hébergement de ses fichiers à un hébergeur tiers agréé, il lui délègue la responsabilité d'assurer la confidentialité, l'intégrité et la disponibilité des données de santé qui lui sont confiées. Il tient ces données à disposition des personnes qui les leur ont confiées et, lorsqu'il est mis fin à l'hébergement, les données lui sont restituées dans leur totalité sans en conserver de copie. Un tiers hébergeur de telles données doit, pour exercer son activité, démontrer sa capacité à mettre en œuvre une politique de sécurité et de confidentialité renforcée, en vue de l'obtention d'un agrément pour exercer l'activité d'hébergeur de données de santé. « *Les conditions d'agrément des hébergeurs des données, quel qu'en soit le support, sont fixées par décret en Conseil d'Etat pris après avis de la CNIL et des conseils de l'ordre des professions de santé* ».

Les modalités d'exercice de l'activité d'hébergeur de données de santé ont été apportées par le décret du 4 janvier 2006 relatif à l'hébergement de données de santé modifiant le code de la santé publique¹⁰⁷. Cet agrément est octroyé pour une durée de trois ans renouvelable par le ministre chargé de la santé, qui se prononce après avis de la CNIL et d'un comité d'agrément placé auprès de lui. Les conditions à réunir ainsi que les démarches à effectuer en vue de son obtention sont abordées dans une sous-section du code de la santé publique (articles R.1111-9 à R.1111-15-1) et le référentiel pour constituer un dossier de demande d'agrément est

¹⁰⁷ Code de la Santé Publique : Hébergement des données de santé à caractère personnel sur support informatique (articles R.1111-9 à R.1111-15-1) et sur support papier (articles R.1111-16 à R.1111-16-1).

disponible sur le site de l'ASIP Santé. Afin de faciliter et accélérer ces procédures d'agrément, l'ASIP Santé publie également l'ensemble des documents et formulaires nécessaires à la constitution du dossier. L'une de ces exigences consiste en la présence d'un médecin inscrit à l'ordre ¹⁰⁸ lié contractuellement à l'hébergeur. Ce « médecin de l'hébergeur » est susceptible d'accéder aux données archivées notamment en cas de problème technique. Nouvellement formé, le collège national des médecins des hébergeurs composé de la plupart des médecins des hébergeurs agréés souhaite faire évoluer les modalités de la protection des données personnelles de santé et clarifier les missions et les responsabilités de ces « nouveaux médecins ».

La liste des hébergeurs de données de santé à caractère personnel agréés est publiée et mise à jour par l'ASIP Santé sur son site internet¹⁰⁹. Au 3 décembre 2012, quarante-quatre décisions d'agrément ont été rendues dans le cadre de la procédure d'agrément des hébergeurs de données de santé à caractère personnel précisée par le décret du 4 janvier 2006.

A.3.1.2 STOCKAGE, SAUVEGARDE ET ARCHIVAGE

Le stockage de données électroniques a pour but de les conserver sur des supports de données de natures diverses (disque dur, CD, DVD, clé USB...) tout en réunissant les conditions nécessaires à la restitution fiable et rapide des informations. L'archivage ou la sauvegarde doivent permettre la lecture de données, il est ainsi possible de les sauvegarder sur un support distinct ou de les enregistrer sur le disque dur du système. Cette fonction de stockage peut être assumée par le professionnel de santé lui-même ou par un hébergeur tiers (10).

La sauvegarde permet de dupliquer les données d'un système afin de les mettre en sécurité. Des sauvegardes régulières permettent de restaurer le système avec un minimum de pertes de données et assurent la continuité de l'activité en cas de panne ainsi que l'intégrité des données et des historiques. On distingue ainsi les sauvegardes incrémentales (journalières) ne concernant que les données ajoutées depuis la dernière sauvegarde et les sauvegardes complètes hebdomadaires ou bimensuelles (10).

Tout comme la sauvegarde, l'**archivage** consiste à créer une copie des données à un moment déterminé permettant ainsi de conserver et classer des documents ne présentant plus un intérêt immédiat (documents non actifs) tout en les rendant facilement accessibles dans le futur. L'archivage est encadré par des normes de qualité définies par l'organisation internationale de normalisation (ISO) et doit répondre aux exigences de la loi informatique et libertés (58) (10).

On distingue ainsi (10):

- les archives courantes qui concernent des données d'utilisation courante ;
- les archives intermédiaires constituées par des données n'étant plus utiles dans l'immédiat mais qui gardent un intérêt à long terme. Elles sont conservées sur un support distinct ;
- les archives définitives constituées par des données dont l'intérêt justifie leur conservation.

¹⁰⁸ Ce médecin peut exercer dans un pays tiers où les données sont hébergées, en vertu du principe de reconnaissance des diplômes. Dans cette hypothèse, il doit pouvoir s'exprimer en français et son contrat, rédigé en langue française doit être transmis avec la demande d'agrément.

¹⁰⁹ <http://esante.gouv.fr/>

Les sauvegardes et les archives sont donc des copies des informations à un moment donné, il ne s'agit donc plus des données originales. Pour faire office de preuve juridique, ces copies doivent associer fond et forme de manière indissociable, être accompagnées de l'historique des modifications depuis la date de copie et être enregistrées sous un format non modifiable, dissocié de l'éditeur.

L'archivage des documents à l'officine permet de conserver et classer de nombreux types de documents ne présentant plus d'intérêt immédiat tout en les gardant facilement accessibles pour une utilisation future. Les documents comptables, sociaux (statuts et actes de société, procès-verbaux, rapports et compte rendus...), commerciaux (contrats, commandes...), les pièces comptables justificatives (factures, bons de livraison...), les documents relatifs aux locaux et aux salariés doivent ainsi être archivés pour des durées définies par le code du commerce, le code civil, le code des impôts, le code du travail, le code de la santé publique et le code de la sécurité sociale (59).

La norme simplifiée n°52 relative aux traitements automatisés de données à caractère personnel mis en œuvre par les pharmaciens à des fins de gestion de la pharmacie prévoit que les informations enregistrées ne peuvent être conservées dans l'application au-delà d'une durée de **trois ans à compter de la dernière intervention sur le dossier du patient**. A l'issue de cette période, elles sont archivées sur un support distinct et peuvent être conservées pendant quinze ans dans des conditions de sécurité équivalentes à celles des autres données enregistrées dans l'application.

DUREES LEGALES DE CONSERVATION DES PRINCIPAUX DOCUMENTS EN OFFICINE	
Type de document	Durée légale de conservation
Ordonnancier unique pour les listes I, II et stupéfiants	10 ans
Registre des préparations magistrales et officinales	10 ans
Registre des stupéfiants	10 ans
Registre des médicaments dérivés du sang	40 ans
Double des FSE et leurs accusés de réception	90 jours
Ordonnances et bons de commande des médicaments stupéfiants, de substitutifs aux opiacés ou de médicaments à délivrance particulière	3 ans
Ordonnances prescrivant : - certains dispositifs médicaux : sondes et canules de longueur supérieure à 18 cm, seringues intra-utérines... - certaines préparations : à base de sabine, de phosphore blanc, d'ergot de seigle, de sels de plomb, de sel insoluble de bismuth...	3 ans
Pièces justificatives numériques destinées à l'assurance maladie	90 jours

Tableau 11 : Durées légales de conservation des principaux documents à l'officine.

Lors d'un changement de logiciel professionnel il arrive que les sauvegardes ou les archives électroniques ne soient plus lisibles, les rendant indisponibles. Il est donc impératif que la SSII à laquelle le pharmacien a recours garantisse la possibilité de récupérer l'intégralité des

archives et sauvegardes. Il peut donc être utile de sauvegarder au moins une fois l'ensemble des données, avec le logiciel et le système d'exploitation permettant une restauration de l'environnement complet.

A.3.1.3 SUPPORTS DE DONNEES DEMATERIALISEES

La diversification des « supports de masse » couplée au développement exponentiel de leurs capacités de stockage permettent aujourd'hui de disposer de périphériques peu mobilisables en raison de leur fragilité et leur difficulté d'accès, inclus au sein d'un système informatique, et d'autres portatifs. Dotés de capacités généralement plus faibles, ces derniers permettent néanmoins la réalisation de sauvegardes efficaces mais encore, de **contourner la dématérialisation de la transmission de données électroniques**, source de nombreux risques d'interception par un tiers.

A.3.1.3.a Le disque dur interne d'un ordinateur

Dotés de capacités allant jusqu'à 4 à 6 Téraoctets (To), le disque dur interne représente le périphérique de mémoire de masse par excellence d'un ordinateur. Outre les fichiers systèmes, il permet de stocker à long terme de très grandes quantités de données électroniques exploitables par le système informatique. Son fonctionnement repose sur des technologies mécaniques constituant ainsi une mémoire de masse magnétique. Intégré à l'unité centrale il n'est pas voué à être transporté car il est très fragile puisque des éléments mécaniques sont en mouvement. Il faut donc veiller à le protéger de chocs (en particulier en cas de remplacement) et de sources magnétiques auxquels il peut être sensible.

A.3.1.3.b Les médias amovibles classiques

Par opposition au disque dur interne, les supports de stockage amovibles sont susceptibles d'être déconnectés de l'ordinateur et transportés à volonté, ils sont donc relativement plus robustes. Il s'agit de mémoires de masse dont les principes de fonctionnement sont variables et dont les avantages sont nombreux. Ils permettent le transport et la conservation de données électroniques d'un système informatique à distance de ce dernier constituant ainsi un moyen efficace de sauvegarde (par exemple en cas d'incendie). Certains nécessitent un périphérique de lecture adapté pour être utilisés tandis que d'autres sont connectés à l'ordinateur par le biais de connexions non spécifiques comme le port USB.

La disquette informatique, ou disque souple (de l'anglais *floppy disk*) nécessite un lecteur spécifique qui n'est généralement plus proposés lors de l'achat d'un ordinateur neuf depuis quelques années. En effet, elle n'est presque plus utilisée en raison de sa faible capacité de stockage (1,4 Mo) et sa fragilité relative (choc, rayures, magnétisme), au profit des clés USB dès le début des années 2000. Les disquettes subsistent de façon optionnelle pour leur facilité d'utilisation avec d'anciens systèmes d'exploitation.

Les disques optiques parmi lesquels on distingue le CD ROM (*compact disc*), le DVD ROM (*digital versatil disk*) et le BD ROM (*blu-ray disc*) sont des périphériques de stockage de masse fonctionnant à l'aide d'un lecteur adapté présent dans l'unité centrale. Ils peuvent être inscriptibles, formatables et réinscriptibles grâce à des graveurs dont la généralisation dès la fin des années 1990 a permis d'en faire le premier média amovible offrant des capacités de stockage suffisantes pour sauvegarder de grandes quantités de données sur un support réduit (bien que lent et fragile car très sensible aux rayures). Si à l'origine le CD était principalement utilisé pour stocker de la musique sous forme numérique il est également possible d'y inscrire différents types de données électroniques. C'est ainsi que les DVD sont également utilisés

pour stocker des vidéos numériques (en haute définition pour les BD) mais sont aussi capables de contenir de très grandes quantités de données (jusqu'à 50 Go pour les BD et bientôt plus).

Type de disque	Utilisations	Capacité de stockage
CD	• Stockage informatique de masse transportable • Audio	682 à 737 Mo
DVD	• Stockage informatique de masse transportable • Vidéo	4,7 à 17 Go
BD	• Stockage informatique de masse transportable • Vidéo haute définition	50 à 200 Go

Tableau 12 : Principales utilisations et capacités maximales de stockage des disques CD, DVD et BD.

Les cartes mémoires sont des médias de stockage de masse le plus souvent utilisés avec les appareils photos numériques, les lecteurs audio numériques ou les consoles de jeux mais sont susceptibles d'archiver tout type de fichiers. Il existe de très nombreux types de cartes mémoires dont les lecteurs ne permettent généralement pas une inter-compatibilité mais c'est le type de carte SD (*standard digital*) qui est actuellement le plus répandu. Les ordinateurs de dernières générations sont le plus souvent équipés de lecteurs de cartes mémoires permettant d'accéder à son contenu. D'une capacité de 2 à 32 Go, ces cartes miniaturisées peuvent ainsi contenir de très grandes quantités de données mais sont actuellement moins utilisées que les clés USB pour le stockage de données non spécifiques en raison de leur relative fragilité et de leur coût.

Les clés USB sont des supports de stockage amovibles ne nécessitant pas de périphérique dédié pour leur lecture par un système informatique mais se branchent directement sur le port USB (*universal serial bus*) qui équipent les ordinateurs commercialisés depuis le début des années 2000. Ce port permet l'alimentation électrique de la clé ainsi que le transfert des données qu'elle contient. Contrairement aux disques durs, les clés USB utilisent une mémoire flash et non des éléments mécaniques pour leur fonctionnement ce qui les rend plus résistantes aux chocs. D'une capacité maximale de 256 Go, elles constituent actuellement la meilleure alternative pour stocker rapidement de grandes quantités de données sur un périphérique externe de taille réduite mais robuste.

Les disques durs externes sont, comme leurs homologues intégrés à l'unité centrale, des périphériques de stockage de masse utilisant une mémoire magnétique. Ils ne sont cependant pas inclus dans l'unité centrale d'un ordinateur mais s'y connectent généralement via le port USB qui en assure l'alimentation électrique et permet le transfert des données. De capacités proches de celles proposées par les disques durs internes, ils sont inclus dans un boîtier robuste permettant de le protéger d'éventuels chocs susceptibles d'être à l'origine d'une perte des données. Certains disques durs externes miniaturisés à l'extrême se présentent sous forme d'un petit boîtier similaire à une clé USB mais n'utilisant pas de mémoire flash, on parle de *microdrive*.

A.3.1.3.c Les serveurs de stockage de données

Les données recueillies par chaque poste de travail informatique au cours d'une journée de travail à l'officine sont centralisées par l'intermédiaire d'un réseau local vers un **serveur de stockage en réseau** ou NAS (*network attached storage*). Il s'agit d'un **serveur « physique »** équipé d'un disque dur de haute capacité ou d'un boîtier généralement composé de plusieurs disques durs offrant un volume de stockage très confortable dont l'accès est généralement autorisé par la saisie d'un mot de passe et éventuellement d'un identifiant. Il héberge la base de données et gère la lecture et l'écriture des postes utilisateurs. Il est dédié à cette fonction et ne doit pas servir de poste de travail à un utilisateur. En effet, si un utilisateur travaille sur le serveur, le traitement des données sera ralenti et il y a un plus grand risque de plantage du poste. Si le serveur est arrêté, l'accès aux données est bloqué pour tous les utilisateurs. C'est pourquoi le serveur doit toujours rester allumé, y compris pour la réalisation de sauvegardes régulières.

Par ailleurs, les **serveurs « virtuels »** dédiés à l'hébergement de données en ligne reposent généralement sur l'utilisation du logiciel *Apache* capable de gérer les requêtes de connexions à de volumineuses bases de données informatiques. Assemblés en « *data centers* » ou centre de traitement des données, ils constituent de véritables coffres forts de données personnelles à distance mis à disposition des usagers.

Si de nombreux prestataires de services en ligne proposent à tous de larges espaces de stockage, l'engouement pour le « *cloud computing* » pourrait s'estomper après les récentes révélations sur l'existence d'un programme secret américain de surveillance de correspondances téléphoniques et électroniques à l'échelle mondiale au moyen de deux outils : *Prism* et *Upstream*, impliquant les plus grandes firmes informatiques mondiales. Dans ce contexte, il est donc légitime de s'interroger sur les conditions d'hébergement des données de santé confiées aux hébergeurs de données de santé agréés par le ministère chargé de la santé en concertation avec la CNIL. L'ASIP Santé fait ainsi preuve d'une grande transparence en mettant à disposition de nombreuses informations relatives aux modalités d'obtention de l'agrément.

Cependant, même si tout contrat d'hébergement précise le lieu où sont hébergées les données, **rien ne s'oppose à ce qu'une base de données de santé à caractère personnel soit hébergée en dehors du territoire français**¹¹⁰ pourvu que des moyens permettant de s'assurer d'un niveau de protection adéquat soient employés lors du transfert de telles données¹¹¹ (60).

A.3.2. LES RESEAUX INFORMATIQUES A L'OFFICINE

L'interconnexion des postes de travail informatiques au moyen d'un réseau local permet de partager et centraliser des données afin d'en faciliter le traitement. De plus, toute officine doit pouvoir télétransmettre les documents électroniques relatifs à la facturation des produits de santé aux organismes d'assurance maladie et proposer le service de dossier pharmaceutique. Il doit pour cela bénéficier d'un accès à un réseau étendu : le réseau internet.

¹¹⁰ Directive communautaire 95/46/CE du 24 octobre 1995 transposée en droit français par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi informatique et libertés.

¹¹¹ Articles 68 et 69 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

A.3.2.1 LE RESEAU INFORMATIQUE LOCAL

Afin de permettre à plusieurs postes de travail informatiques de partager des données, les ordinateurs peuvent être reliés entre eux grâce à des lignes de communication (câbles réseaux, ondes wifi...) et des éléments matériels (cartes réseau, *hubs*...). Plusieurs postes informatiques peuvent ainsi communiquer entre eux au travers d'un réseau local ou LAN (*local area network*) propre à l'officine. Ce type de réseau privé permet de relier des ordinateurs et des périphériques de l'officine entre eux.

L'arrangement physique, c'est-à-dire la configuration spatiale du réseau, est appelé topologie physique. Par opposition, la topologie logique représente la façon dont les données transitent dans les lignes de communication. A l'heure actuelle, la grande majorité des pharmacies utilise un câblage Ethernet (RJ45) dont le débit est jusqu'à huit fois supérieur au wifi et garantissant une connexion physique *a priori* inviolable entre les postes.

Si plusieurs modèles d'organisation proposés par le cahier des charges SESAM Vitale sont acceptables, la topologie la plus adaptée à la pratique officinale utilisant plusieurs postes de travail (configuration multiposte) consiste à :

- associer un lecteur de cartes bi-fente par poste de travail informatique (on parle de poste de travail mono-canal) ;
- connecter chaque poste de travail au serveur central de l'officine selon une topologie en étoile.

Dans une **topologie en étoile**, les ordinateurs du réseau sont indépendamment reliés au **serveur central de l'officine**. Comme nous l'avons vu, la carte réseau connectée à la carte mère de chaque ordinateur comporte un connecteur (que nous désignerons connecteur 1a) permettant de connecter un câble réseau de type RJ45 reliant ainsi chaque poste au **serveur central de l'officine** (connecteur 1b). Ce dernier, comporte un **séquenceur** chargé de transmettre les requêtes de connexions. Les connecteurs sont des intermédiaires de communication entre des éléments informatiques de natures différentes qui permettent d'exprimer les informations dans un format compréhensible par ces différents éléments. Les connecteurs 1a et 1b permettent ainsi de standardiser les informations entre les postes de travail et le serveur central de l'officine et les connecteurs 2a et 2b permettent de standardiser les informations entre le serveur central de l'officine et un serveur distant. Il s'agit d'une composante fondamentale du développement d'un cadre d'interopérabilité des systèmes d'information du domaine de la santé permettant la compréhension mutuelle et l'échange de données entre deux systèmes distants.

Au cœur du réseau local, **le séquenceur** est un module installé sur le serveur central de l'officine permettant le traitement des requêtes de connexions entre le réseau local (via son connecteur 2a) et un serveur distant (connecteur 2b). Il permet ainsi :

- de recevoir et concentrer les requêtes émises par chaque poste de travail puis les transmettre vers le serveur distant ;
- d'identifier chaque requête par un numéro unique ;
- de vérifier le format de ces requêtes afin qu'elles soient comprises du serveur distant ;
- d'assurer certaines fonctions de sécurité dans la transmission des données ;

- de gérer les erreurs de connexions (pannes techniques, coupures réseaux...) en créant une file d'attente des données afin de tenter une réémission ultérieure ;
- d'enregistrer l'ensemble des opérations et des erreurs dans un journal de traces...

Ce séquenceur est capable de fonctionner en **mode synchrone** (ou total), c'est-à-dire immédiatement (par exemple pour une création, une consultation ou une alimentation « en direct » d'un dossier pharmaceutique) ou en **mode asynchrone** (ou partiel) où la connexion avec le serveur a lieu à instant préalablement défini.

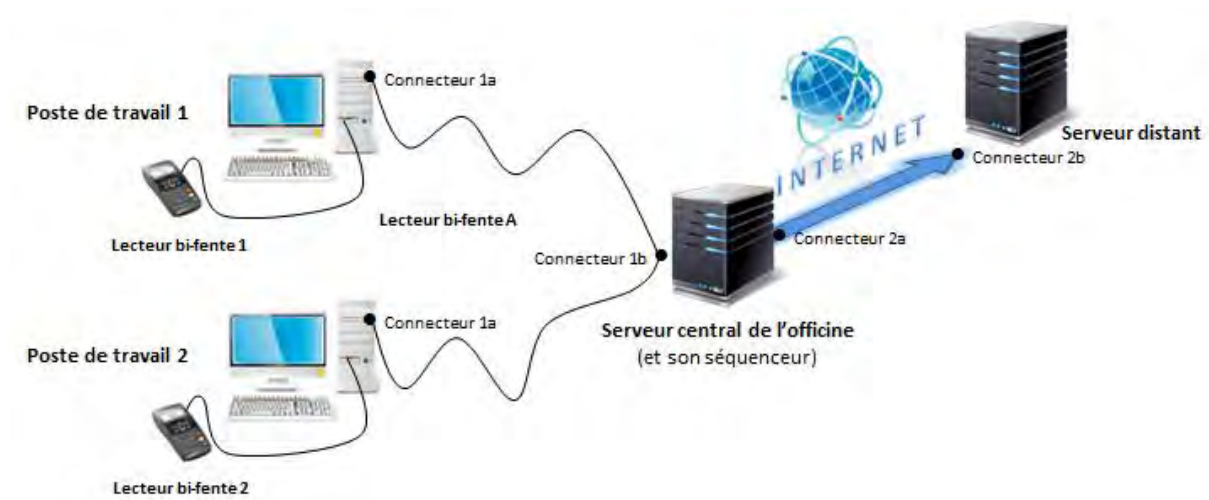


Figure 8 : Mise en évidence du rôle d'interface du serveur central de l'officine dans une topologie réseau en étoile.

Contrairement aux réseaux bâtis selon une topologie en bus¹¹², les réseaux suivant une topologie en étoile sont beaucoup moins vulnérables car une des connexions peut être débranchée sans paralyser le reste du réseau. Le point névralgique de ce réseau est le concentrateur, car sans lui, plus aucune communication entre les ordinateurs du réseau n'est possible.

A.3.2.2 LE RESEAU INTERNET

Le réseau internet est très fréquemment utilisé par les professionnels de santé et tout particulièrement les pharmaciens leur permettant notamment :

- la recherche d'informations médicales ou non, utiles à la pratique professionnelle ;
- l'envoi et la réception de courriers électroniques ;
- la transmission de commandes aux laboratoires et aux organismes répartiteurs ;
- la télétransmission des factures électroniques et des pièces justificatives aux organismes d'assurance maladie ;
- l'alimentation des dossiers pharmaceutiques et la réception d'informations en retour comme des alertes sanitaires, des retraits de lots...

¹¹² Une topologie en bus utilise une ligne de transmission unique à laquelle chaque ordinateur est connecté.

L'utilisation de ce réseau grand public par des professionnels responsables de la confidentialité des données qu'ils transmettent doit donc intégrer un besoin fort des professions de santé : la sécurisation des connexions distantes.

A.3.2.2.a Modalités d'accès et sous-traitance

Afin de mettre œuvre la transmission de données électroniques, tout pharmacien doit disposer d'un accès à internet. Il est cependant nécessaire de différencier (10) :

- **les transmissions à caractère obligatoires** telles que la télétransmission des factures électroniques aux organismes d'assurance maladie ou l'alimentation du dossier pharmaceutique, dont la sécurisation est réglementairement définie et repose sur l'utilisation d'infrastructures qualifiées (cartes à puces, lecteurs et chiffrement de transport...) ;

- **les transmissions à caractère volontaire** comme l'externalisation du tiers-payant, dont la sécurisation repose sur le respect de la réglementation par le pharmacien lui-même ou le prestataire de service auquel il a recours. En effet, tout pharmacien peut faire appel à un organisme gestionnaire pour la gestion des rejets de tiers-payant. Les données transmises entre le pharmacien et cet organisme sont chiffrées et transitent par un réseau privé virtuel dédié.

Les modalités d'accès au réseau internet sont conditionnées par les conditions d'accès au réseau SESAM-Vitale définies réglementairement par la convention pharmaceutique qui laisse aux pharmaciens le libre choix de l'équipement informatique grâce auquel il établit les FSE et les transmet, conformément au cahier des charges SESAM-Vitale et dans la limite des équipements agréés par le comité national de dépôt et d'agrément.

Tout pharmacien peut donc librement choisir son fournisseur d'accès à internet. Pour cela, il peut avoir recours aux services d'un organisme concentrateur technique (OCT) qui agit pour le compte et sous la responsabilité du pharmacien¹¹³.

A.3.2.2.b Les protocoles réseaux

Le réseau Internet est un réseau informatique étendu de portée mondiale (type WAN ou *wide area network*) composé de réseaux publics et privés utilisant un ensemble standardisé de protocoles permettant le transfert de données au sein de cette toile. La norme « *open systems interconnexion* » (OSI) de l'ISO permet ainsi de décrire comment deux systèmes informatiques peuvent communiquer.

L'ensemble des protocoles utilisés pour le transfert de données sur internet est représenté par la suite TCP/IP (*transmission control protocol / internet protocol*) comportant plusieurs couches protocolaires. Lors de leur transmission électronique, les données sont formatées lors du passage des couches successives, constituant ainsi des paquets de données.

¹¹³ Dans le respect des dispositions légales et réglementaires ayant trait plus particulièrement à l'informatique et aux libertés, ainsi qu'à la confidentialité et à l'intégrité des FSE et des dispositions du cahier des charges OCT publié par le GIE SESAM-Vitale.

On distingue ainsi :

- **une couche applicative** qui assure l'interface entre les applications et constitue le point d'accès au réseau, au plus près de l'utilisateur. On y distingue des protocoles pour le transfert de fichiers (par exemple FTP), pour l'envoi (SMTP) ou la réception (POP3, IMAP¹¹⁴) de messages électroniques, pour la navigation sur internet (HTTP)...

- **une couche de transport** qui détermine l'ordre de transmission des données découpées en paquets, comme le protocole TCP ;

- **une couche internet** (protocole IP) gérant l'adressage et le routage des paquets de données ainsi que leur assemblage à la réception ;

- **une couche d'interface réseau** qui détermine la façon dont sont transportés les paquets de données et particulièrement leur tramage (ajout de séquences de bits particulières en début et en fin de chaque paquet de données permettant par exemple de renseigner la destination des paquets). Cette couche peut être associée à une dernière, la couche physique décrivant les caractéristiques physiques de la communication (câbles, fibres, ondes) et notamment les modalités de conversion des bits en signaux électrique ou optiques selon le type de ligne utilisée.

Au passage de chaque couche une information est ajoutée au paquet de données constituant un « en-tête » permettant de disposer de toutes les informations nécessaires à leur transmission, on parle d'encapsulation des données. A la réception, le système lit l'entête puis le supprime afin de restituer le message original.

Les deux principaux protocoles que nous retiendrons pour la suite sont :

- **le protocole HTTP** (*hypertext transfer protocol*) permettant un accès aux serveurs hébergeant des pages internet ;

- **le protocole SMTP** (*simple mail transfer protocol*) utilisé pour l'envoi de courriers électroniques. Il s'agit en réalité du protocole SMTP enrichi au format MIME (*multipurpose internet mail extensions*) permettant d'inclure une diversité de données plus étendue au message (notamment en termes de caractères de la table).

Les paquets de données transitant chaque seconde sur le réseau internet ne sont toutefois pas à l'abri d'une interception malintentionnée. Afin de préserver la confidentialité de ces données, il est possible d'appliquer des couches de sécurité supplémentaires, optionnelles, entre la couche application et la couche internet. Le protocole de transport HTTP peut ainsi être sécurisé (HTTPS) par l'utilisation des protocoles SSL (*secure sockets layer*) ou TLS (*transport layer security*) tout comme le protocole de transport SMTP peut l'être (SMTPS) à l'aide du protocole S/MIME.

Comme nous le verrons, ces protocoles permettant de sécuriser la transmission des données électroniques utilisent des méthodes cryptographiques basées sur l'utilisation de certificats électroniques.

¹¹⁴ Les protocoles POP3 et IMAP permettant la réception de courriers électroniques via une plateforme de messagerie. La différence entre ces deux protocoles réside dans la persistance des messages sur le serveur via le protocole IMAP permettant une consultation ultérieure avec différents *webmails*.

A.3.2.3 LE RESEAU SESAM-VITALE

Le réseau SESAM-Vitale est un réseau privé d'échanges entre le GIE SESAM-Vitale, les organismes d'assurance maladie obligatoire et complémentaire, les professionnels de santé et les industriels sous-traitants du GIE SESAM-Vitale. L'opérateur choisi par le GIE SESAM-Vitale est la société ATOS WORLDLINE, chargé d'assurer le transfert des flux électroniques vers les serveurs des organismes d'assurance maladie.

A.3.2.3.a Modalités d'accès

Comme nous l'avons vu, la convention pharmaceutique laisse aux professionnels de santé la liberté de choix de leur fournisseur d'accès à internet. Elle lui permet également de transmettre les FSE en se connectant à tout réseau pouvant communiquer avec le réseau SESAM-Vitale. La télétransmission de flux destinés à l'assurance maladie utilisant les protocoles SMTP et TCP/IP, toute officine adhérant au dispositif doit disposer d'un accès à internet. Pour cela les pharmaciens peuvent avoir recours :

- à un fournisseur d'accès internet grand public ou plus fréquemment à un réseau dédié réservé aux professionnels de santé qui proposent des offres spécialement conçues pour leur activité (messageries spécialisées, assistance...) ;
- à un organisme concentrateur technique (OCT) ¹¹⁵ proposant un service d'accès à internet ou utilisant les services d'un réseau existant et permettant d'assurer le regroupement, ainsi que l'éclatement des flux de télétransmission. Un OCT peut également proposer un service de réseau dédié.

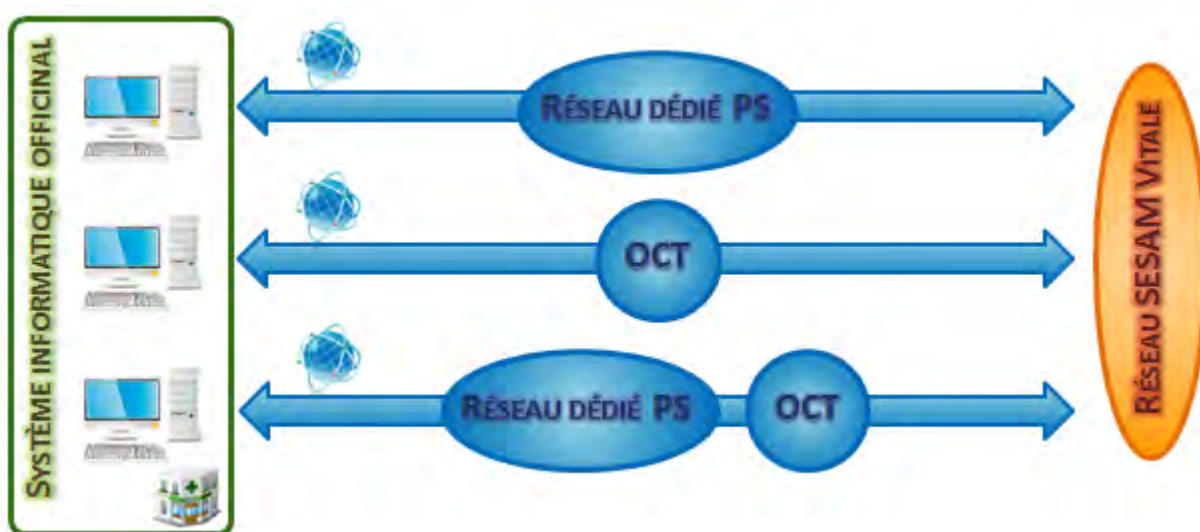


Figure 9 : Modalités d'accès au réseau SESAM-Vitale conformes au cahier des charges SESAM-Vitale 1.40.

¹¹⁵ La liste des OCT agréés est publiée par le GIE SESAM-Vitale sur son site internet à l'adresse : <http://www.SESAM-vitale.fr/>

A.3.2.3.b Modalités de télétransmission

Le réseau SESAM-Vitale propose un ensemble d'infrastructures sécurisées permettant d'orienter les flux électroniques entre les professionnels de santé et les organismes d'assurance maladie. On distingue :

- **Des flux de feuilles de soins électronique (FSE) ;**
- **Des flux de demandes de remboursement électronique (DRE) et de DRE d'annulation ou rectificative ¹¹⁶ ;**
- **Des flux de pièces justificatives ;**
- **Des flux de mise à jour des cartes Vitale ;**
- **Des flux retours des organismes d'assurance maladie aux professionnels de santé.**

Les pharmaciens d'officine utilisent quotidiennement certaines de ces infrastructures et notamment :

- **une plateforme de messagerie** permettant de télétransmettre les factures électroniques (FSE et/ou DRE) vers les frontaux de facturation (serveurs d'accueil des flux) des organismes d'assurance maladie. Un volume total de flux de 2 272 Go fut ainsi traité par cette infrastructure en 2011 (27);

- **un portail de mise à jour des cartes Vitale** qui est une infrastructure utilisée pour assurer la mise à jour des cartes au moyen des bornes disponibles en officine. Cette infrastructure communique avec les organismes d'assurance maladie via les frontaux CAC (chaîne d'administration des cartes).

Une plateforme nationale mutualisée unique ou PAIR (point d'accueil inter-régimes) permet de recueillir les pièces justificatives numérisées en provenance des officines afin de les transmettre aux organismes d'assurance maladie obligatoire. Dans l'attente de la généralisation de leur télétransmission, ainsi qu'en cas de dysfonctionnement de ce service, le pharmacien peut transmettre les pièces justificatives numériques en les reproduisant sur un CD-ROM non réinscriptible et unique pour l'ensemble des régimes, qui est ramassé périodiquement.

A.3.3. L'INTEROPERABILITE DES SYSTEMES INFORMATISES DE SANTE

Afin d'échanger, communiquer et se comprendre, les différents systèmes doivent utiliser des langages communs. L'utilisation du même vocabulaire et des mêmes procédures d'échange par les systèmes d'information est, par analogie, une réponse pour favoriser leur communication. L'utilisation de normes et standards internationaux pour faciliter les échanges entre systèmes d'information est un moyen de surmonter les obstacles techniques qui surviennent lorsque différents groupes se rassemblent, chacun avec une large base d'utilisateurs partageant des systèmes bien établis entre eux mais mutuellement incompatibles (61). L'interopérabilité représente ainsi la **capacité qu'ont plusieurs systèmes d'échanger de l'information entre eux et d'utiliser l'information qui a été échangée**. Le développement de l'administration en ligne ayant profondément bouleversé les relations entre

¹¹⁶ Lorsqu'un professionnel de santé souhaite annuler ou modifier une DRE.

les usagers et les autorités administratives, l'interopérabilité est devenue une composante incontournable pour l'épanouissement des systèmes informatisés de santé.

Un échange réussi entre système informatisé fait intervenir différents niveaux d'interopérabilité et particulièrement (62) :

- **l'interopérabilité sémantique** ou « savoir se comprendre » traite du sens des informations et se distingue en cela du niveau syntaxique relatif à la façon dont les données sont codées et formatées ;

- **l'interopérabilité syntaxique** ou « savoir communiquer » traduit quant à elle le sens en symboles. Il existe entre interopérabilités sémantique et syntaxique le même rapport qu'entre le fond et la forme ;

- **l'interopérabilité technique** ou « pouvoir communiquer » définit les paramètres de transmission des informations définies au niveau sémantique et mises en forme au niveau syntaxique.

Tout comme elle introduit le principe d'un référentiel général de sécurité, l'ordonnance du 8 décembre 2005 apporte la notion de référentiel général d'interopérabilité « *dont l'objet est de fixer les règles techniques permettant d'assurer l'interopérabilité de tout ensemble de moyens destinés à élaborer, traiter, stocker ou transmettre des informations faisant l'objet d'échanges par voie électronique avec une autorité administrative* ». Il s'appuie sur le développement de normes et de standards communs aux différents systèmes amenés à fonctionner de manière collaborative. Lorsque les systèmes émetteur et récepteur partagent un langage commun pour chaque couche de la norme OSI, l'interopérabilité est assurée.

A.3.3.1 INTERETS DE LA STRUCTURATION ET DU CODAGE DES DONNEES DE SANTE

Le degré de structuration et de codage des données exploitées ou échangées par différents systèmes conditionne directement leurs possibilités de traitement. Les données contenues par le dossier informatisé d'un patient ne sont cependant pas toutes exprimées de façon normalisée ou codée car ce mode de recueil et de représentation de l'information n'est pas naturel pour les professionnels de santé qui préfèrent bien souvent s'exprimer librement. Il est donc nécessaire de trouver un équilibre entre les données non structurées permettant aux professionnels de santé de s'exprimer avec toute la subtilité que requiert le jargon médical, et les données structurées ou codées facilitant l'interopérabilité et conférant une certaine valeur ajoutée aux dossiers informatisés.

La possibilité d'échanger des données au sein des systèmes d'information de santé est fondamentale puisqu'elle conditionne la bonne **coordination des soins et le suivi des patients**. Le cadre d'interopérabilité des systèmes d'information de santé (CI-SIS) développé par l'ASIP Santé permet ainsi de définir les conditions d'une interopérabilité reproductible et efficiente entre les systèmes, dans le respect des exigences de sécurité et de confidentialité des données personnelles de santé. Ce référentiel à destination des éditeurs de logiciels spécifie les standards (le plus souvent internationaux) à utiliser dans les échanges et lors du partage de données de santé. Dans ce domaine, l'ASIP Santé possède un rôle incontournable puisque l'agence est un acteur majeur de l'organisation IHE (*integrating the healthcare enterprise*) dont elle adapte les profils d'intégration au contexte français.

Un profil d'intégration IHE se présente comme un guide de mise en œuvre de normes, standards et bonnes pratiques au service d'un objectif de traitement coopératif impliquant plusieurs systèmes et s'appuyant sur le partage ou l'échange de données de santé (61). Les profils IHE présentent de nombreux avantages et proposent des spécifications en faveur de l'interopérabilité des systèmes en s'appuyant sur des normes et standards internationaux conformes au référentiel général d'interopérabilité.

Le développement d'un cadre d'interopérabilité favorisant la coordination entre les différents acteurs ne doit cependant pas déroger aux grands principes du traitement des données. Encourager le développement de l'interopérabilité des systèmes d'information de santé est l'une des missions majeures de l'ASIP Santé. Dans ce contexte, les systèmes d'information du domaine de la santé, principaux vecteurs des échanges de données électroniques des patients, doivent adapter leurs propres capacités d'ouverture et de communication.

A.3.3.2 INTEROPERABILITES SEMANTIQUE ET SYNTAXIQUE

L'interopérabilité sémantique doit permettre de définir le vocabulaire commun qui sera utilisé par les différents systèmes pour l'expression des données mais encore, de réaliser une mise en correspondance de données entre deux langues différentes via des tables et des nomenclatures¹¹⁷.

Dans la continuité des travaux menés par la Haute Autorité de santé pour la certification des logiciels d'aide à la prescription, il apparaît désormais nécessaire d'assurer une correspondance sans faille entre les données de prescription et les données d'identification des produits de santé en vigueur. La normalisation de l'expression des données relatives aux pathologies et aux médicaments constitue donc un point incontournable pour le développement de tout système d'e-santé.

L'enjeu principal de l'interopérabilité sémantique des systèmes d'information consiste à définir un référentiel définissant les règles d'émission, de réception et d'interprétation des informations échangées, non seulement par une personne, mais encore par une machine (3).

Les différentes recommandations du référentiel général d'interopérabilité permettent de faciliter l'interopérabilité syntaxique, c'est-à-dire la façon dont sont codées et formatées les données par les différents systèmes. La syntaxe de l'information est interprétable par les systèmes émetteur et récepteur car elles sont conformes à un modèle d'observation ou « *template* » paramétrable. Ce modèle comprend la désignation d'un paramètre par exemple « dosage », sa valeur et son unité. La couche « contenu » du CI-SIS contient ainsi des modèles de documents (observations cliniques, résultats biologiques, posologie d'un traitement...) et les terminologies de référence utilisées pour leur codage comme la classification commune des actes médicaux (CCAM) et la classification anatomique thérapeutique et chimique (ATC) des médicaments...

Les normes et standards applicables doivent ainsi considérer différents paramètres de mise en forme syntaxique comme :

- le codage des caractères au format UTF-8 (*UCS transformation format 8 bits*), extension du code ASCII où chaque caractère est codé par une suite de un à quatre octets ;

¹¹⁷ Cette composante est primordiale pour assurer une bonne compréhension d'un vocabulaire très spécialisé entre deux professionnels de santé ne parlant pas la même langue, compte tenu de l'expansion et de l'interconnexion des systèmes d'information de santé à l'échelle européenne.

- le choix des polices de caractères à utiliser devant être supportées nativement par toutes les plates-formes (arial, courier, times new roman, verdana...) ;
- l'exportation de base de données et l'échange de documents structurés au format XML ;
- les méthodes de compression des fichiers à réaliser de préférence au format ZIP car il est très répandu¹¹⁸, sous licence ouverte et supporté nativement par les principaux systèmes informatiques...

D'un point de vue technique l'utilisation de différentes normes et standards recommandés par le référentiel permettent de garantir l'interopérabilité des systèmes. Les modèles d'informations échangées peuvent être traduits en différents langages informatiques, notamment le langage XML dont de nombreux schémas sont disponibles tel que le schéma **HL7** pour les données de santé. Cette norme développée par l'organisation **Health Level 7** permet de définir un ensemble de spécifications techniques pour les échanges informatisés de données entre système d'informations. De nombreuses versions et implémentations du standard HL7 sont actuellement disponibles : HL7 version 2.0, HL7 version 3.0, ou encore HL7 CDA R2 (*clinical document architecture release 2*)... Il s'agit donc de langages informatiques en syntaxe XML (*extensible markup language*) permettant de faciliter l'échange automatisé de contenus complexes entre des systèmes d'information hétérogènes.

D'autres organismes de standardisation tels qu'IHTSDO¹¹⁹ ou l'Organisation mondiale de la santé, proposent des terminologies utilisées pour coder les données de santé au sein des systèmes d'information comme SNOMED CT ou LOINC.

A.3.3.3 L'INTEROPERABILITE TECHNIQUE

L'interopérabilité technique vise à définir des formats informatiques communs afin d'interconnecter les différents logiciels du marché et échanger des données. Les recommandations du référentiel portent donc principalement sur :

- **les messageries électroniques** dont les protocoles de transport permettent, comme nous l'avons vu de véhiculer (SMTP, MIME, POP3, IMAP4) et sécuriser (S/MIME) des courriers électroniques ;
- **les protocoles réseaux** et notamment IPv4 déployé universellement pour la couche internet et associé au protocole de transport TCP ;
- **les protocoles « client-serveur » de la couche applicative** comme HTTP 1.1 pour le transfert de fichiers (HTML, CSS, PHP...) avec un navigateur web lorsqu'un utilisateur consulte un site web éventuellement sécurisé par les protocoles TLS ou SSL ;
- **les services web**, programmes informatiques en ligne permettant l'échange de données entre des applications de systèmes hétérogènes devant supporter des interactions et des échanges de données normalisées. Le protocole SOAP (*simple objet access protocol*) permet ainsi de définir les mécanismes d'échanges d'information structurée et assure le dialogue entre ses systèmes en utilisant la notation XML. Si le transport de données est le plus souvent réalisé à l'aide du protocole HTTP, SOAP reste indépendant du protocole de transport et autorise ainsi l'emploi d'autres protocoles comme SMTP ;

¹¹⁸ Le format ZIP fut créé en 1989 par la société PKWARE, pionnier en matière de compression des données.

¹¹⁹ *International health terminology standards development organization.*

- **les messageries instantanées** permettant de communiquer avec un correspondant connecté au même réseau informatique dont le protocole XMPP (*extensible messaging and presence protocol*) basé sur une architecture client/serveur, permet les échanges décentralisés de messages de manière instantanée ou non entre les clients. Les flux de données transmis par le protocole XMPP sont au format XML ce qui lui offre de larges perspectives d'extension et d'implémentation dans des environnements très divers. Comme nous le verrons lors de l'étude des messageries sécurisées de santé, ce service peut être sécurisé par le protocole TLS.

A.3.4. LA SECURITE DU SYSTEME INFORMATIQUE OFFICINAL

Si l'informatique fournit une aide si précieuse qu'elle en devient presque indispensable, l'hébergement et la transmission de données électroniques n'est pas dénué de risques. Il est donc nécessaire de mettre en œuvre un ensemble de moyens techniques, organisationnels, juridiques et humains afin de réduire la vulnérabilité du système informatique contre des menaces accidentelles ou intentionnelles. Sécuriser les locaux et les matériels apparaît donc tout aussi important que les moyens logiciels utilisés pour protéger les données.

Par ailleurs, la multiplication des ordinateurs portables, des clés USB et des *smartphones* rend indispensable l'anticipation d'une possible perte d'informations consécutive au vol ou à la perte d'un tel équipement. Afin de sécuriser l'informatique mobile, la CNIL recommande d'ailleurs de prévoir des moyens de chiffrement des données afin qu'elles ne puissent être consultées par un tiers non autorisé.

En adoptant une démarche de sécurisation du système informatique officinal conformément aux recommandations de la CNIL et du Conseil de l'ordre, les pharmaciens disposent de tous les éléments pour assurer l'hébergement et la transmission de données sensibles en toute sécurité.

A.3.4.1 LA DEMARCHE DE SECURISATION DU SYSTEME INFORMATIQUE OFFICINAL

Le panel d'outils numériques utilisés au quotidien par les pharmaciens d'officine permet de constituer de larges bases de données sensibles imposant la mise en œuvre quotidienne de moyens adaptés afin d'en préserver la confidentialité. Les risques d'intrusions dans les systèmes informatiques ne sont en effet pas négligeables et peuvent conduire à l'implantation de virus ou de programmes espions.

En prévenant les tentatives d'accès frauduleux, l'exécution de virus ou encore la prise de contrôle à distance du système (notamment via Internet), la mise en œuvre d'une démarche de sécurisation du système informatique officinal vise à analyser les risques, établir une politique de sécurité et mettre en application des techniques de sécurisation adaptées. C'est avec cette volonté d'assurer la confidentialité des données de santé détenues par les professionnels de santé que la CNIL a publié dès 2010 un guide destiné aux professionnels de santé couplé à un guide sur la sécurisation des données leur détaillant les moyens à mettre en œuvre au quotidien afin d'assurer ces fonctions (15) (63).

Plus récemment, en janvier 2013, le Conseil national de l'ordre des pharmaciens a publié un guide de recommandations relatives au « *respect de la confidentialité des données de patients dans l'usage de l'informatique* » destiné à l'application officinale, identifiant les démarches de sécurisation du système informatique à mettre en œuvre (10).

• **L'analyse des risques** consiste à identifier et quantifier les risques liés à la sécurité du système informatique (potentialité, impacts, effets, conséquences, gravité) et les causes associées. Cette analyse passe par une succession d'étapes :

- le recensement des fichiers de données à caractère personnel ainsi que les traitements associés ;

- l'identification des supports matériels, logiciels et les infrastructures de communication ;

- la détermination des atteintes possibles classées selon leur gravité et leur mode de traitement¹²⁰ ;

- l'étude des risques en fonction du type de menace (vol, matériel, contagion par un virus...) et leur hiérarchisation selon leur impact et leur probabilité d'occurrence ;

- la détermination des mesures de sécurité à mettre en œuvre pour anticiper, éviter ou détourner les risques.

• Etablir **une politique de sécurité** vise à élaborer les règles et procédures pour pallier les risques identifiés, définir les actions à entreprendre et enfin sensibiliser les utilisateurs aux problèmes liés à la sécurité du système informatique tout en précisant les rôles et responsabilités de chacun.

• **Les techniques de sécurisation** du système informatique officinal doivent ainsi prendre en compte les actions définies par la politique de sécurité.

Elles visent à assurer :

- la sécurité des données (chiffrement, intégrité, contrôle d'accès, authentification...) ;

- la sécurité du réseau (pare-feu, système de détection d'intrusion) ;

- la surveillance des informations de sécurité ;

- la formation des utilisateurs ;

- l'audit de vulnérabilités par des tests d'intrusion.

A.3.4.2 MISE EN ŒUVRE D'UNE POLITIQUE DE SECURITE

La gestion des moyens visant à assurer la sécurité des données se base sur des exigences fondamentales, véritables critères d'évaluation du niveau de sécurité d'un système informatique. Toute politique de sécurité du système informatique doit donc veiller à assurer la disponibilité, l'intégrité et la confidentialité des données ainsi que la traçabilité et la non-répudiation de l'information (10).

• **La sécurisation des locaux et des matériels** est le point de départ de la sécurisation de tout système informatique. Le tableau ci-dessous présente les différents niveaux d'action possibles pour limiter les risques de vols ou de dégradation des matériels.

¹²⁰ Par exemple, une atteinte à la confidentialité peut consister en l'usurpation d'identité ou encore une atteinte à l'intégrité en une modification d'un fichier afin d'accuser quelqu'un à tort...

LA SECURITE DES LOCAUX ET DES MATERIELS	
LA SECURITE PHYSIQUE DES LOCAUX CONTENANT DES DONNEES SENSIBLES	
IDENTIFICATION DES RISQUES	MESURES A METTRE EN ŒUVRE
Intrusion	Alarmes
Accès par un personnel non autorisé	Limitation d'accès aux locaux
Incendie	Dispositif anti-incendie (alarmes, extincteurs...)
Inondation	Panneaux anti-inondation, surélévation du matériel
Panne du climatiseur	Détecteurs de température
LA SECURITE DU MATERIEL ET DU CABLAGE	
IDENTIFICATION DES RISQUES	MESURES A METTRE EN ŒUVRE
Perte d'alimentation	Système de secours électrique (onduleur)
Surchauffe	Climatisation
Pannes	Contrat de maintenance

Tableau 13 : La sécurité des locaux et des matériels : identification des risques et mesures à mettre en œuvre (10).

- **La sécurisation des postes de travail informatiques**, des systèmes d'exploitation et des logiciels vise à protéger l'accès et l'intégrité des données confidentielles sauvegardées.

LA SECURITE DU POSTE DE TRAVAIL INFORMATIQUE, DU SYSTEME D'EXPLOITATION ET DES LOGICIELS	
IDENTIFICATION DES RISQUES	MESURES A METTRE EN ŒUVRE
Tentative d'accès frauduleux	• Etablir des niveaux d'accès selon les métiers et les fonctions et établir la notion d'administrateur, seul détenteur du droit à l'installation de logiciels et des matériels et à l'accès à tous les fichiers. L'accès à ce compte administrateur doit être protégé par un couple (identifiant/mot de passe). • Etablir et respecter les règles de connexion et déconnexion du poste de travail. • Exiger la possibilité de visualiser l'historique des connexions ou de modifications effectuées.
Exécution d'un virus	• Utiliser un logiciel anti-virus mis à jour régulièrement. • Installer un pare-feu¹²¹ • Limiter les actions sur chaque poste de travail au strict nécessaire pour assurer l'activité de poste.
Prise de contrôle à distance	• Installer un pare-feu
Pannes matérielles	• Contrat de maintenance • Service après-vente

¹²¹ Un pare-feu ou *firewall* est un programme permettant de protéger un ordinateur connecté à un réseau local ou à internet de messages provenant de domaines interdits (sites de commerce) ou d'attaques externes (filtrage entrant) et de connexion illégitimes vers l'extérieur (filtrage sortant), initialisés par des programmes ou personnes. Il protège ainsi des intrusions, de l'infection et la propagation de certains virus, vers et chevaux de Troie informatiques.

Existence de failles de sécurité dues à l'interfaçage des logiciels	• Utiliser des outils de détection des vulnérabilités pour détecter les failles de sécurité. • Harmoniser les logiciels pour faciliter les interfaces. • Effectuer régulièrement les mises à jour des logiciels et du système d'exploitation afin d'acquérir les corrections de failles de sécurité.
Accès frauduleux à des logiciels supportés par des serveurs nécessitant l'utilisation de navigateurs internet et d'hébergeurs	• Renforcer les mesures de sécurité dans le cas des serveurs.

Tableau 14 : La sécurité du poste de travail informatique, du système d'exploitation et des logiciels : identification des risques et mesures à mettre en œuvre (10).

- **La sécurisation de l'accès aux données personnelles** doit garantir un accès limité au professionnel de santé responsable du traitement ou à un confrère désigné par le patient, au patient, à ses ayants-droits en cas de décès, à l'autorité parentale, au tuteur ou encore un tiers de confiance.

Les risques identifiés concernent :

- l'accès aux données de santé par un tiers non autorisé ;
- l'accès à des données sensibles sans rapport avec l'activité de l'utilisateur ;
- la connexion avec le code d'un autre utilisateur (usurpation d'identité).

Les mesures susceptibles de prévenir les risques d'accès aux données sensibles consistent ainsi à :

- **sécuriser l'accès aux données sensibles** par un processus d'identification voire d'authentification. Comme nous le verrons, l'authentification consiste à apporter la preuve d'une identité. Elle peut être mise en œuvre à l'aide d'une politique de mot de passe sécurisés, uniques et non utilisables simultanément, ou encore par l'utilisation de la carte CPS et son certificat électronique d'authentification. La mise en œuvre d'une politique de contrôle d'accès permet de définir des niveaux d'accès aux données par les utilisateurs, dans les limites de leurs fonctions et selon la finalité du traitement.

Certaines règles concernant l'élaboration et la gestion des mots de passe doivent également être respectées. Il doit contenir si possible huit caractères différents (combinant des caractères spéciaux, numériques, alphabétiques en minuscules et majuscules) sans utiliser de suite logique (1234, abcd, azerty...) et ne doit pas contenir d'information personnelle (date, ville de naissance...). Un mot de passe doit être réservé à une utilisation précise et doit être renouvelé régulièrement (en général tous les trois mois). Un système permettant de bloquer l'accès après trois tentatives de connexions infructueuses doit permettre de limiter les risques d'usurpation d'identité par recherche exhaustive des données d'authentification.

- **déterminer les règles de connexions et de déconnexions des utilisateurs** par une politique d'horodatage attestant de l'existence d'une donnée à un instant précis ou de la date

d'un acte réalisé par voie électronique¹²². D'autres mesures peuvent être mises en œuvre comme l'impossibilité de se connecter avec le même identifiant ou mot de passe sur plusieurs postes au même moment, la limitation du nombre de tentatives d'accès, la déconnexion automatique de l'utilisateur en cas d'inactivité pendant une certaine durée...

- **formaliser par une procédure la création et le blocage d'accès des comptes informatiques** en cas d'enrôlement ou de suppression d'un utilisateur ou de perte d'habilitation.

- **signer un engagement de confidentialité** pour les non-professionnels de santé ou prévoir une clause de confidentialité dans le contrat de travail.

- **faire adhérer les utilisateurs à ces règles** de base en les sensibilisant à la sécurité des systèmes d'information par des formations spécifiques et en rédigeant une charte informatique rappelant les règles de base à respecter afin d'assurer la confidentialité des données sensibles appliquées à l'officine.

- **tenir à la disposition des patients la liste des personnes habilitées** à effectuer le traitement de données personnelles au sein de l'officine ainsi que les finalités et les destinataires potentiels de ces données.

- **La sécurisation des données stockées, sauvegardées et archivées** s'inscrit dans le cadre de la mise en œuvre de la politique de sécurité de tout hébergeur de données de santé. Afin d'éviter une perte, une indisponibilité ou un accès non autorisé, il est donc nécessaire de sécuriser les données sauvegardées et archivées soit :

- en les stockant sur un support de données distinct conservé dans un lieu sécurisé, à distance du lieu d'exercice ;

- en procédant au chiffrement des données au moyen de logiciels cryptographiques disponibles gratuitement comme TrueCrypt¹²³ ou PGP¹²⁴ ;

- en limitant les droits d'accès aux sauvegardes et aux archives.

- **La destruction** (volontaire) de données électroniques mise en œuvre par exemple lors du renouvellement du matériel informatique doit être réalisée par destruction physique¹²⁵ des supports de stockage ou effacement par réécriture avec un logiciel dédié. Avant destruction, il est nécessaire de s'assurer de la récupération des données afin de respecter les durées légales d'archivage. Lorsqu'elle est mise en œuvre par une SSII, celle-ci doit remettre un document au pharmacien attestant de la méthode de destruction des supports ou de l'effacement des données. En effet, ces matériels informatiques obsolètes ne bénéficient d'aucune filière de recyclage adaptée à la protection des données qu'ils sont susceptibles de contenir de sorte que l'on puisse craindre au fur et à mesure du renouvellement des équipements que des données de santé ne se diffusent au-delà des personnes initialement autorisées à y accéder (6).

¹²² Décret n° 2011-434 du 20 avril 2011 relatif à l'horodatage des courriers expédiés ou reçus par voie électronique pour la conclusion ou l'exécution d'un contrat, JORF n°0094 du 21 avril 2011.

¹²³ TrueCrypt permet de créer un disque virtuel encrypté dont l'accès nécessite un mot de passe.

¹²⁴ PGP ou « *Pretty good privacy* » permet de créer une paire de clés cryptographiques (publique et privée). Les signatures effectuées avec la clé privée peuvent être vérifiées en utilisant la clé publique correspondante, et les messages chiffrés utilisant la clé publique sont déchiffrables en utilisant la clé privée correspondante.

¹²⁵ Par écrasement, incinération ou torsion des disques durs, broyage des CD ou DVD. Par démagnétisation pour certaines unités de stockage.

Enfin, dans le cas particulier d'une fermeture d'officine, l'article R.5125-30 du code de la santé publique prévoit que « *le titulaire de celle-ci remet l'ordonnancier à un pharmacien qu'il désigne au conseil régional de l'ordre dont il relève* » ou à défaut de désignation « *au pharmacien le plus proche proposé par ledit conseil* ».

• **La maintenance** du système informatique par les SSII doit être de nature à préserver la confidentialité des données stockées. Ainsi, dans tout contrat avec une SSII, il est nécessaire de prévoir :

- une clause prévoyant qu'aucune intervention ne peut être entreprise sans l'accord préalable du pharmacien ;
- une clause de confidentialité sur les données personnelles des patients ;
- une demande de rapport détaillé pour chaque intervention ;
- la possibilité de réaliser une traçabilité des interventions avec le système de journalisation ;
- la possibilité de visualisation à l'écran des manipulations effectuées lors d'une prise de contrôle du système à distance par l'intervenant ;
- un rapport de destruction des supports de données ;
- le chiffrement des données transmises.

• **La traçabilité** des données consiste à suivre l'acheminement de l'information avec la possibilité de mener des analyses ou « journal des traces » devant être consulté régulièrement. La traçabilité peut donc permettre d'identifier un accès frauduleux ou une utilisation abusive des données personnelles tout en enregistrant les activités de chaque utilisateur et les événements liés : connexions, tentatives de connexion, accès aux données, actions réalisées (ajout, modification, suppression). Ce processus de **journalisation** des accès pour chaque identifiant avec les dates et heures de connexion et déconnexion et des actions menées nécessite toutefois une bonne synchronisation des horloges des différents systèmes de traitement.

• **La sécurisation des réseaux et de l'accès à internet** est une composante fondamentale assurant la confidentialité des données télétransmises. Si l'utilisation de la carte CPS est obligatoire pour préserver la confidentialité de données transmises électroniquement par chiffrement, la sous-traitance de la transmission à un prestataire tiers n'est pas dénuée de risque. Les cyber-menaces sont désormais nombreuses et quotidiennes et les solutions à apporter parfois complexes. Certaines mesures permettent ainsi aux professionnels de santé de se protéger notamment contre l'infection et la propagation éventuelle de virus, vers et chevaux de Troie informatiques mais encore contre une usurpation d'identité ou contre tout accès, vol ou détournement illicite de données confidentielles.

Sécuriser l'accès à internet passe avant tout par l'utilisation d'un pare-feu couplé à un antivirus régulièrement mis à jour mais encore par certaines précautions supplémentaires permettant d'atteindre un niveau de sécurité plus élevé comme :

- restreindre la connexion à internet aux utilisateurs autorisés et limiter les flux au strict minimum ;

- installer un système de détection d'intrusion s'il n'est pas inclus dans le logiciel antivirus ;
- ne jamais utiliser un compte administrateur pour la navigation sur internet ;
- utiliser le protocole WPA pour les connexions au Wi-Fi offrant une meilleure sécurité que le protocole WEP encore souvent utilisé ;
- procéder au chiffrement des données confidentielles échangées.

A.3.5. LA SECURITE DES ECHANGES DEMATERIALISES

Le caractère hautement confidentiel des données de santé implique une mise en œuvre de moyens élaborés afin d'en assurer la sécurité. Il s'agit à la fois de sécuriser l'accès et le contenu de données hébergées ou télétransmises électroniquement mais encore d'assurer une identification précise, voire une authentification des utilisateurs des systèmes d'information.

Comme nous l'avons vu, l'usage de la carte CPS est obligatoire afin d'accéder à des informations médicales personnelles ou de les partager par voie électronique. Celle-ci est en effet dotée d'un coprocesseur cryptographique permettant d'assurer des fonctions de sécurité cryptographiques conformément aux conditions prévues par le référentiel général de sécurité.

Traditionnellement qualifiée de « science du secret », la **cryptologie** peut être divisée en deux branches : la **cryptographie** qui étudie les mécanismes permettant d'assurer des propriétés de sécurité et la **cryptanalyse** qui analyse ces fonctions de sécurité, voire de les mettre en défaut. Cette discipline ne date pas d'hier puisque le plus vieux document chiffré connu fut retrouvé en Irak et daterait du XVIème siècle av. J-C¹²⁶. A la frontière entre informatique et mathématiques, la **cryptologie moderne** est un outil incontournable pour sécuriser les systèmes d'information utilisant des mécanismes cryptographiques au moyen de supports tels que les cartes à puce. Des méthodes cryptographiques utilisant des clés de chiffrement sont donc utilisées afin de garantir la mise en œuvre de **fonctions de sécurité** destinées à assurer la confidentialité, l'intégrité et la non-répudiation d'une correspondance, ainsi que l'identification et l'authentification des correspondants (1).

En résumé, l'utilisation de techniques cryptographiques permet d'assurer les fonctions de sécurité suivantes :

- le chiffrement de données les rendant inintelligibles ;
- l'authentification d'une entité (personne ou machine) ;
- la signature électronique (combinant l'authentification des correspondants, l'analyse de l'intégrité de données et la non-répudiation d'une correspondance).

Comme nous le verrons, la mise en œuvre de ces fonctions est assurée par l'utilisation de certificats électroniques. En combinant l'utilisation combinée de différents types de certificats électroniques, il est possible de mettre en œuvre l'ensemble de ces fonctions de sécurité lors d'une même correspondance.

¹²⁶ Il s'agissait d'une tablette d'argile sur laquelle était gravée une recette secrète chiffrée en supprimant les consonnes et en modifiant l'orthographe des mots.

A.3.5.1 CONFIDENTIALITE ET CHIFFREMENT

Le but de la **confidentialité** est de s'assurer que des informations transmises ou stockées ne sont accessibles qu'aux personnes autorisées à en prendre connaissance. Cet objectif de sécurité est classiquement assuré par le chiffrement mais peut bien entendu également l'être par tout autre moyen approprié à commencer par des mesures organisationnelles non cryptographiques. La confidentialité des informations peut aussi être protégée par des mesures complémentaires de gestion des droits d'accès de chacun, en lecture, en écriture ou en modification, aux données contenues dans le système d'information (64).

Chiffrer un message, c'est lui appliquer une fonction de transformation (un algorithme mathématique de chiffrement) personnalisée, c'est-à-dire rendue unique par l'application d'un paramètre (clé cryptographique) partagé par deux correspondants, le rendant illisible au tout-venant ne partageant pas le secret permettant de réaliser l'opération inverse de déchiffrement.

Le chiffrement utilise des procédés cryptographiques appliquant des algorithmes garantissant la confidentialité des données ainsi cryptées contre toute personne ne possédant pas la clé de déchiffrement. Il s'agit du mécanisme essentiel de protection de la confidentialité. Dans tous les cas, les mécanismes de chiffrement et les mécanismes techniques de gestion des droits d'accès, dès lors qu'ils font appel à des mécanismes cryptographiques, doivent respecter les exigences du référentiel général de sécurité.

Le chiffrement d'une donnée électronique consiste à modifier la suite d'octets qui la constitue au moyen d'algorithmes mathématiques la rendant incompréhensible. Ces algorithmes étant connus de tous, un paramètre supplémentaire appelé **clé** est nécessaire afin que les seuls possesseurs de la clé appropriée puissent déchiffrer les données.

Il existe ainsi deux méthodes principales de chiffrement :

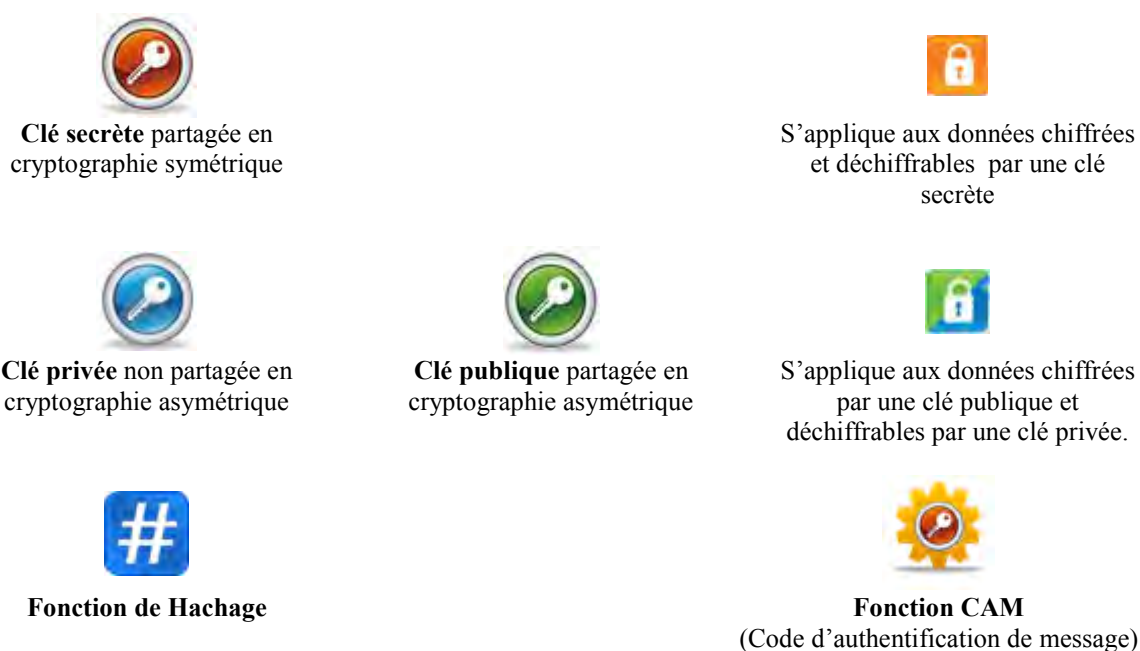
- **Le chiffrement symétrique** ou cryptographie à **clé secrète** où une même clé permet de chiffrer et déchiffrer les informations ;

- **Le chiffrement asymétrique** qui utilise des **paires de clés (ou bi-clés)**, l'une **publique et l'autre privée**. La clé privée que seul un utilisateur possède est utilisée pour les opérations privées tandis que la clé publique peut être connue de tous afin de réaliser les opérations publiques.

Cette séparation est issue de l'article fondateur de W. Diffie et M. Hellman¹²⁷ qui, en 1976, a donné naissance à la cryptographie asymétrique en suggérant que pour chiffrer un message à l'attention d'un destinataire donné il n'est pas nécessaire de partager au préalable un secret avec lui.

¹²⁷ Whitfield Diffie et Martin Hellman. *New directions in cryptography*. IEEE Transactions on Information Theory, 1976.

Pour une meilleure compréhension de ces mécanismes nous définirons symboliquement :



A.3.5.1.a Méthodes de chiffrement symétrique

Les deux entités souhaitant échanger des données confidentielles disposent tous les deux d'une clé identique appelée par convention « clé secrète ». Elle permet à l'émetteur de chiffrer des données et au récepteur de les déchiffrer au moyen d'un secret partagé : la clé secrète. Cette clé est une suite quelconque de bits (0 et 1) de taille (n) déterminée, conditionnant le niveau de sécurité du système. Il est ainsi possible de former 2^n clés de longueur n et une attaque par « recherche exhaustive » consistant à énumérer toutes les clés possibles ne pourra aboutir qu'à l'aide de moyens informatiques capables d'effectuer de telles opérations¹²⁸.

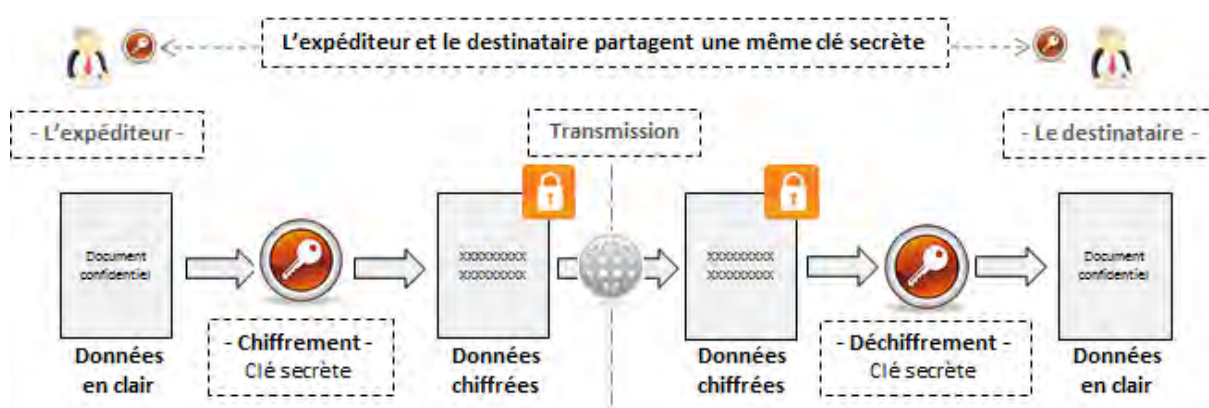


Figure 10 : Principe du chiffrement symétrique à clé secrète.

Cette méthode aussi appelée « chiffrement conventionnel », assure la confidentialité des données car en cas d'interception du message, celui-ci ne pourra pas être déchiffré sans avoir eu connaissance de la clé secrète. En revanche, cette méthode ne permet pas d'assurer

¹²⁸ Le référentiel général de sécurité précise que 2^{46} opérations par jour peuvent être effectuées à l'aide d'un système informatique d'une puissance d'1 GHz (1 milliard d'opérations par seconde). Il faudrait 15 milliards d'années pour effectuer 2^{90} opérations dans ces mêmes conditions. Il est admis en cryptographie qu'il ne sera jamais possible d'effectuer 2^{256} calculs de ce type.

l'identification ou l'authentification des correspondants sauf si l'on considère qu'ils sont les seuls à disposer de la clé secrète.

Ce système à une seule clé présente cependant certains inconvénients :

- la clé secrète unique doit être communiquée au destinataire en toute sécurité sans utiliser le média à sécuriser ;
- il nécessite autant de paires de clés que de couples de correspondants (ou bien tout le monde doit avoir connaissance de la clé secrète);
- il ne peut empêcher le correspondant de chiffrer un message avec la même clé usurpant ainsi son identité.

La principale difficulté dans la gestion des clés secrètes réside dans la **distribution**, des clés aux différents correspondants afin de partager les mêmes secrets initiaux sans qu'un attaquant potentiel ne puisse l'intercepter. Ceci peut être réalisé à l'aide de méthodes organisationnelles dont la criticité peut constituer une faille non négligeable de ce système ou au moyen de techniques cryptographiques asymétriques.

Afin de permettre à un groupe d'individu souhaitant s'authentifier mutuellement par des techniques symétriques il est donc possible :

- soit de prévoir autant de clés que de paires d'individus ;
- soit de donner la même clé à tous les individus.

Cependant, dès lors que l'on souhaite ajouter un nouveau membre, cette dernière solution devient impossible. Il convient alors d'attribuer à chaque membre du groupe un bi-clé dont la clé publique est certifiée.

Afin de protéger une clé secrète lors de son **stockage** il est possible de la chiffrer à l'aide d'une autre clé non partagée. Certaines clés peuvent ainsi être stockées de manière chiffrées ou « en clair ».

Il existe deux méthodes de chiffrement symétrique parmi lesquelles on distingue le **chiffrement par bloc** utilisant un algorithme mathématique traitant les données à chiffrer par blocs de taille fixe (typiquement 64 ou 128 bits). Un tel mécanisme permet ainsi de combiner une suite de k bits de données avec une clé de n bits afin d'obtenir un bloc de données chiffrées de même taille k que le bloc de données claires. Il combine des opérations de substitution, visant à remplacer des symboles par d'autres afin d'en cacher le sens, avec des opérations de permutation échangeant la position des symboles.

La mise en œuvre d'un algorithme de chiffrement symétrique par bloc ou **mode opératoire**, permet de définir les modalités de découpage du message initial en blocs (taille des blocs) ainsi que le mode de chiffrement de ces blocs permettant d'obtenir au final, un message chiffré. L'un des modes opératoires les plus utilisés¹²⁹ est le **CBC** (*cipher-block chaining*) permettant d'introduire une complexité supplémentaire dans le processus de chiffrement en créant une dépendance entre les blocs successifs (le chiffrement d'un bloc est lié au chiffrement des blocs précédents) (64).

¹²⁹ Notamment pour le chiffrement des données sensibles contenues dans les FSE.

Les principales propriétés attendues d'un mécanisme de chiffrement par bloc sont d'être facilement inversible si l'on dispose de la clé secrète de chiffrement et que, sans informations sur la clé secrète, il soit impossible en pratique de retrouver le message d'origine. Seuls les détenteurs de la clé secrète sont alors capables de transformer des données claires en données chiffrées et, inversement, des données chiffrées en données claires.

Parmi les algorithmes de chiffrement symétrique, l'algorithme DES (*data encryption standard*) fut défini en 1977 par le NIST¹³⁰, institut de standardisation américain, comme standard de chiffrement à usage commercial. Cet algorithme permet de découper les données en blocs de $k = 64$ bits et de les coder grâce à une clé secrète de $n = 56$ bits connue par le couple d'utilisateurs.

La sécurité du DES a fait couler beaucoup d'encre depuis sa création car la taille des clés serait sous-dimensionnée ce qui rend une attaque par la méthode de « recherche exhaustive » réalisable en quelques heures seulement. Cependant, afin de rendre possible une telle opération, de nombreux ordinateurs sont nécessaires afin de générer une puissance de calcul suffisante. Ceci a pu être mis en œuvre grâce au réseau internet et le bénévolat d'internautes acceptant d'effectuer des calculs sur leur ordinateur personnel en tâche de fond. Il fallut 250 jours pour réussir à casser les premières clés DES de 56 bits par cette méthode collaborative en 1997 alors qu'il ne fallait plus que 22 heures deux ans plus tard¹³¹. On utilise cependant toujours couramment le DES mais sous la forme du « triple-DES » ou « 3DES », permettant d'enchaîner trois applications successives de l'algorithme DES sur un même bloc de 64 bits en utilisant trois clés différentes (de 112 bits), inattaquable par recherche exhaustive. L'objectif à moyen terme est cependant de le remplacer par l'AES (*advanced encryption standard*) capables de traiter des blocs de 128 bits au moyen de clés de 128, 192 ou 256 bits.

Le référentiel général de sécurité précise que l'AES est le seul algorithme de chiffrement symétrique conforme au référentiel tandis que le l'algorithme 3DES, du fait de la faible taille du bloc, **peut** ne pas être conforme au référentiel. La taille minimale des blocs utilisés est de 64 bits (limite portée à 128 bits pour 2020).

A.3.5.1.b Méthodes de chiffrement asymétrique

La cryptographie asymétrique, telle que décrite par W. Diffie et M. Hellman utilise des « clés privées », que seul un utilisateur possède et peut utiliser pour les opérations privées ainsi que des « clés publiques », connues de tous pour les opérations publiques. Ces deux clés sont reliées par des équations mathématiques dont la difficulté de résolution peut être imagée de manière simple. A partir d'un pot de peinture jaune et d'un pot de peinture bleue, il est facile par simple mélange d'obtenir un pot de peinture verte. En revanche, l'opération inverse consistant à séparer les pigments jaunes des pigments bleus, sans être théoriquement infaisable, l'est en pratique. Dans cet exemple, le vert fait office d'élément public, et le bleu et le jaune sont privés : tout le monde sait que le but est de diviser le vert en bleu et jaune pour retrouver la clé privée, mais l'opération est considérée comme très difficile. De même, dans le monde mathématique, il existe de telles opérations inversibles mais asymétriques dans leur difficulté. On les appelle souvent problèmes difficiles ou asymétriques.

Ce système utilise donc des paires de clés (ou bi-clés) associées l'une à l'autre. Un expéditeur souhaitant transmettre un document chiffré à un correspondant doit, par ce système, prendre connaissance de la clé publique de ce dernier. L'expéditeur chiffre le document au moyen de

¹³⁰ National institute of standards and technology.

¹³¹ On estime très officiellement (dans un rapport présenté au Sénat américain) à cette date à quelques secondes le temps nécessaire pour percer les secrets d'un message chiffré avec le DES.

la clé publique du destinataire, puis le transmet à son correspondant qui utilise sa seconde clé, privée, connue de lui seul, afin de procéder à l'opération inverse de déchiffrement. La complexité de tels algorithmes asymétriques est telle qu'il est impossible de retrouver la clé privée en connaissant la clé publique. La clé publique peut donc être largement diffusée tandis que la clé privée doit être gardée confidentielle.

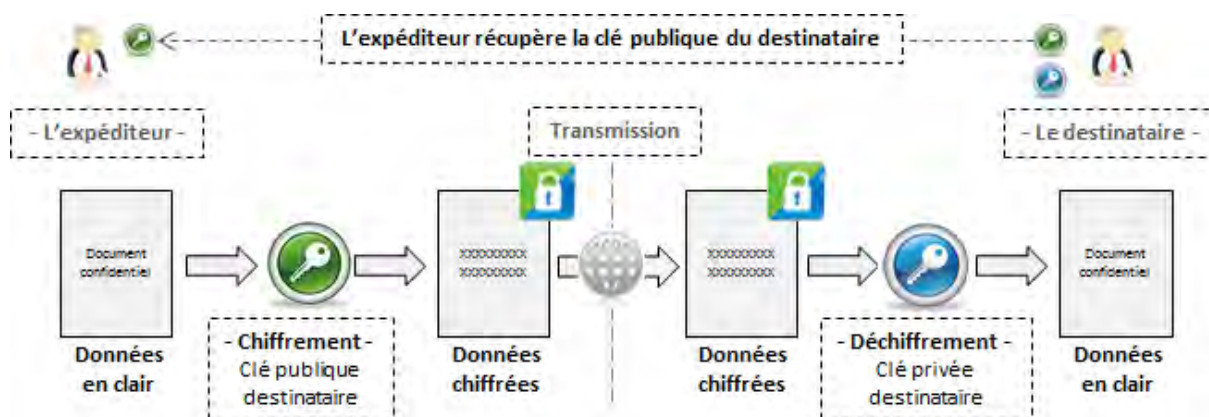


Figure 11 : Principe du chiffrement asymétrique à clé publique.

S'il existe de nombreux algorithmes de chiffrement asymétrique, l'exemple le plus connu, mais également le plus utilisé actuellement est le cryptosystème RSA¹³² qui consiste à multiplier de grands nombres premiers¹³³. L'opération inverse, consistant à retrouver ces nombres à partir du résultat, est appelée factorisation. Si la taille des entiers manipulés est suffisamment grande, il n'existe à ce jour aucune méthode efficace permettant de retrouver ces facteurs premiers à partir de la simple valeur de leur produit¹³⁴. Il existe plusieurs sous-standards d'algorithme de la famille RSA ou *PKCS* (*public key cryptography standards*) numérotés de 1 à 15. Le standard PKCS#1 permet notamment de mettre en œuvre des signatures électroniques.

La sécurité d'un tel système s'évalue donc en fonction de la difficulté à résoudre un algorithme mathématique et non pas selon la taille des clés. Ainsi, lorsque l'on parle de RSA-2048, cela signifie que l'on utilise cet algorithme avec un paramètre, appelé module, long de 2048 bits et obtenu par multiplication de deux nombres premiers de 1024 bits chacun. Il ne faut par conséquent pas s'étonner de voir apparaître en cryptographie asymétrique des paramètres ou des clés de 2048 bits ou plus alors qu'en cryptographie symétrique les clés dépassent rarement 128 bits, voire 256 bits pour les plus longues. Les tailles de clés symétriques et asymétriques ne sont donc pas comparables¹³⁵. Le référentiel général de sécurité précise que l'emploi de modules de 1024 bits est incompatible avec des conditions de sécurité acceptables et recommande ainsi d'utiliser des modules d'une taille minimale de 2048 bits (cette limite sera portée à 4096 bits à l'horizon 2020).

Comme il est possible de concevoir des machines dédiées à des fins de calculs exhaustifs sur des clés de chiffrement symétrique, il est aujourd'hui envisagé de concevoir de telles

¹³² Du nom de ses inventeurs : Rivest, Shamir et Adleman.

¹³³ Les nombres premiers étant les nombres divisibles uniquement par 1 et par eux-mêmes. Par exemple, 2, 3, 5, 7 sont premiers.

¹³⁴ Une telle factorisation n'est pas impossible, il existe même des algorithmes forts simples permettant de la retrouver. Le problème réside dans la complexité temporelle, soit le temps de calcul nécessaire à ces méthodes pour trouver le résultat.

¹³⁵ Ainsi, si une clé symétrique de 256 bits est largement suffisante, un module RSA de 256 bits peut être factorisé par tout ordinateur en moins d'une heure.

machines afin de factoriser des modules RSA. Ainsi, même si aucune annonce officielle n'a été faite à ce jour, il serait possible de réaliser une machine capable de factoriser des modules de 1024 bits en moins d'un an moyennant quelques dizaines de milliers d'euros¹³⁶ (65).

A.3.5.1.c Chiffrement hybride et clé de session

En raison de leur complexité, les algorithmes de chiffrement asymétriques ne constituent pas la solution la plus efficace à mettre en œuvre pour le chiffrement de longs messages. Il est donc possible, pour de grandes quantités de données à chiffrer, de combiner l'utilisation des techniques symétriques et asymétriques, on parle de chiffrement hybride.

L'expéditeur génère une clé de chiffrement symétrique ou clé de session (3DES, AES...) avec laquelle il chiffre son message. Comme nous l'avons vu, le talon d'Achille des méthodes de chiffrement symétrique réside dans la confidentialité de l'échange de la clé secrète entre les correspondants. Afin de s'affranchir de cette contrainte, l'expéditeur chiffre la secrète au moyen de la clé publique non confidentielle du destinataire (qu'il aura préalablement récupéré). La clé de session ainsi sécurisée est transmise au destinataire, seul capable d'inverser le processus au moyen de sa clé privée, restituant ainsi la clé de session. Il est également possible d'associer une fonction de hachage au chiffrement symétrique afin de garantir l'intégrité des données, on parle alors de code d'authentification de message (CAM).

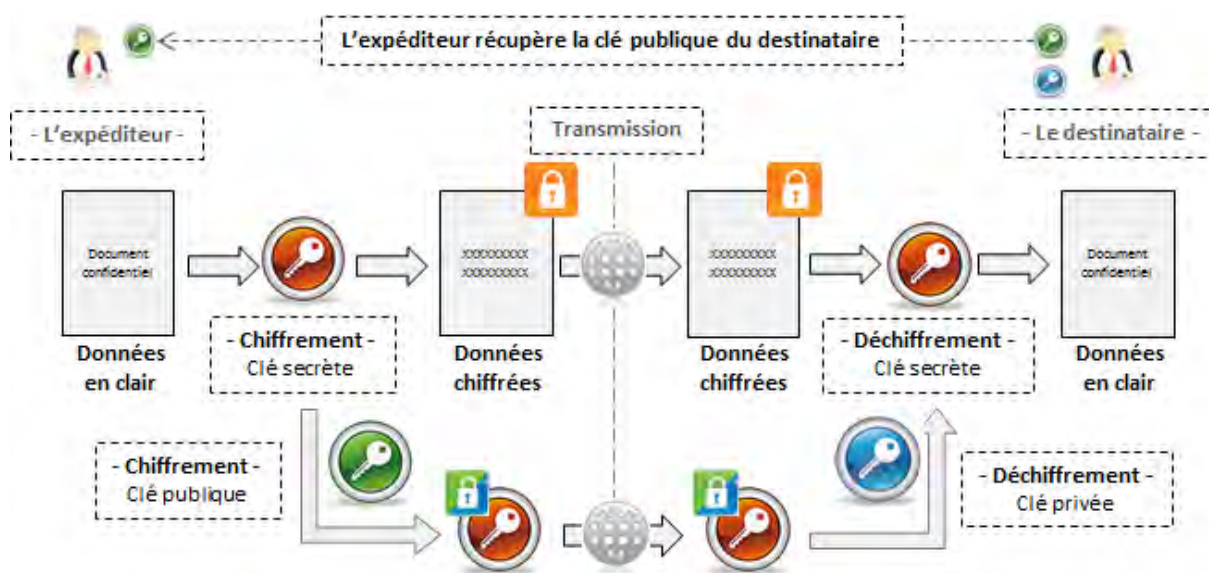


Figure 12 : Principe du chiffrement hybride.

A.3.5.1.d Fonctions de hachage et codes d'authentification de message

Une fonction de hachage permet de transformer une suite de bits de longueur quelconque en un condensat appelé empreinte ou haché, de taille déterminée, représentant le texte initial sous forme condensée et cryptée selon un algorithme de hachage. Elle utilise des mécanismes qui ne sont pas paramétrés par des clés comme les précédents mais permet de rendre l'identification de données plus rapide au moyen de cette empreinte et surtout d'en garantir l'intégrité. Cette fonction doit être irréversible et sans collision (deux messages distincts ne peuvent avoir une même empreinte). Ce caractère irréversible est fondamental dans la compréhension de ce mécanisme puisqu'il ne sert pas à déchiffrer l'empreinte.

¹³⁶ Le projet le plus abouti fut présenté par Adi Shamir et Eran Tromer en août 2003.

Le principal algorithme de hachage utilisé est l'algorithme SHA-2 regroupant SHA-224, SHA-256, SHA-384 et SHA-512. Son fonctionnement repose sur le principe suivant : le message à hacher est complété par une chaîne de caractères afin que sa taille corresponde à un multiple de 512 bits. Chaque bloc de 512 bits est découpé en seize sous-blocs de 32 bits, eux-mêmes convertis en quatre-vingt mots de 32 bits sur lesquelles quatre-vingt opérations mathématiques sont appliquées. L'empreinte ainsi générée est un message de taille fixe spécifique du message dont toute modification conduirait à l'élaboration d'une empreinte totalement différente (3).

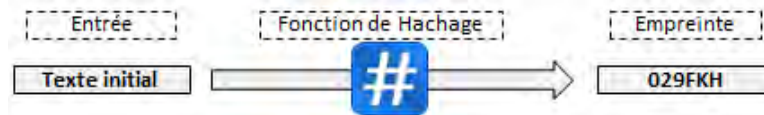


Figure 13 : Fonction de hachage : calcul d'une empreinte.

Lorsqu'un correspondant souhaite assurer l'intégrité d'un document, il applique l'algorithme de hachage à celui-ci, calculant ainsi son empreinte. Il transmet ensuite à son interlocuteur son document original ainsi que son empreinte. Afin de vérifier l'intégrité du document, le receveur en calcule l'empreinte en utilisant le même algorithme et la compare à l'empreinte fournie par l'expéditeur afin d'en vérifier la correspondance. Si les deux empreintes concordent, l'intégrité du document est assurée.

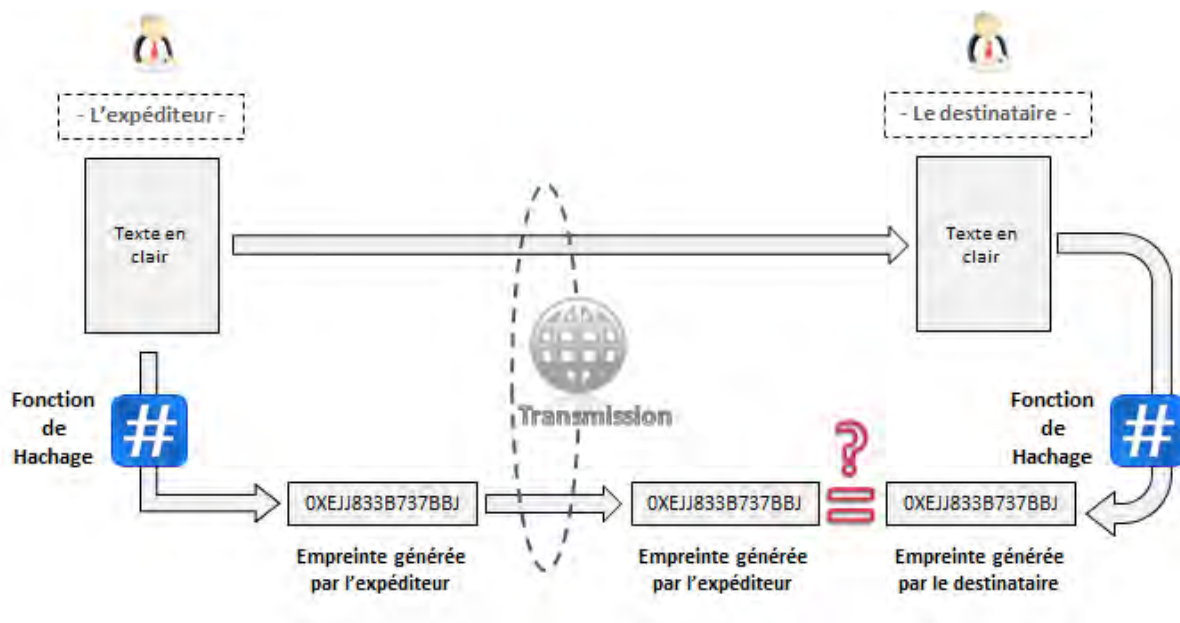


Figure 14 : Principe de mise en œuvre d'une fonction de hachage.

S'il est impossible de reconstituer le document initial à partir de son empreinte, il reste en revanche possible pour quiconque de recalculer une nouvelle empreinte du document initial modifié. En août 2004, de nombreuses publications annonçaient l'attaque possible des principales familles de fonctions de hachage. Depuis, le panel des fonctions de hachage considérées comme sûres s'est beaucoup réduit puisque n'y apparaissent plus ni MD5 (définitivement cassé) ni SHA-1 (qui n'atteint plus le niveau standard). Dans l'attente de la publication de nouveaux standards, dont par exemple SHA-3, et de leur mise à l'épreuve, la famille SHA-2 reste utilisable (64).

L'une des nombreuses applications des fonctions de hachage apparaît dans les schémas de signature numérique afin d'en assurer l'intégrité et réduire le message de longueur quelconque à un simple condensat de taille fixée et petite (64).

Comme nous l'avons vu, l'algorithme SHA-256 est également mis en œuvre dans le cadre de l'élaboration de l'INS-C. L'acquisition des données par le progiciel du professionnel de santé à partir des champs des différents volets accessibles en lecture de la carte Vitale permettent de faire remonter les valeurs des champs NIR (15 chiffres), prénom et date de naissance (au format jj/mm/aa). Ces valeurs sont normalisées (en majuscule, suppression de caractères non autorisés...) puis assemblées en un bloc sur lequel est appliqué l'algorithme de hachage. Les 16 premiers digits de l'empreinte ainsi générée sont convertis en base décimale permettant de constituer l'INS-C enrichi de sa clé (45).

Un **code d'authentification de message CAM** (ou MAC pour *message authentication code*) est un code accompagnant des données attestant de leur intégrité. Ce système est semblable aux fonctions de hachage car un algorithme crée un bloc authenticateur de taille fixe (comparable à l'empreinte), la différence résidant dans l'utilisation d'une clé secrète permettant d'en authentifier l'expéditeur.

Le CAM, typiquement long de 128 bits est généré à partir des données à protéger et chiffré à l'aide d'une clé secrète partagée avec le correspondant. Il est transmis au correspondant en pièce jointe du message transmis. Après réception, le destinataire recalcule le CAM à partir du message reçu en appliquant le même algorithme et la même clé que l'expéditeur et le compare avec le CAM qui lui a été transmis. S'ils sont identiques, il est extrêmement probable que les données soient intègres et proviennent donc de la bonne personne (64).

L'un des algorithmes les plus utilisés est le CBC-MAC (*cipher bloc chaining message authentication code*) où le CAM est calculé en appliquant le mode de chiffrement CBC au message (64).

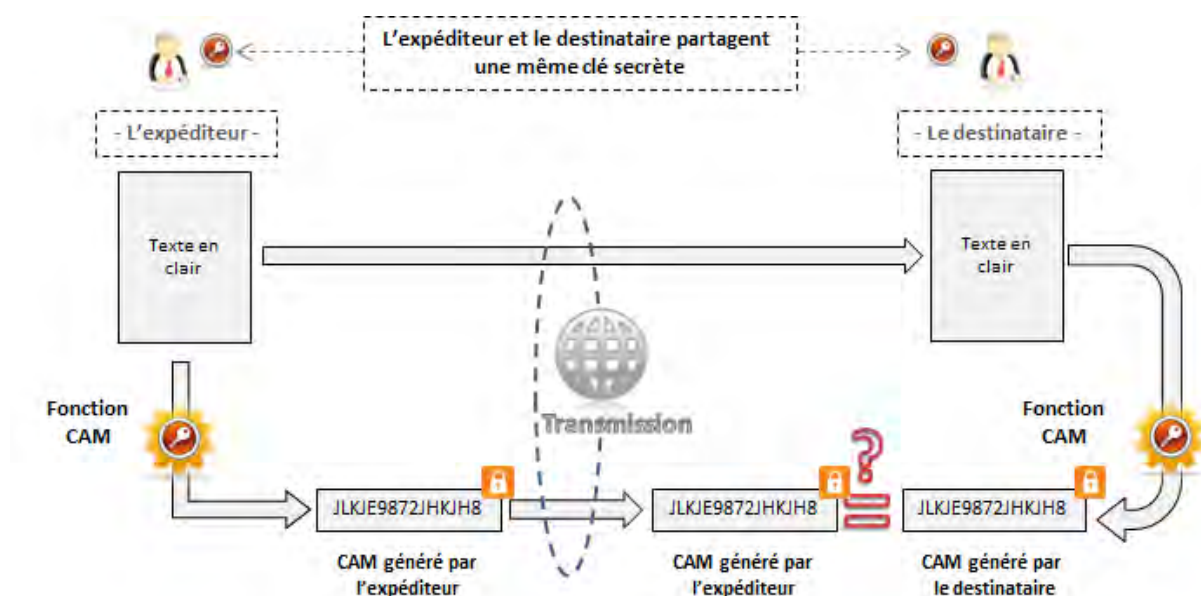


Figure 15 : Principe de mise en œuvre d'une fonction de code d'authentification de message (CAM).

A.3.5.2 IDENTIFICATION ET AUTHENTIFICATION ELECTRONIQUES

Comme nous l'avons vu, les mécanismes utilisant des clés cryptographiques assurent la confidentialité des données par chiffrement. Lors de toute correspondance électronique, il est cependant primordial de pouvoir s'assurer de l'identité de l'expéditeur et du destinataire.

L'authentification a pour but de vérifier l'identité dont une entité (personne ou machine) se réclame. Elle est toujours précédée ou combinée avec une **identification** qui permet à cette entité de se faire reconnaître du système par un élément dont on l'a doté : un identifiant. En résumé, s'identifier c'est communiquer un identifiant présumé, s'authentifier c'est apporter la preuve que l'entité s'est vue attribuer cet identifiant (64).

L'authentification peut viser :

- soit à contrôler l'accès à des informations ou des locaux...
- soit à garantir une imputabilité avec vérification forte de l'identité affichée ;
- soit à assurer une combinaison de ces fonctions.

Il est possible de distinguer trois schémas d'authentification (66) :

- **l'authentification de machines entre elles** à l'aide de mécanismes utilisant des clés cryptographiques associées à un certificat électronique ;

- **l'authentification d'une personne vis-à-vis d'une machine** précédée d'un déverrouillage comme la saisie d'un mot de passe, la présentation d'un badge personnel, l'insertion d'un support amovible, qui donne l'accès aux données qu'il contient, la saisie d'un code porteur qui active des fonctionnalités d'une carte à puce, la reconnaissance d'une caractéristique biométrique... L'authentification s'effectue en réalité de machine à machine au moyen de certificats électroniques mais grâce à un déverrouillage de l'environnement de confiance local par l'utilisateur. Ce mécanisme d'authentification n'offre qu'un niveau de sécurité limité car de nombreuses techniques de piratage comme l'« hameçonnage » permettent de récupérer le couple identifiant/mot de passe de l'utilisateur et d'usurper ainsi son identité. Cette méthode suggère donc l'utilisation d'un mot de passe fiable, complexe et régulièrement changé.

- **l'authentification de bout en bout** (de personne à personne) peut être modélisée par symétrie du modèle précédent puisque l'authentification mutuelle des utilisateurs distants résulte de la double authentification des utilisateurs et de la confiance de chacun dans son propre système du fait des mécanismes de déverrouillage utilisés.

La méthode **d'authentification symétrique** la plus simple et la plus utilisée afin de s'assurer de l'identité d'un correspondant consiste dans le partage de la clé secrète avec lui au risque d'une interception du secret par un tiers. Par conséquent, la méthode dite par « *challenge-response* » ou « défi-réponse » peut être mise en œuvre en envoyant un message quelconque à celui que l'on souhaite authentifier, et lui demander de le chiffrer en utilisant la clé secrète partagée, puis de renvoyer le résultat obtenu. Si la réponse reçue se déchiffre correctement et aboutit à la question posée, il y a une forte probabilité pour que la personne ayant calculé le chiffré possède effectivement la clé secrète et, par conséquent, soit la personne qu'elle prétend être.

L'authentification asymétrique d'entités peut être mise en œuvre selon une méthode similaire : afin d'authentifier quelqu'un dont on connaît la clé publique, il suffit par exemple de chiffrer à son attention un message quelconque au moyen de celle-ci et de lui demander de retourner ce message en clair (déchiffré avec la clé privée dont il est le seul détenteur) et vice-versa. Les certificats électroniques évoqués ci-après permettent ainsi de s'assurer formellement de l'identité d'un destinataire grâce à l'établissement d'une chaîne de confiance entre les différentes autorités chargées d'établir le lien entre l'identité de la personne et un certificat électronique.

A.3.5.3 LA SIGNATURE ELECTRONIQUE

La directive européenne 1999/93/CE du 13 décembre 1999 relative au statut de la signature électronique visant à en « *faciliter l'utilisation et contribuer à leur reconnaissance juridique* » fut introduite afin de promouvoir une reconnaissance juridique de la signature électronique et des services de certification à l'échelle de l'Union. Transposée en droit français par la loi n°2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, l'article 1316-4 du code civil définit la signature comme la manifestation du consentement de celui qui l'appose et permet de l'identifier. Lorsqu'elle est électronique, elle consiste en « *l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie* ». Le décret n°2001-272 du 30 mars 2001 pris pour l'application de cet article décrit les conditions selon lesquelles le procédé de signature électronique est présumé fiable (article 2) :

- elle doit être sécurisée, c'est-à-dire « *être propre au signataire, être créée par des moyens que le signataire puisse garder sous son contrôle exclusif et garantir que toute modification de l'acte soit détectable* » (article 1) ;

- elle doit être établie au moyen d'un dispositif sécurisé de création de signature électronique, c'est-à-dire « *un matériel ou un logiciel destiné à mettre en application les données de création de signature électronique* » (article 1) sécurisé notamment en garantissant la protection de la signature contre la falsification et ne devant pas altérer le contenu du document...

- sa vérification repose sur l'utilisation d'un certificat électronique qualifié c'est-à-dire « *un document sous forme électronique attestant du lien entre les données de vérification de signature électronique et un signataire* » (article 1) délivré par un prestataire services de certification électronique (PSCE) reconnu par l'Etat. Ce point fondamental sera explicité plus en détail ci-après afin de mettre en évidence le rôle de l'ASIP Santé en tant socle de l'infrastructure de gestion des certificats électroniques dédiés à l'usage des professionnels de santé.

La signature électronique constitue donc un moyen efficace pour authentifier son auteur tout en attestant de l'intégrité d'un document électronique. Elle traduit ainsi la manifestation du consentement du signataire quant au contenu des informations signées tout en garantissant sa non-répudiation¹³⁷. Si la signature électronique ne permet pas d'assurer la confidentialité du

¹³⁷ Assurer l'intégrité de données consiste à empêcher, ou tout du moins à détecter, toute altération non autorisée de données, c'est à dire toute modification, suppression partielle ou insertion d'informations. L'intégrité des données est classiquement assurée en cryptographie par des fonctions de hachage et les codes d'authentification de message (CAM). La non-répudiation vise quant à elle à éviter qu'une entité puisse nier avoir effectué une certaine action (65).

document transmis à elle seule, il est tout à fait envisageable de procéder à un chiffrement du document avant de le signer électroniquement.

La signature électronique utilise à la fois la cryptographie asymétrique et des techniques comme les fonctions de hachage. C'est en effet par l'association de ces méthodes qu'il est possible de réunir les cinq caractéristiques d'une telle signature (authentique, infalsifiable, non réutilisable, inaltérable, irrévocable). La signature utilise ainsi un mécanisme cryptographique asymétrique ayant de nombreuses similitudes avec le chiffrement à clé publique. Le principal point commun est l'emploi de bi-clés formés d'une clé privée et d'une clé publique associée. La clé privée permet de générer la signature d'un message tandis que la clé publique permet d'en vérifier la validité. Par conséquent, tout le monde peut potentiellement s'assurer de l'authenticité d'un message puisque la clé publique peut être librement rendue disponible.

A l'aide de sa clé privée, l'expéditeur chiffre l'empreinte générée par une fonction de hachage à partir du document original. Cette empreinte signée ou « sceau » est transmise au destinataire conjointement au document original. Après réception, le destinataire déchiffre le sceau au moyen de sa clé publique puis compare l'empreinte reçue à celle qu'il a lui-même générée à partir du document reçu.

Grâce à ce système à clé publique combiné à une fonction de hachage ou un code d'authentification de message, la signature électronique permet au destinataire de s'assurer de l'intégrité des données, de l'authenticité d'un correspondant et de la non-répudiation de la correspondance.

Le principe de fonctionnement et d'interaction des composants entre eux est le suivant (67):

- l'application de création de signature déployée sur une machine (ordinateur, borne publique, serveur...) calcule une empreinte à l'aide d'une fonction de hachage, à partir des informations à signer ;
- elle transmet ce condensat au dispositif de création de signature (carte à puce par exemple) également connecté à la machine;
- le dispositif de signature réalise un calcul cryptographique de signature du condensat en utilisant la clé privée de signature de l'utilisateur, activée le cas échéant par un code d'activation (code porteur de la carte CPS par exemple) ;
- ce condensat signé, dit signature électronique, est retourné à l'application ;
- la vérification de la signature s'effectue à l'aide d'un module de vérification de signature et du certificat électronique délivré par le PSCE qui lie l'identité de l'agent ou de l'utilisateur avec sa clé publique, comme nous le verrons ci-après. Un calcul cryptographique est effectué à l'aide de la clé publique sur la signature électronique et comparé au condensat obtenu par hachage des informations à signer.

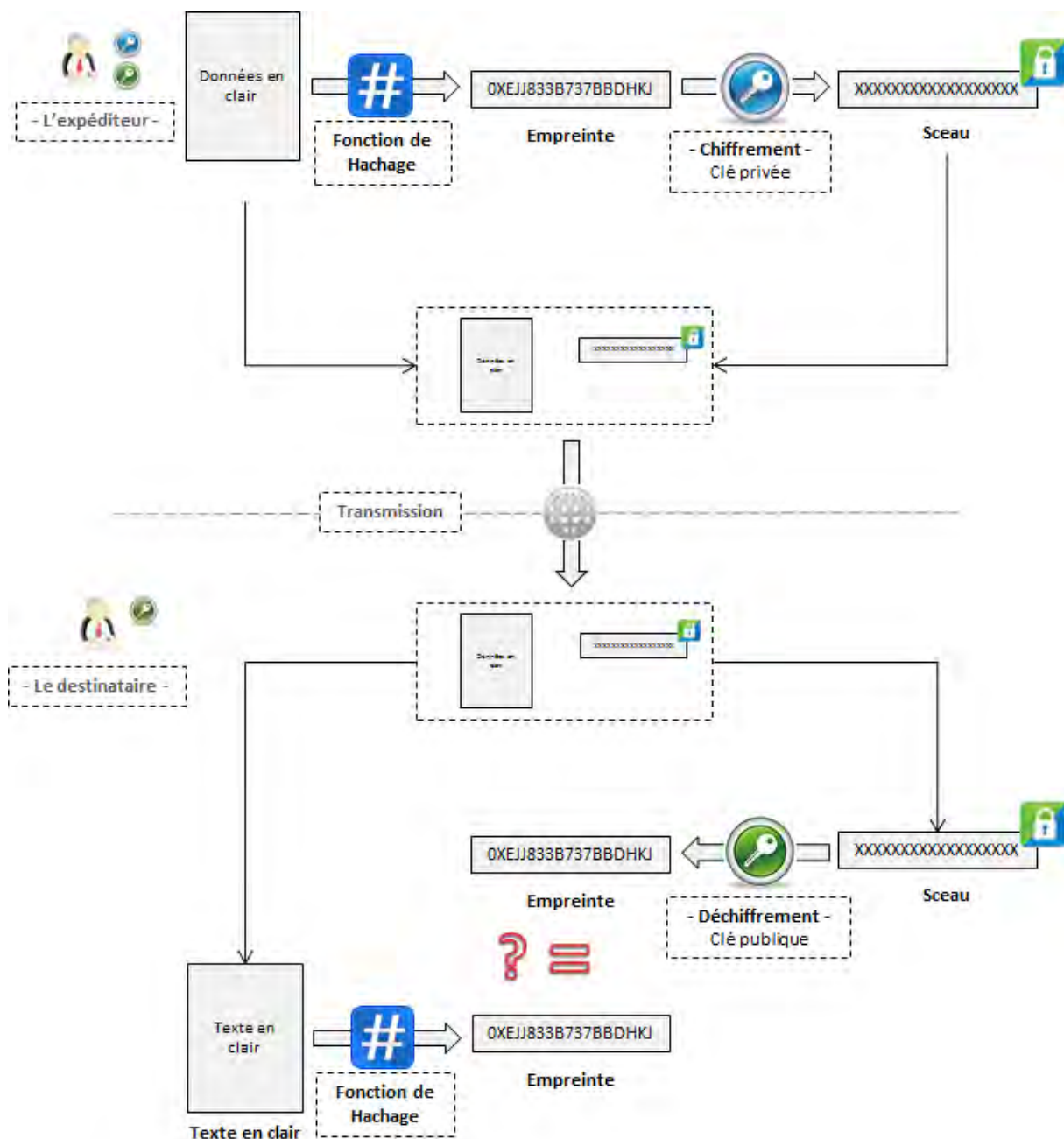


Figure 16 : Principes de création et de vérification d'une signature électronique.

A.3.5.4 LES CERTIFICATS ELECTRONIQUES

Un **certificat électronique** ou numérique est une « carte d'identité numérique » permettant de lier une entité physique (personne, élément matériel, serveur...) à une identité numérique (virtuelle). Il s'agit d'un fichier électronique **structuré et normalisé** attestant qu'une paire de clés cryptographiques appartient bien à cette personne (1). Il existe ainsi dans une carte à puce telle que la CPS3 un certificat pour chaque fonction de sécurité assurée par la carte.

Tout comme la préfecture de police garantit la validité des informations d'une pièce d'identité papier, pour qu'un certificat électronique soit digne de confiance, l'autorité émettrice doit être digne de confiance et répondre à certaines exigences de sécurité. La gestion de ces certificats électroniques nécessite donc la mise en œuvre d'une **infrastructure de confiance** dédiée à

l'attribution, le renouvellement, la mise à jour, la révocation ou encore la publication des clés publiques au moyen d'un annuaire et de la liste des certificats révoqués.

Le système de certificats électroniques destinés à l'usage des professionnels de santé étant parfaitement décrit par l'ASIP Santé, nous utiliserons donc ce modèle pour illustrer la structure, les fonctions et la gestion de ces certificats.

A.3.5.4.a La gestion des certificats électroniques

L'un des avantages de la cryptographie asymétrique est qu'il n'est pas nécessaire de partager des secrets entre utilisateurs, la clé privée n'étant connue que par son seul détenteur et la clé publique connue de tous. La principale difficulté de mise en œuvre de ce système réside dans la nécessité d'associer un couple clé privée / clé publique à l'identité de son détenteur légitime tout en mettant à disposition la clé publique aux correspondants (68).

Une **infrastructure de gestion de clés (IGC)** est un ensemble de moyens physiques humains et logiciels employés afin de gérer le cycle de vie des certificats électroniques. Il s'agit d'une véritable chaîne de confiance permettant d'attester de la qualité des pratiques de gestion des clés publiques mises en œuvre par les autorités concernées.

Les **prestataires de service de certification électronique (PSCE)** chargés de la délivrance des certificats électroniques aux usagers incluent une **chaîne de certification** hiérarchisée composée de différentes **autorités de certification (AC)**. Cette chaîne de certification est une infrastructure à plusieurs niveaux où les « AC émettrices » (ACE) qui délivrent les certificats aux usagers pour une fonction de sécurité particulière (authentification, signature électronique...) sont elles-mêmes certifiées par des « AC intermédiaires » (ACI) de niveau supérieur, jusqu'aux « AC racines » (ACR) de plus haut niveau. Une durée de vie maximale ou crypto-période, est généralement associée à chaque clé afin d'en limiter « l'usure » et la compromission. Il peut s'agir d'une date limite d'emploi ou d'un compteur du nombre d'utilisations qui ne doit pas dépasser une certaine limite. Les PSCE sont donc chargées de la gestion des certificats tout au long de leur cycle de vie (68) .

L'IGC dédiée à la gestion des certificats électroniques des professionnels de santé, sous la responsabilité de l'ASIP Santé est l'IGC CPS2ter. Dans l'attente de la mise en œuvre d'une nouvelle IGC, dite « IGC-Santé », il a été décidé de proroger l'IGC-CPS2ter jusqu'à fin 2020 alors désignée IGC CPS2ter-2020 (69). Comme tout PSCE, l'ASIP Santé est autorisée à exercer cette activité après une **procédure de qualification** permettant d'apporter la preuve de leur conformité aux exigences portant sur la délivrance de **certificats électroniques qualifiés**. Le prestataire de service de certification choisit un organisme accrédité par le COFRAC pour procéder à l'évaluation des services qu'il propose, selon un référentiel d'évaluation puis l'Agence nationale de sécurité des systèmes d'information réalise un contrôle *a posteriori* conformément à un référentiel de contrôle (70). La liste des PSCE qualifiés (dont l'ASIP Santé) est mise en ligne via le site de la direction générale de la compétitivité de l'industrie et des services (DGCIS)¹³⁸ .

En résumé, l'ASIP Santé émet des **certificats électroniques qualifiés** à l'usage des professionnels de santé permettant notamment de **s'authentifier fortement** dans un système d'information et de mettre en œuvre une **signature électronique sécurisée au niveau *** du référentiel général de sécurité**. Elle est composée de plusieurs services impliqués dans la

¹³⁸<http://www.dgcis.redressement-productif.gouv.fr>

délivrance et la gestion des cartes CPS munies de certificats électroniques de signature et d'authentification.

Le **service d'enregistrement** de l'IGC CPS2ter-2020 collecte et vérifie l'origine, l'intégrité et la cohérence des données d'identification professionnelle fournies par les autorités compétentes (ordre, ARS, CNAMTS). Il transmet une demande de fourniture de carte CPS au **service fourniture CPS** chargé de personnaliser la nouvelle carte à partir des informations reçues du service d'enregistrement et des éléments cryptographiques fournis par le **service de génération des clés et des certificats**. Afin de générer les certificats électroniques et les clés cryptographiques correspondantes, le service de génération des clés et des certificats utilise les informations reçues du service fourniture CPS. Le **service de diffusion** assure ensuite la publication de ces certificats dans un **annuaire** disponible sur un site dédié¹³⁹ afin de communiquer les informations utiles à tout correspondant (clé publique du certificat, informations associées...) (71).

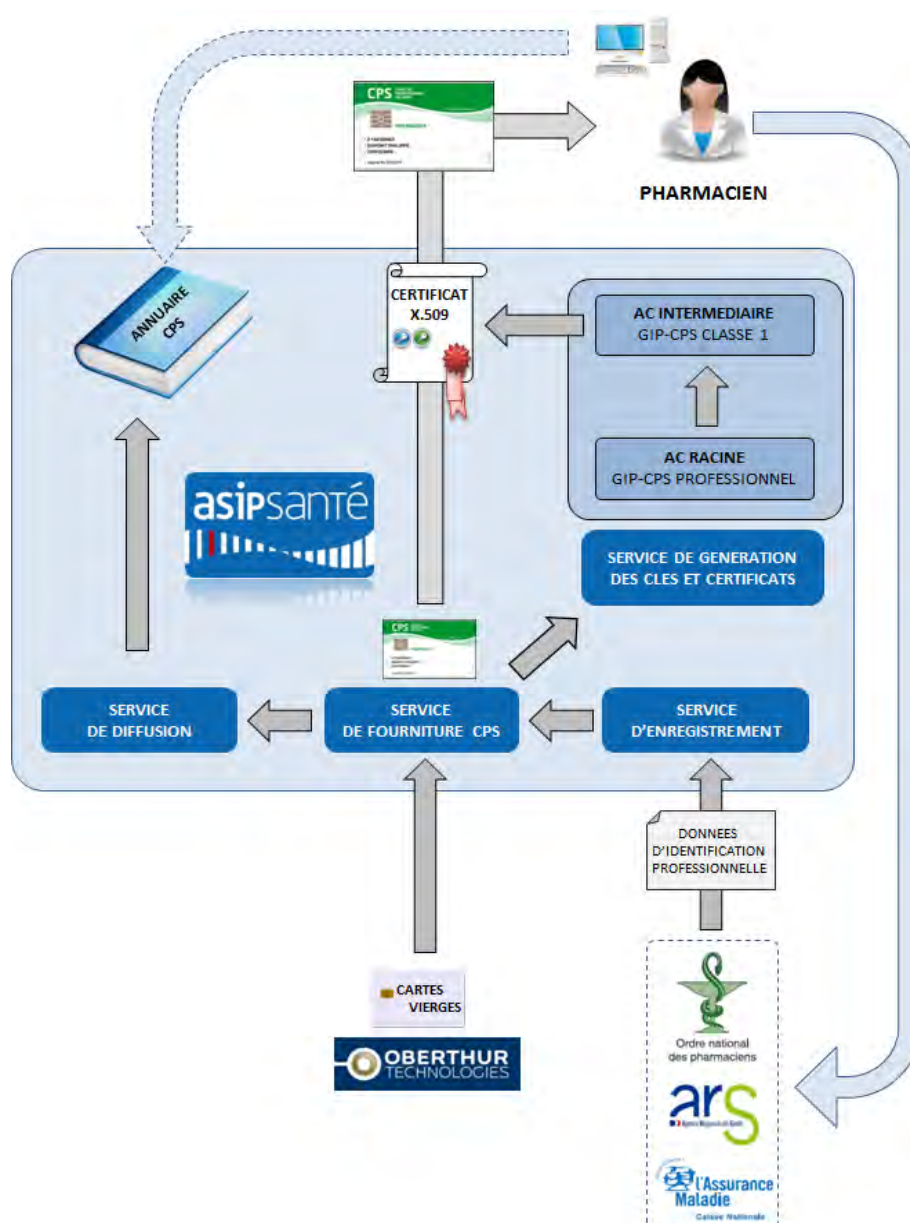


Figure 17 : Principales étapes d'élaboration des cartes CPS3 par l'IGC CPS2ter-2020 (71).

¹³⁹ Accessible à l'adresse <http://annuaire.gip-cps.fr/>

A.3.5.4.b Structure et fonctions des certificats émis par l'ASIP Santé

Il existe plusieurs standards définissant la structure des certificats électroniques mais les certificats les plus utilisés actuellement sont conformes au standard X.509 version 3¹⁴⁰. Il existe ainsi au sein d'une même IGC différents niveaux de certificats (racine, intermédiaire, utilisateur) assurant une chaîne de certification au sein de l'infrastructure. Nous nous concentrerons donc sur les certificats du « niveau utilisateur » ou certificats de classe 1, utilisés quotidiennement par tout professionnel de santé.

CERTIFICAT X.509 version 3	
Contenu du certificat (<i>Données certifiées</i>)	
Version et numéro de série du certificat	
Informations sur l'AC émettrice du certificat permettant de résumer la chaîne de certification : pays, dénomination de l'AC, AC Racine, AC Intermédiaire	
Informations sur le porteur du certificat : pays d'exercice, profession, n° RPPS, nom, prénom	
Informations sur l'algorithme de signature : types d'algorithmes utilisés, taille et paramètres de la clé publique	
Période de validité du certificat	
Adresse à laquelle est disponible la liste des certificats révoqués (CRL) ainsi que les informations sur l'autorité la mettant en œuvre ;	
Informations sur la carte CPS : numéro de série, type (CPS, CPE...), profession, n° ADELI et n° RPPS	
Extensions du certificat (informations complémentaires sur les clés, les politiques de certification...) telles que le tableau d'inscription à l'ordre des pharmaciens (A, D, G...)	
Signature du certificat par l'AC	
Informations sur l'algorithme de signature du certificat	
Valeur de la signature numérique du certificat par l'AC (calculée avec la clé privée de l'AC Intermédiaire "ACI CLASSE-1")	

Tableau 15 : Structure générale d'un certificat X.509 V3 (69).

En tant qu'autorité de certification du domaine de la santé, l'ASIP Santé est chargée de délivrer les certificats électroniques de niveau utilisateur des professionnels de santé. Elle délivre et garantit ainsi quatre types de certificats à l'usage des professionnels de santé (72) :

- **Un certificat d'authentification électronique** embarqué dans la carte CPS qui permet au porteur de la carte de s'authentifier vis-à-vis d'un serveur distant¹⁴¹ à l'aide d'un bi-clé RSA de 1024 bits.
- **Un certificat de signature électronique**, embarqué dans la carte CPS mis à contribution dans la signature électronique des messages à l'aide d'un bi-clé RSA de 2048 bits couplé à un hachage SHA-256.

¹⁴⁰ Selon le référentiel RFC 5280 - *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*.

¹⁴¹ La saisie du code porteur combinée à l'utilisation de ce certificat permet une **authentification forte** du porteur de la carte.

L'annexe 5 présente le contenu détaillé de des champs de valeurs des certificats d'authentification et de signature électronique des cartes CPS.

Seuls ces deux types de certificats sont portés par la CPS, **les certificats de confidentialité** permettant à certaines applications informatiques de chiffrer des données, sont quant à eux mis à disposition des professionnels de santé par l'ASIP Santé au moyen de l'annuaire CPS. Le chiffrement repose sur l'utilisation de l'algorithme RSA (clé de 1024 bits) (73).

Les certificats électroniques inclus dans chaque carte CPS permettent donc d'en authentifier le porteur et de générer une signature électronique sécurisée. Afin de s'assurer des mêmes fonctions de sécurité au sujet du correspondant, l'usage réciproque de certificats électroniques par le correspondant est nécessaire (par exemple au moyen de certificats de serveur).

- **Des certificats de serveur** permettent de garantir l'authentification et la signature électronique d'un serveur distant. Ainsi, à l'aide d'un certificat associé à un utilisateur (par exemple le certificat d'authentification d'une carte CPS) et d'un certificat de serveur, il est possible de réaliser une authentification réciproque des correspondants permettant de créer comme un « tunnel sécurisé » entre le poste de travail utilisateur et le serveur distant ou VPN (*virtual private network*) (74).

Il existe actuellement deux types de certificats de serveurs émis par l'ASIP Santé (tous deux reposant sur un algorithme RSA et des clés de 1024 bits) (75) :

- **les certificats SSL (*security sockets layer*) et TLS (*transport layer security*)**¹⁴² qui sont des certificats d'authentification principalement utilisés pour authentifier des sites internet vis-à-vis d'utilisateurs connectés. Il permet ainsi d'appliquer des fonctions de sécurité particulières au protocole de transfert HTTP (on parle alors de HTTP sécurisé ou HTTPS).

Il est possible de représenter l'impact du protocole SSL sur le transfert de données comme la création d'un tunnel où seuls les ordinateurs à l'entrée et à la sortie peuvent lire le message (76) :



Figure 18 : Illustration de la transmission sécurisée de données par création d'un tunnel SSL.

Il permet donc la sécurisation d'une voie d'échange entre un client (utilisateur) et un serveur, ceci pendant toute la durée de la connexion (session). La sécurisation consiste en l'authentification réciproque du serveur vis-à-vis des utilisateurs (ou d'autres serveurs), ainsi que la confidentialité et l'intégrité des données échangées (77).

¹⁴² Par abus de langage, les protocoles SSL et TLS sont bien souvent confondus. La version 3 du protocole SSL correspond en réalité à la version 1 du protocole TLS, plus sécurisée.

Le principe général d'établissement d'une connexion sécurisée au moyen du protocole SSL est le suivant (78):

- le client envoie une requête de connexion au serveur. Ils échangent leurs certificats floqués de leur clé publique respective, s'authentifient mutuellement et négocient les paramètres de sécurisation (sélection d'un algorithme commun) ;

- le client génère un message (suite quelconque de 48 bits) ou *PreMaster Secret* chiffré au moyen de la clé publique du serveur (seul ce dernier peut donc le déchiffrer). Ce PMS chiffré est transmis au serveur qui le déchiffre avec sa clé privée afin de restituer le PMS initial, en clair.

- le client et le serveur génèrent ensuite une même clé de session à partir du même PMS resté confidentiel, celle-ci permet le chiffrement des données échangées lors de la session web selon un algorithme symétrique (3DES, AES) et garantit l'intégrité des données grâce à une fonction de hachage associée (SHA). Ce chiffrement symétrique couplé à l'utilisation d'une fonction de hachage est assimilable à l'utilisation d'une fonction de code d'authentification de message (CAM)

Comme nous le verrons, un tel schéma de sécurisation des flux HTTP est notamment mis en œuvre lors de l'utilisation du dossier pharmaceutique en ligne. La sécurisation d'un système d'e-prescription pourrait, comme nous le verrons, être mise en œuvre par un tel mécanisme, à l'image des différents systèmes opérationnels en Europe.

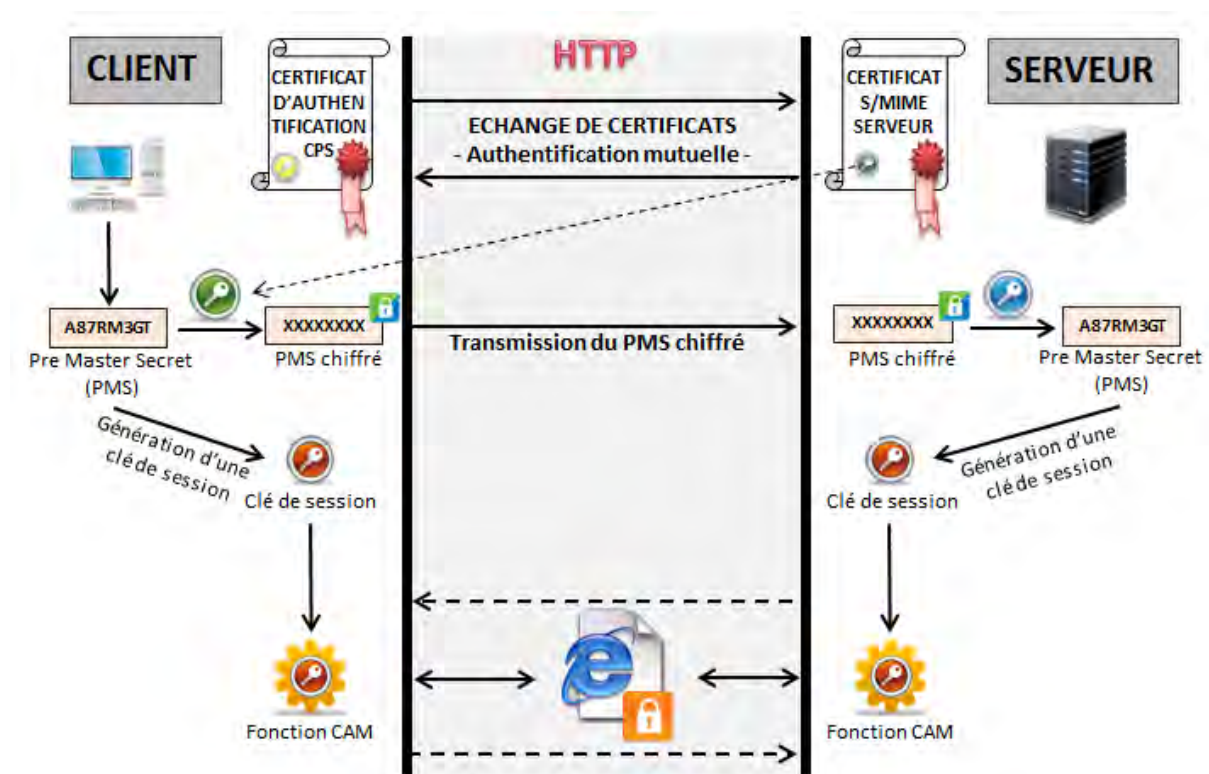


Figure 19 : Principe de création d'un tunnel SSL :
authentification, intégrité et confidentialité des échanges.

Afin de décrire la succession des processus impliqués dans l'établissement du tunnel SSL, la **suite de chiffrement** réalisée est ainsi exprimée : **SSL_X_WITH_Y_Z** où :

- X désigne l'algorithme utilisé pour l'échange de clé et l'authentification (certificats client et serveur), il s'agit donc de l'algorithme de chiffrement du PMS ;
- Y désigne l'algorithme de chiffrement symétrique utilisé par la clé de session ;
- Z désigne l'algorithme de hachage associé à la clé de session.

- **les certificats S/MIME (*secure /multipurpose internet mail extensions*)** sont des certificats de signature et de chiffrement destinés à des serveurs, notamment de messagerie électronique. Ils permettent la sécurisation des objets échangés, avant ou au moment de la correspondance, à l'aide du protocole de sécurité S/MIME appliqué au protocole de transport SMTP utilisé pour la transmission de courriers électroniques.

Ce protocole utilise des méthodes cryptographiques assurant :

- la confidentialité du message par l'utilisation d'un algorithme de chiffrement symétrique (type 3DES ou AES) ;

- l'authentification du serveur, l'intégrité du message et la non-répudiation de la correspondance par l'utilisation du certificat électronique de signature.

Le logiciel de messagerie électronique du client (expéditeur) génère un message aux formats SMTP et MIME qui est sécurisé par l'application du protocole S/MIME consistant à apposer la signature électronique de l'expéditeur et chiffrer le contenu du message. Pour cela, l'expéditeur utilise sa clé privée de signature électronique et une clé de session permettant un chiffrement conventionnel ou symétrique du message.

Afin de sécuriser le processus d'échange de la clé de session permettant au serveur de déchiffrer le message, celle-ci est chiffrée selon un mécanisme asymétrique à l'aide la clé publique du serveur issue de son certificat. Le message signé et chiffré ainsi que la clé de session chiffrée sont envoyés conjointement au serveur dans une même entité qui procède à l'opération inverse de déchiffrement de la clé de session au moyen de sa clé privée. Le serveur vérifie la signature de l'expéditeur, garante de son authentification et de l'intégrité du message échangé, puis déchiffre le contenu du message au moyen de la clé de session (78).

Comme nous le verrons, un tel schéma de sécurisation des flux SMTP peut notamment être mis en œuvre lors de la télétransmission des lots de factures et de pièces justificatives électroniques.

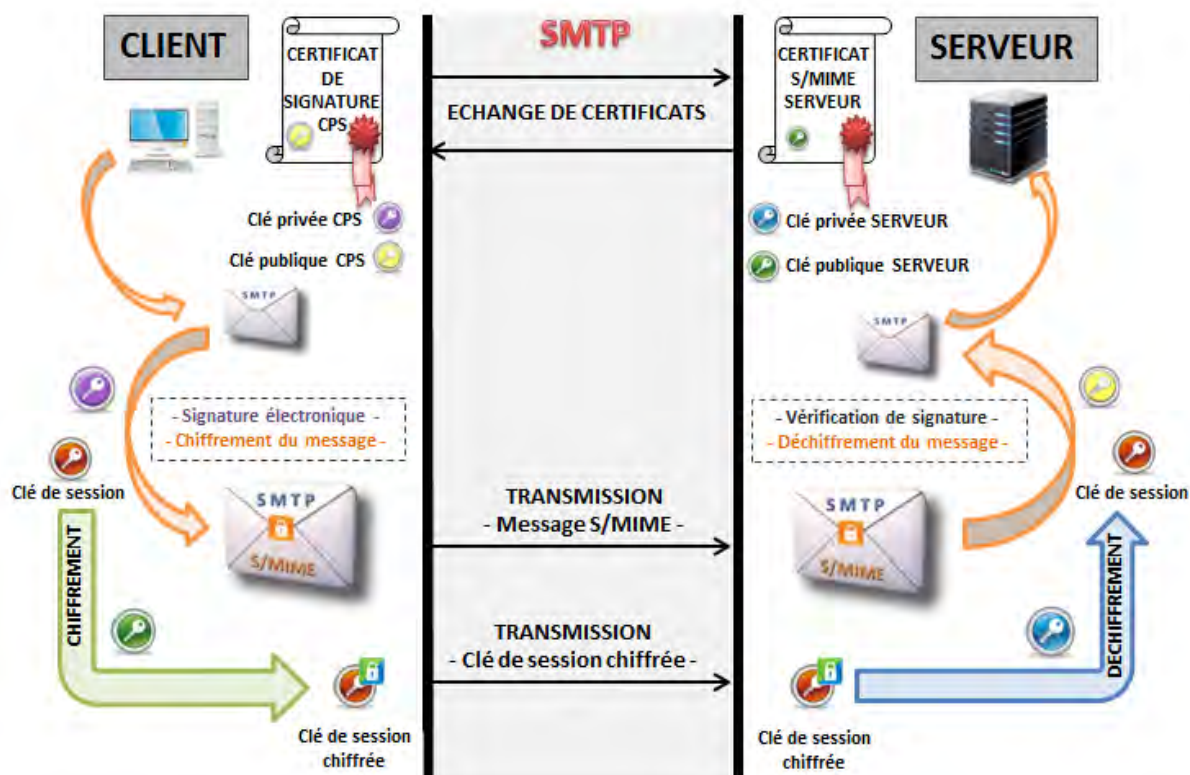


Figure 20 : Principe de sécurisation d'un courriel par le protocole S/MIME.

L'évolution des fournitures matérielles et logicielles proposées conjointement par le GIE SESAM-Vitale et l'ASIP Santé a pour objectif principal de développer un environnement de confiance en sécurisant l'identification et/ou l'authentification formelle des patients et des professionnels de santé afin de sécuriser l'accès aux données de santé ainsi que leur contenu. Pour cela, les cartes Vitale 2 et CPS3 élaborées au standard IAS embarquent un crypto-processeur permettant la mise en œuvre de mécanismes cryptographiques capables d'assumer des fonctions de chiffrement, d'identification, d'authentification et de signature électronique au moyen d'applications embarquées et d'un lecteur SESAM-Vitale homologué. Comme nous le verrons, seules les fonctions de sécurité de la carte CPS sont mises à contribution tandis que la carte vitale, bien que dotée des éléments matériels nécessaires, n'est pas utilisée à ces fins puisque les porteurs de carte Vitale ne bénéficient pas de certificats électroniques.

A.3.5.4.c Fonctions de sécurité offertes par la carte CPS3

Véritable clé d'entrée des systèmes d'information en santé, la carte CPS vise notamment à en authentifier son porteur et à préserver la confidentialité de données sensibles lors de leur transmission à un tiers par voie électronique. Il s'agit d'une carte multi-applicative comportant 2 volets ou applications :

- le volet CPS2ter assurant la compatibilité des moyens et la continuité du service avec la précédente version de la carte;
- le volet IAS, standard retenu pour la carte CPS3.

A la mise sous tension de la carte CPS3 dans un lecteur, celle-ci se comporte rigoureusement comme sa version précédente, la carte CPS2ter. Ceci est un gage de compatibilité avec toutes les applications existantes et notamment avec les applications SESAM-Vitale.

Outre l'ensemble des données métiers, la carte CPS3 embarque les clés cryptographiques associées aux certificats d'authentification et de signature émis par l'ASIP Santé. Elle est ainsi dotée de deux types de certificats X.509 associés à leurs clés, inscrits en double dans la carte : un jeu dans le volet CPS2ter et l'autre dans le volet IAS (79):

- un certificat pour la clé publique de signature (bi-clé RSA de 2048 bits).
- un certificat pour la clé publique d'authentification (bi-clé RSA de 1024 bits).

Ces applications visent à permettre la mise en œuvre de fonctions de sécurité indispensables pour l'e-santé telles que :

- **L'identification et l'authentification** de tout professionnel de santé de manière fiable et certifiée au niveau national permettant de garantir leur identité. Après insertion dans un lecteur approprié, l'ensemble des fonctions de la carte est accessible. Le professionnel de santé peut s'authentifier fortement grâce à son code confidentiel et la mise en œuvre des fonctions cryptographiques d'authentification de la carte.

Une **identification simple** avec ou sans lecture de données applicatives permet une identification de la carte par simple lecture du numéro de série. Ce mode est à la fois disponible en mode « contact » et « sans contact » pour permettre par exemple un contrôle d'accès physique (locaux, applications...).

L'authentification simple disponible également dans les deux modes d'utilisation permet de simplifier le processus d'authentification sans imposer de saisie du code confidentiel après une authentification forte préalable (usage de type « badgeage à la volée ») tout en garantissant un niveau de sécurité acceptable.

L'authentification forte avec contact, et saisie du code confidentiel (code porteur) reste cependant l'usage classique de la carte. C'est le mécanisme standard d'authentification combinant une double authentification d'une part du porteur en tapant son code confidentiel et d'autre part de la carte au moyen d'un certificat électronique d'authentification. Ce cas d'usage permet de se protéger du risque de clonage du support. Cette authentification ne peut être mise en œuvre qu'en mode « contact », au moyen d'un lecteur approprié.

Le code porteur (code à 4 chiffres) est tapé par le professionnel de santé lors de l'introduction de la carte CPS3 dans le lecteur en début de journée. Tant que la carte n'est ni retirée du lecteur ni mise hors tension, les lectures suivantes ne nécessitent pas une nouvelle saisie du code. Celui-ci ne doit cependant pas être mémorisé par le progiciel du professionnel de santé.

Afin de s'authentifier fortement dans un système d'information, la carte CPS3 embarque un bi-clé RSA d'authentification de 1024 bits et son certificat d'authentification associé. Un bi-clé RSA pour l'authentification du support en mode sans contact ainsi que son certificat associé est également proposé afin de profiter des nouvelles fonctionnalités de la carte.

- **La signature électronique** des transactions et des messages électroniques par les professionnels de santé est reconnue par les administrations de l'Etat et les organismes de sécurité sociale comme garantissant l'identité et la qualité du titulaire de la carte ainsi que l'intégrité du document signé¹⁴³. La carte CPS3 embarque pour cela un bi-clé RSA de signature de 2048 bits associé à un certificat électronique de signature.

¹⁴³ Article R.161-58 du code de la sécurité sociale.

Le tableau ci-dessous résume les principales caractéristiques des différentes applications de la CPS3 et leurs usages (12) :

CARACTERISTIQUES ET USAGES	VOLET IAS ECC	VOLET CPS2TER
Accès par authentification simple (sans PIN)	✓	✗
Accès par authentification forte	✓	✓
Signature électronique	✓	✓
Compatibilité avec les lecteurs SESAM Vitale homologués	✗	✓
Utilisation du middleware Cryptolib et API-CPS	✗	✓
Utilisation avec le Middleware ASIP Santé « IAS ECC »	✓	✗
Lecture / Ecriture de données applicatives	✓	✗

Tableau 16 : Caractéristiques et usages des volets de la carte CPS3 (12).

Comme nous le verrons, les principales applications des fonctions de sécurité de la carte CPS équipant les pharmaciens sont destinées à :

- sécuriser l'utilisation du dossier pharmaceutique et des messageries sécurisées de santé au moyen du protocole SSL faisant appel au certificat numérique d'authentification de la carte CPS et au certificat SSL du serveur distant ;
- signer électroniquement chaque FSE et chaque lot de FSE et sécuriser leur télétransmission par l'usage du protocole S/MIME faisant appel au certificat numérique de signature de la carte CPS et au certificat du serveur distant. Cette fonction permettant de sécuriser l'envoi de courriers électroniques peut également être employée pour sécuriser la télétransmission des pièces justificatives ainsi que les correspondances électroniques entre professionnels.

A.3.5.4.d Capacités cryptographiques de la carte Vitale 2

La carte Vitale 2 bénéficie elle aussi des dernières avancées technologiques en matière de sécurité. Le site AMELI de l'assurance maladie en assure même la « *sécurité renforcée pour l'authentification de la carte et de son titulaire et pour la signature des feuilles de soins électroniques* » (80). L'Agence nationale de sécurité des systèmes d'information certifie d'ailleurs la carte Vitale 2 et ses deux applications comme étant « *en tout point conforme aux exigences du Référentiel général de sécurité pour le niveau *** et permet donc de générer des signatures électroniques présumées fiables* » (11) (81) (82). Il s'agit du seul niveau de sécurité permettant d'élaborer une signature présumée fiable telle qu'elle est prévue par l'article 1316-4 du code civil (67) (29).

Cette carte est en effet dotée d'un système d'exploitation développé par l'entreprise Morpho™ ou masque SESAM VITALE qui coordonne deux applications¹⁴⁴ :

- L'application ADELE (pour administration électronique) qui fournit des services de signature électronique, des fonctions d'authentification et de chiffrement des données ;
- L'application VITALE qui reprend les mêmes services que l'application ADELE mais est enrichie de services spécifiques dont Vitale 1 (11).

¹⁴⁴ Une 3^{ème} application : « AIP carte vitale 2 » (application d'initialisation et de personnalisation) est utilisée en phase de pré-personnalisation et de personnalisation puis est inactivée par la suite.

Chaque carte Vitale est donc munie d'un coprocesseur cryptographique susceptible d'assumer des fonctions de sécurité similaires à celles de la carte CPS3, à savoir (11):

- **une authentification simple** utilisant l'algorithme RSA avec des clés de 2048 bits et l'algorithme 3DES. L'utilisation d'un code porteur afin d'authentifier fortement le porteur d'une carte Vitale n'a pas été retenue pour des raisons pratiques d'utilisation. En conséquence, cette fonction demeure inactivée à ce jour. Le référentiel général de sécurité recommande pourtant que dans le cas de l'utilisation d'une carte à puce et tout particulièrement au niveau ***, d'utiliser un lecteur de carte à puce avec PIN/PAD intégré permettant de saisir son code d'activation (83).

- **une signature électronique** de type RSA PKCS#1 (2048 bits) avec fonction de hachage SHA-1 ou SHA-2 ;

- **le chiffrement de données** basé sur un algorithme 3DES.

Si la carte Vitale 2 embarque toute la technologie nécessaire à la mise en application de fonctions de sécurité reposant sur des techniques cryptographiques, aucun prestataire de service de certification électronique ne semble reconnu pour l'attribution de certificats électroniques aux porteurs de cartes Vitale et donc à chaque assuré. De même, aucune communication sur une éventuelle infrastructure de gestion de clé dédiée à la gestion des certificats électroniques de la carte Vitale n'a été réalisée qu'il s'agisse du GIE SESAM-Vitale ou de la Caisse nationale d'assurance maladie en raison de la sensibilité de ce sujet.

Dans son rapport annuel sur la sécurité sociale¹⁴⁵, la Cour des comptes soulignait l'absence de certificats électroniques dans les cartes Vitale 2 dès 2008. Il s'agissait pourtant de l'un des points fondamentaux mis en avant par la direction générale de la modernisation de l'Etat dès 2006 afin de sécuriser l'accès des usagers à tout service en ligne de données personnelles de santé. Ce constat, toujours d'actualité, est d'ailleurs réitéré par la Cour dans son rapport de 2013 sur la sécurité sociale et recommande « *d'imposer les certificats des cartes Vitale 2 comme partie intégrante du mode d'accès à tout service en ligne de données personnelles de santé* »¹⁴⁶.

Cette volonté d'implanter des certificats électroniques au sein des cartes vitale est née avec le développement des dossiers médicaux en ligne et particulièrement le dossier médical personnel afin que chacun puisse accéder et gérer son DMP en toute autonomie. Compte tenu du retard accumulé dans la finalisation et la généralisation du DMP, il n'existait pas encore d'autres téléservices destinés aux assurés nécessitant des fonctions de sécurité fortes en 2007. Cette voie fut donc abandonnée au profit de la remise d'un couple identifiant/mot de passe au patient lors de la création de son DMP.

Par ailleurs, la direction de la sécurité sociale aurait estimé le coût d'implantation de certificats électroniques dans chaque carte Vitale, entre 50 et 130 millions d'euros par an pour les cinq premières années. Ce coût est évalué par la Caisse nationale d'assurance maladie entre 0,85 et 2,2 euros par carte Vitale et par an. S'y ajoutent les frais liés à la mise en œuvre d'une lourde infrastructure de gestions de clés cryptographiques ainsi que le déploiement de

¹⁴⁵ Cour des comptes, Rapport 2008 sur l'application des lois de financement de la sécurité sociale, septembre 2008, chapitre VII, pages 223-262.

¹⁴⁶ Cour des comptes, Rapport public annuel de 2013, Les téléservices publics de santé : un pilotage toujours insuffisant, février 2013, Tome II, 2^{ème} partie, chapitre 2, page 364.

ces fonctions sur les postes des professionnels de santé, l'envoi postal des codes, le renouvellement des certificats...

Enfin, la nécessité pour l'utilisateur de disposer d'un lecteur approprié à domicile fut perçue comme un frein à l'utilisation de cartes à puces électroniques en tant que moyen d'authentification des patients dans un contexte d'accès autonome à un service web. Il s'agit également de l'une des raisons de l'abandon du projet de carte nationale d'identité électronique dont le fonctionnement devait également reposer sur l'utilisation de certificats électroniques. Des périphériques compatibles avec les ordinateurs de bureau sont pourtant disponibles à un faible coût (parfois moins de 10 euros) sous forme de lecteurs PC/SC. Ce type de matériel est d'ailleurs couramment utilisé par les citoyens Estoniens pour l'accès aux téléservices publics et notamment le vote aux élections.

Le projet de création d'une carte nationale d'identité électronique (CNIE) française a vu le jour dès 2007 sous l'impulsion de la création de l'agence nationale des titres sécurisés. Celle-ci devait faire l'objet d'un projet de loi déposé au Parlement au premier semestre 2008, et son déploiement devait avoir lieu en janvier 2009. C'est ainsi que la proposition de loi du 6 mars 2012 adoptée en séance ordinaire de l'Assemblée nationale¹⁴⁷ prévoyait initialement que la CNIE :

- soit munie d'un « *composant électronique sécurisé* » contenant le nom, le prénom, le sexe, la date et le lieu de naissance de son porteur ainsi que son adresse, sa taille et la couleur de ses yeux, ses empreintes digitales et sa photographie (article 2) ;

- contienne des données permettant au titulaire « *de s'identifier sur les réseaux de communications électroniques, et de mettre en œuvre sa signature électronique* » si celui-ci en fait la demande (article 3) ;

- fasse l'objet d'un traitement de données à caractère personnel et que l'accès à ces données puisse être accordé à certaines autorités sur autorisation du procureur de la république pour identifier le responsable d'une infraction au code pénal, au code de la route... (article 5) ;

C'est dans ce contexte que Monsieur le Président de la République Nicolas Sarkozy prévoyait l'évolution de la carte Vitale selon un système biométrique en se greffant sur le projet de la CNIE engagé quelques jours plus tôt afin de lutter contre les fraudes à l'assurance maladie¹⁴⁸. Le Conseil Constitutionnel a cependant émis certaines réserves quant à l'application de cette loi en déclarant plusieurs articles (notamment les articles 3 et 5) comme non conformes, limitant ainsi considérablement les services initialement proposés (84). La loi fut ainsi promulguée le 27 mars 2012¹⁴⁹ amputée de l'intérêt principal de son déploiement : l'attribution d'un certificat électronique à chaque citoyen français. Compte tenu de cette censure du Conseil Constitutionnel et du coût évalué à 85 millions d'euros par an, l'actuel ministre de l'intérieur Manuel Valls a finalement déclaré qu'il n'était « *pas souhaitable* » de développer un tel projet¹⁵⁰. Comme nous le verrons lors de l'étude des différents systèmes

¹⁴⁷ <http://www.assemblee-nationale.fr/13/ta/ta0883.asp>

¹⁴⁸ Monsieur le Président de la République Nicolas Sarkozy déclarait sur la chaîne de télévision BFM-TV le 8 mars 2012 « *Notre système social est le meilleur du monde, il est le plus généreux du monde, il nous impose de lutter contre la fraude* ».

¹⁴⁹ Loi n° 2012-410 du 27 mars 2012 relative à la protection de l'identité. JORF n°0075 du 28 mars 2012, page 5604.

¹⁵⁰ Réponse du ministre de l'intérieur Monsieur Manuel Valls (JORF 1^{er} janvier 2013) à la question au Gouvernement n°4746 du député Monsieur Philippe Meunier (JORF 18 septembre 2012).

d'e-santé européen, de telles cartes sont utilisées dans un contexte d'administration en ligne élargi en Estonie où elles assurent l'authentification des usagers pour l'accès à l'e-santé mais encore pour le paiement des impôts et de nombreuses démarches administratives.

Les principales étapes critiques de la sécurisation de la transmission de données électroniques étant assurées par la carte CPS, les conséquences d'une absence éventuelle de certificats associés à la carte Vitale restent pour le moment mesurées et concerneraient principalement des fraudes marginales à l'assurance maladie. Seules 56 fraudes auraient été dénombrées à ce titre en 2010, qui ont entraîné 21 saisines du parquet, une pénalité financière et 20 demandes de restitution de remboursements totalisant 255 668 euros¹⁵¹.

Selon certains spécialistes, il serait en effet possible de réaliser des clones de cartes Vitale à partir d'une carte valide dont les données administratives sont dupliquées et éventuellement modifiées afin de bénéficier illégalement de l'avance des frais de produits de santé dispensés par une officine. La médiatisation d'une telle faille de sécurité du système de facturation par la chaîne de télévision W9 en janvier 2010 démontrait qu'une telle carte pourrait permettre à un individu mal intentionné de bénéficier du tiers-payant pharmaceutique sans que la carte ne soit électroniquement détectée comme fausse. Ceci pourrait être en partie expliqué par la vérification des signatures des FSE qui n'est réalisée qu'*a posteriori*, après télétransmission du lot de FSE par le pharmacien en fin de journée, laissant le temps au fraudeur de disparaître.

Malgré l'évolution du visuel de la carte Vitale 2 enrichi de la photo de l'assuré, une carte vierge (*basic card*) falsifiée peut être rendue visuellement indétectable en tant que contrefaçon au moyen d'une imprimante adaptée capable de reproduire ce visuel sur une carte vierge.

L'intérêt d'implanter de telles mécanismes de sécurité dans la carte Vitale consisterait donc principalement à :

- authentifier la carte, sans ambiguïté, comme étant liée à l'identité de son porteur par exemple dans un contexte de facturation ou d'accès autonome du patient à son dossier pharmaceutique ou à son DMP...

- élaborer une signature électronique présumée fiable du patient pour signer les feuilles de soins électroniques, conformément à l'article R.161-43 du code de la sécurité sociale.

Ce dernier point est cependant mal explicité par le code de la sécurité sociale puisque qu'il rend obligatoire les signatures manuscrites « *de l'assuré et du ou des professionnels ayant effectué les actes ou servi les prestations* » des feuilles de soins papiers mais ne précise ni l'origine, ni la nature exacte des signatures électroniques des feuilles de soins électroniques « *données par la lecture* » des cartes Vitale et CPS.

Elément fondamental de toute politique d'e-santé, le traitement automatisé des données personnelles relatives aux patients à l'officine obéit donc à de nombreuses contraintes techniques et juridiques permettant d'assurer leur hébergement et leur échange en toute sécurité. La confidentialité et la sécurisation des données ne sont toutefois pas seulement affaires de technique, de politique et de droit, mais aussi de comportement. Il est donc primordial d'informer et de sensibiliser tous les acteurs des systèmes d'information de santé à des usages et des points de vigilance nouveaux (85).

¹⁵¹ Cour des comptes, Rapport public annuel de 2013, Les téléservices publics de santé : un pilotage toujours insuffisant, février 2013, Tome II, 2^{ème} partie, chapitre 2, page 365.

Partie B : LA DEMATERIALISATION AU QUOTIDIEN DU PHARMACIEN D'OFFICINE

L'informatisation progressive des officines françaises permet aujourd'hui d'automatiser de nombreuses tâches, facilitant l'exercice professionnel des pharmaciens. Le logiciel de gestion d'officine, au cœur du système informatique officinal, offre une panoplie d'outils performants au service des pharmaciens leur promettant de nombreux bénéfices au quotidien.

Outre la gestion des prix, des ventes, des stocks et des commandes de l'officine, l'informatique assiste les pharmaciens dans l'accomplissement de leurs missions quotidiennes. La dématérialisation s'est initialement invitée dans l'exercice officinal sous l'impulsion de la Caisse nationale d'assurance maladie dans l'optique de moderniser notre système de santé et d'en améliorer l'efficacité. En effet, toute dispensation donnant lieu à une prise en charge financière par un organisme d'assurance maladie fait l'objet d'échanges de documents justificatifs entre la personne ayant avancé les frais et l'assurance maladie. Lorsqu'un assuré bénéficie du tiers-payant pharmaceutique, le pharmacien avance les frais pour son compte et sera directement remboursé par la caisse concernée. Afin d'améliorer la qualité et la sécurité de ces échanges, les premiers pas de la dématérialisation au sein des systèmes d'information de santé furent marqués par la dématérialisation des feuilles de soins et l'obligation de les télétransmettre par voie électronique. Désormais étendue aux demandes de remboursement électronique à destination des organismes complémentaires, l'assurance maladie a récemment franchi un pas décisif dans la modernisation de notre système de santé en généralisant la numérisation des ordonnances par les pharmaciens d'officine.

En automatisant de nombreuses tâches liées à la dispensation des produits de santé, les pharmaciens bénéficient d'un gain de temps et d'attention à l'égard des patients. Les logiciels utilisés par les professionnels de santé permettant de sécuriser les processus de prescription et de dispensation doivent être distingués des outils accessibles « en ligne » tels que le dossier pharmaceutique, le dossier médical personnel (DMP) ou le web-médecin dont l'utilisation partagée sur l'ensemble du territoire favorise la coopération entre professionnels de santé ainsi que le suivi de patients dont la mobilité ne cesse de croître. La finalisation et la généralisation du DMP devraient ainsi permettre d'étoffer notre modèle d'e-santé déjà doté d'un outil d'e-dispensation performant proposé par l'ordre des pharmaciens : le dossier pharmaceutique.

Compte tenu des orientations stratégiques visant à enrichir les missions des pharmaciens d'officines, les TIC pourraient constituer un atout majeur pour faciliter et optimiser leur exercice quotidien, au bénéfice de la santé de leurs patients.

Enfin, le développement des techniques d'acquisition, de transmission et d'hébergement des données offre d'incroyables perspectives d'avenir pour les systèmes d'information en santé et particulièrement l'e-prescription, déjà opérationnelle dans certains pays membres de l'Union européenne. Nous verrons comment un tel outil pourrait favoriser l'épanouissement du e-pharmacien correspondant, né de la loi HPST et permettre de finaliser notre système d'e-Santé.

Chapitre 1 : LES ECHANGES DEMATERIALISES AVEC L'ASSURANCE MALADIE

La télétransmission de feuilles de soins au format électronique a permis de réaliser le premier pas d'un long chemin vers la dématérialisation totale des échanges entre les professionnels de santé et les organismes d'assurance maladie. En permettant aux pharmaciens de numériser les 550 millions d'ordonnances qui leur sont présentées chaque année, une nouvelle étape fut récemment franchie. L'assurance maladie estime ainsi que la surface liée à l'archivage des pièces justificatives papier dans les caisses représentait 424 kilomètres linéaires chaque année. A titre d'exemple, dans la caisse primaire d'assurance maladie de Bobigny, ce sont 132 mètres linéaires d'ordonnances papier qui sont archivés chaque mois. A Paris, six tonnes d'ordonnances parviennent chaque semaine à la caisse. De plus, la collecte des ordonnances papier par l'assurance maladie auprès des pharmacies représentait une dépense de quatre millions d'euros chaque année. Tout laisse donc à penser que la dématérialisation des pièces justificatives par les professionnels de santé permettra de réduire considérablement cet espace d'archivage et les coûts liés à leur traitement (86).

Faciliter les relations avec les professionnels de santé, simplifier leurs tâches administratives et gagner en efficacité constituent ainsi des engagements forts de l'assurance maladie, conformément à la volonté de moderniser notre système de santé du Ministère du travail, de l'emploi et de la santé.

B.1.1. LA MODERNISATION DU SYSTEME DE FACTURATION DES PRODUITS DE SANTE

B.1.1.1 CONTEXTE REGLEMENTAIRE

Les difficultés financières de notre régime de protection sociale ont conduit le Gouvernement à adopter de nombreuses mesures destinées à limiter le déficit de la sécurité sociale. Les ordonnances adoptées par le Gouvernement Juppé en avril 1996 se sont intégrées dans un plan global de réforme de notre système de santé.

Auparavant, les données de facturation étaient établies, sur une facture papier normalisée ou feuille de soins matérialisant les données de facturation d'actes de soins ou de produits de santé dispensés à un assuré, aux organismes d'assurance maladie. Co-signé par l'assuré et le professionnel de santé, ce document conforme au modèle CERFA en vigueur atteste du paiement de tout ou partie des prestations effectivement reçues par l'assuré. Le modèle destiné aux pharmaciens correspond au type « S3115g » qui renseigne notamment le code CIP des produits de santé facturés par le biais de la vignette pharmaceutique décollée du conditionnement extérieur du produit et apposé sur la feuille. Comme nous le verrons, cette procédure peut toutefois être toujours utilisée en cas d'impossibilité d'établir une feuille de soins électronique.

L'instauration de la carte Vitale a ainsi rendue nécessaire l'informatisation des officines et des cabinets médicaux afin de permettre la dématérialisation des feuilles de soins et leur télétransmission aux organismes d'assurance maladie d'ici la fin de l'année 1998. Depuis, 22 885 pharmaciens télétransmettaient les feuilles de soins à l'assurance maladie en 2012, soit 98,4 % d'entre eux. Il s'agit de la profession de santé qui atteint le meilleur taux de télétransmission, de 20 points supérieur à la moyenne (78,65 %). Les médecins généralistes télétransmettent à 85,6 %, les spécialistes à 62,1 %, les centres de santé à 49,3 % (20).

Le principe général repose sur l'édition d'un fichier électronique ayant même force probante que la traditionnelle feuille de soins papiers ou feuille de soins électronique (FSE) « dont la

signature est donnée par la lecture de la carte Vitale et de la carte de professionnel de santé »¹⁵². Les modalités de mise en œuvre de la télétransmission à l'officine sont régies par la Convention nationale organisant les rapports des pharmaciens avec l'assurance maladie.

Lorsqu'elle est électronique, la feuille de soin véhicule les données de facturation et donc le code CIP par le biais de normes d'échanges permettant de formaliser l'interprétation de leur contenu par les différents acteurs du système (en l'occurrence les pharmaciens et les organismes d'assurance maladie)¹⁵³. La dématérialisation de ce formulaire en facture électronique a bouleversé le schéma de facturation et de remboursement des actes de soins et des produits de santé. Le pharmacien adresse ainsi la feuille de soins électronique par télétransmission aux caisses d'assurance maladie, pour le compte de l'assuré social. Dans ce cas, le pharmacien estampille la vignette ou le code-barres resté sur le conditionnement du produit de santé¹⁵⁴ afin d'éviter une réutilisation frauduleuse de ce dispositif.

Cette obligation de télétransmission des feuilles de soins électroniques également affirmée par le code de la sécurité sociale¹⁵⁵ est aujourd'hui assortie d'une obligation de télétransmission de pièces justificatives par différentes catégories de professionnels de santé parmi lesquels les pharmaciens font figure de proue étant donné leur forte implication au dispositif de télétransmission existant.

L'objectif pour les pharmaciens est de remplacer le duplicata de l'ordonnance originale d'un patient sur lequel le pharmacien imprimait les données de facturation de la prestation, par une copie numérique de l'ordonnance à laquelle sont associées les données de facturation, sous forme d'un fichier au format PDF. Ces duplicatas papiers étaient regroupés en lot puis transmis par voie postale parallèlement aux lots de feuilles de soins électroniques transmis par voie dématérialisée. Ce duplicata doit permettre aux organismes d'assurance maladie concernés de vérifier que les données effectivement facturées correspondent à la prestation servie et aux modalités de sa prise en charge. En numérisant l'ordonnance originale du patient au moment de la dispensation, il est ainsi possible de s'affranchir de l'envoi de ces duplicatas papier et ainsi, de dématérialiser la quasi-totalité des échanges entre l'officine et les organismes d'assurance maladie pour la facturation des produits de santé.

Cette dernière simplification administrative vise à améliorer la gestion des quelques 550 millions d'ordonnances papier qui transitent dans les officines françaises chaque année en d'alléger cette lourde procédure, consommatrice de temps à la fois pour les caisses et les officines. Les objectifs sont multiples : faciliter les relations entre les pharmaciens et l'assurance maladie, simplifier leurs tâches administratives et améliorer l'efficacité du système de santé¹⁵⁶. La dernière convention pharmaceutique prévoit par ailleurs de poursuivre les efforts ainsi entrepris en dématérialisant la prescription à la source ainsi que sa transmission par voie électronique¹⁵⁷.

¹⁵² Arrêté du 4 mai 2012 portant approbation de la convention nationale organisant les rapports entre les pharmaciens titulaires d'officine et l'assurance maladie, article 36.3.1 Qualification de la feuille de soins au regard des modes de transmission.

¹⁵³ Arrêté du 4 mai 2012 portant approbation de la convention nationale organisant les rapports entre les pharmaciens titulaires d'officine et l'assurance maladie, articles 36.3.2, 36.4.1, 36.4.2.

¹⁵⁴ Article R.161-51 du code de la sécurité sociale.

¹⁵⁵ Article L.161-35 du code de la sécurité sociale.

¹⁵⁶ Une enquête de la Caisse primaire d'assurance maladie de décembre 2011 estime que la numérisation des ordonnances par les pharmaciens d'officine leur offre un gain de temps allant jusqu'à 2h par jour.

¹⁵⁷ Arrêté du 4 mai 2012 portant approbation de la convention nationale organisant les rapports entre les pharmaciens titulaires d'officine et l'assurance maladie, article 36.5.1 la dématérialisation de la prescription.

Afin de nourrir cet élan vers une dématérialisation toujours plus étendue des données de santé, les taux de télétransmission de FSE ainsi que l'intégration au dispositif de numérisation des pièces justificatives font aujourd'hui partie des indicateurs du principe de rémunération sur objectif affirmé par la convention pharmaceutique¹⁵⁸. En effet, si le seuil de télétransmission de 95% des FSE est atteint, les pharmaciens perçoivent une contribution d'un montant de 0,05 € par FSE élaborée, émise et reçue par les caisses selon les spécifications du système SESAM-Vitale. S'il utilise un dispositif conforme à la version 1.40 du cahier des charges SESAM-Vitale, cette contribution atteint 0,064 € par FSE. Par ailleurs, les pharmaciens qui numérisent les pièces justificatives et qui les adressent à la caisse perçoivent une rétribution totale de 418,60 €. Ces contributions financières versées annuellement par l'assurance maladie permettent aux pharmaciens de financer une partie de l'équipement nécessaire pour atteindre ces objectifs¹⁵⁹.

B.1.1.2 CONTEXTE TECHNIQUE

Afin d'élaborer les outils techniques les plus adaptés à ce dispositif, le cahier des charges publié par le GIE SESAM-Vitale impose des contraintes d'efficacité et de sécurité toujours plus fortes aux éditeurs de logiciels de gestion d'officine et plus particulièrement concernant le progiciel de facturation. Parmi ces innovations, il est désormais possible de télétransmettre simultanément les FSE aux organismes d'assurance maladie obligatoire (AMO) et les demandes de remboursement électroniques (DRE) aux organismes complémentaires (AMC). En effet, dès lors que l'assuré fournit les éléments nécessaires et suffisants à la prise en charge d'une part complémentaire des dépenses de santé, il peut bénéficier de l'avance de ces frais ainsi que de la télétransmission de ces données de facturation complémentaires aux organismes concernés¹⁶⁰. Afin de mieux comprendre les opérations du processus de facturation à l'officine il est possible de résumer la succession des événements à l'échelle d'une journée de travail.

En début de journée, lorsque le pharmacien met en route son système informatique, il introduit sa carte CPS dans le lecteur bi-fente homologué et s'identifie par saisie de son code porteur sur le clavier du lecteur ou par le biais de son logiciel (qui n'a d'ailleurs aucune vocation à l'enregistrer).

Lorsqu'un patient se présente à l'officine muni d'une ordonnance réglementairement valable, d'une carte Vitale à jour et d'une attestation de prise en charge complémentaire éventuelle, le pharmacien insère la carte Vitale du patient dans le lecteur bi-fente homologué, et accède à son logiciel de gestion d'officine. Il sélectionne le mode de facturation « tiers-payant » proposé par le progiciel qui procède à la lecture de la carte Vitale. Le pharmacien saisit manuellement ou à l'aide d'une carte à puce (carte Vitale ou autre) les données relatives à une éventuelle part complémentaire. Les données nécessaires à l'identification du patient et à la facturation sont remontées au progiciel afin de constituer la fiche informatisée du patient.

Il renseigne les informations relatives à l'ordonnance (identification du prescripteur, date de prescription) puis scanne la vignette de chaque conditionnement à dispenser. Le progiciel dresse la liste des produits facturés classés par code CIP en précisant les quantités délivrées. Pour chaque ligne de facturation, les montants des parts obligatoires et complémentaires facturées sont précisés ainsi que le montant total. Le pharmacien introduit l'ordonnance

¹⁵⁸ Arrêté du 4 mai 2012 portant approbation de la convention nationale organisant les rapports entre les pharmaciens titulaires d'officine et l'assurance maladie, article 30.

¹⁵⁹ Arrêté du 4 mai 2012 portant approbation de la convention nationale organisant les rapports entre les pharmaciens titulaires d'officine et l'assurance maladie, articles 31.1.1 et 31.1.2.

¹⁶⁰ Sous réserve que le pharmacien ait signé une convention avec ledit organisme complémentaire.

originale dans le scanner et la numérise, l'image encapsulée dans un fichier PDF est ensuite remontée au progiciel. Avant de rendre l'ordonnance au patient, le pharmacien imprime sur celle-ci les informations relatives à la facturation ou « ticket vitale patient » prévu par la convention pharmaceutique *« permettant de garantir aux assurés sociaux une bonne information sur le coût des produits de santé qui leur sont délivrés. »*¹⁶¹.

En fin de journée, le progiciel procède à la mise en lots des FSE enregistrées au cours de la journée auxquelles sont associés les lots de pièces justificatives correspondants (ordonnances numérisées et données de facturation associées). Selon le cas, des FSE et des DRE sont envoyées aux organismes d'AMO et/ou d'AMC tandis que les pièces justificatives ne sont transmises qu'aux organismes d'AMO. Un système d'accusé de réception permet au pharmacien de s'assurer, *a posteriori*, de la bonne transmission des données et d'éventuels rejets de paiement. Sauf anomalie, les caisses procèdent ainsi au paiement du pharmacien ayant avancé les frais pour le compte du patient dans un délai de quatre jours.

B.1.2. LA DEMATERIALISATION DES FEUILLES DE SOINS

Les factures de produits de santé pris en charge par les organismes d'assurance maladie sont générées par le progiciel de facturation intégré au logiciel de gestion d'officine, sous forme de factures électroniques. La convention pharmaceutique permet d'apporter quelques définitions permettant de distinguer différents types de factures électroniques selon les modalités de prise en charge ainsi que leur modalité de transmission et le contexte technique.

On distingue :

- **Les FSE (feuilles de soins électroniques)** : feuilles de soins dont la signature est donnée par la lecture de la carte Vitale et de la carte de professionnel de santé au moyen d'un lecteur homologué.

Le processus d'élaboration de ces factures électroniques est étroitement lié à la manière dont les flux sont sécurisés et télétransmis. On entend par **feuille de soins SESAM « dégradée »** la feuille de soins dont la signature est donnée par la lecture de la seule carte du professionnel de santé.

On entend enfin par **feuille de soins « en norme IRIS B2 »** la feuille de soins télétransmise hors du dispositif SESAM-Vitale, sans carte CPS et sans faire appel au module SESAM-Vitale. Les flux SESAM-Vitale dégradés sont sécurisés tandis que les flux IRIS sont élaborés dans le cadre d'un contrat passé directement entre le professionnel de santé et sa caisse d'assurance maladie et ne sont pas sécurisés (87).

Lorsqu'il est impossible pour le pharmacien de générer une FSE, il peut toujours avoir recours à la traditionnelle feuille de soins papier matérialisant la facturation des produits de santé délivrés, aux régimes d'assurance maladie. Le progiciel de facturation officinal est capable d'imprimer directement les données nécessaires à la facturation en se calquant sur ce modèle.

- **Les DRE (demandes de remboursement électroniques)**, lorsque le patient présente les justificatifs ouvrant droit à une prise en charge d'une partie des dépenses par un organisme complémentaire avec lequel le pharmacien a passé une convention.

¹⁶¹ Arrêté du 4 mai 2012 portant approbation de la convention nationale organisant les rapports entre les pharmaciens titulaires d'officine et l'assurance maladie, article 36.5.2.

Lorsque le professionnel de santé réalise une FSE et une DRE, les deux factures sont établies sur la base des mêmes informations ce qui en garantit la cohérence. Les informations nécessaires au remboursement de la part obligatoire sont transmises dans la FSE tandis que les informations nécessaires au remboursement d'une éventuelle part complémentaire peuvent être transmises, selon les conditions de génération des flux, soit dans la DRE, soit dans la FSE (25).

Il est alors possible de distinguer différents schémas de facturation :

- Constitution d'une **FSE sans DRE** où deux cas sont à distinguer :
 - **La FSE ne comporte que des données nécessaires au remboursement de la part obligatoire :** lorsque la prestation ne fait pas l'objet d'une part complémentaire remboursable, lorsque l'assuré ne cotise pas à un organisme AMC ou que le professionnel de santé n'a pas signé de convention avec l'organisme sollicité.
 - **La FSE comporte des données nécessaires au remboursement de la part obligatoire et de la part complémentaire :** lorsque l'AMO ou l'AMC gère à la fois les parts obligatoires et complémentaires (on parle dans ce cas de FSE enrichie) ou si le professionnel de santé délègue l'éclatement des flux à un organisme concentrateur technique ayant signé une convention avec l'organisme d'AMC concerné.
- Constitution d'une **FSE avec DRE** : lorsqu'une prestation dont la part obligatoire fait l'objet d'une FSE et pour laquelle il reste une part complémentaire à rembourser par un organisme d'AMC. Les deux flux peuvent être adressés :
 - Séparément et directement aux organismes d'assurance maladie concernés : la FSE est adressée directement à l'AMO tandis que la DRE est adressée directement à l'AMC ;
 - A un organisme concentrateur technique qui procède à un « éclatement des flux » et les transmettra aux organismes d'AMO et d'AMC concernés dûment informés de l'éclatement des flux.
- Constitution d'une **DRE sans FSE** : lorsque le professionnel de santé réalise une prestation dont la part complémentaire est facturée seule ou si une prestation n'est prise en charge que par un organisme complémentaire.

Dans le cas particulier de l'élaboration d'une FSE dans le cadre de la délivrance d'une contraception d'urgence à une personne mineure et pour assurer son anonymat, les pharmaciens peuvent utiliser le mode de sécurisation SESAM sans vitale. Un NIR fictif est attribué à la patiente dont la date de naissance est enregistrée et la FSE sera directement télétransmise à la Caisse primaire d'assurance maladie de la circonscription du lieu d'implantation de la pharmacie.

B.1.2.1 LA PREPARATION DES FACTURES ELECTRONIQUES

Les éléments constitutifs des FSE et des DRE sont créés et importés sur le poste de travail du pharmacien à partir :

- **D'informations définies réglementairement¹⁶² :**
 - informations d'identification, de situations d'exercice et de facturation du pharmacien contenues dans sa carte CPS et/ou sur son poste de travail ;
 - informations contenues dans la carte Vitale identifiant le bénéficiaire et la caisse d'AMO dont il dépend ainsi que ses droits ;
 - informations saisies par le pharmacien ;
 - d'autres données enregistrées dans le logiciel de gestion d'officine (aide médicale d'Etat, couverture maladie universelle...) ;
- **D'informations définies conventionnellement :** il s'agit des données relatives aux conventions qui lient le professionnel de santé aux organismes d'AMO ;
- **Eventuellement d'informations liées à la part complémentaire :**
 - informations contenues dans la carte Vitale ou tout autre support d'AMC identifiant l'organisme complémentaire et les droits de l'assuré pour la part complémentaire ;
 - données relatives à la convention qui lie le professionnel de santé aux organismes gérant à la fois les parts obligatoire et complémentaire.

L'élaboration des factures électroniques fait appel aux supports d'identification des patients et des pharmaciens (cartes Vitale et CPS) ainsi qu'à leurs lecteurs, mais encore à des composantes logicielles telles que le logiciel de gestion d'officine et les modules fournis par la bibliothèque SESAM-Vitale.

La succession des étapes permettant l'élaboration et la mise en forme des lots de factures électroniques est décrite par le cahier des charges SESAM-Vitale et le cahier des charges relatif à la norme de télétransmission B2 défini par l'assurance maladie et consistent en (25) (88) :

- **L'acquisition des données relatives au pharmacien¹⁶³** reposant sur la lecture de sa carte CPS via la fonction **SSV_LireCarteCPS¹⁶⁴**. Il n'est cependant pas imposé une lecture systématique de la carte CPS pour chaque facture. La carte est introduite dans le lecteur en début de journée et le pharmacien s'authentifie en tapant son code porteur une seule fois¹⁶⁵. Il réalise une première lecture de la CPS puis pourra réutiliser l'information autant de fois que désiré sans avoir à retaper son code porteur, tant que la carte n'aura pas été retirée du lecteur.

¹⁶² Article R.161-42 du code de la sécurité sociale.

¹⁶³ Cette acquisition peut ne pas être effectuée systématiquement pour chaque facture, les données obtenues lors d'un accès pouvant être stockées et réutilisées ultérieurement.

¹⁶⁴ D'autres données paramétrées sur le poste de travail du professionnel de santé peuvent également recueillies.

¹⁶⁵ Si le code porteur peut être techniquement fourni par le logiciel du professionnel de santé celui-ci n'a pas vocation à le mémoriser.

ACQUISITION DES INFORMATIONS DE LA CARTE CPS
Groupe titulaire carte PS
- Type de carte (CPS, CPE...) - Type d'identification nationale : ADELI, RPPS... - Numéro d'identification nationale du professionnel de santé et sa clé - Code civilité, nom et prénom du professionnel de santé
Groupe situation du PS
- Numéro logique de situation de facturation du professionnel de santé - Mode d'exercice (libéral, salarié, remplaçant...) - Secteur d'activité (pharmacie) - Identification de la structure (type, n° d'identification et clé, raison sociale) - Numéro d'Identification de facturation du professionnel de santé et sa clé - Code conventionnel liant le professionnel de santé à l'AMO - L'habilitation à signer les factures et les lots

Tableau 17 : Résumé des informations relatives au pharmacien remontées par le progiciel de facturation (25).

- **L'acquisition des données relatives à l'assuré** peut faire appel à la carte Vitale ou tout autre support éventuel telle une attestation de droit papier ou directement enregistrées par le logiciel de gestion d'officine. Lors de la réalisation d'une facture en mode sécurisé, ces données sont fournies par la lecture de la carte Vitale via la fonction **SSV_LireDroitsVitale** ou par le progiciel. Lors de la réalisation d'une facture en mode SESAM Vitale dégradée, ces données sont saisies par le professionnel de santé ou fournies par le progiciel.

ACQUISITION DES INFORMATIONS DE LA CARTE VITALE
Données relatives à l'assuré et à la carte
- Type de carte Vitale, numéro de série et date de fin de validité - Numéro national d'immatriculation (NIR) et sa clé - Le code régime, la caisse et le centre gestionnaires ainsi que le code gestion - Nom, prénom, adresse du bénéficiaire - Date et rang de naissance, qualité (lien de parenté avec l'assuré) - Dates de début et de fin du service AMO
Données relatives à la prise en charge
- Dates de début et de fin de droits AMO et AMC - Identification et garanties effectives des mutuelles pour lesquelles le bénéficiaire est couvert par l'organisme d'AMC - Identification des bénéficiaires de la CMU-C, d'ALD ou d'AME

Tableau 18 : Résumé des informations relatives au patient remontées par le progiciel de facturation (25).

Le cahier des charges SESAM Vitale précise qu'à ce stade, le progiciel du professionnel de santé doit être capable :

- **de vérifier les dates de validité de la carte** et ne permettre la facturation qu'en mode dégradé si celle-ci est invalide ;
- **de vérifier la non-opposition de la carte** en consultant la liste d'opposition et le cas échéant, avertir le professionnel de santé de la mise en opposition de la carte et empêcher la création de flux vers les organismes d'assurance maladie.

- **L'acquisition des informations relatives à la prestation** est réalisée par saisie du code d'identification du produit de santé délivré (manuellement ou par lecture du code-barres de la vignette ou du code Datamatrix). Le pharmacien précise la quantité d'unités dispensées pour chaque ligne de facturation. Sont également pris en compte la date à laquelle chaque acte ou prestation a été servie ainsi que les données d'identification du professionnel de santé prescripteur telles que :

- le numéro d'identification de facturation et le numéro RPPS du prescripteur ;
- la condition d'exercice et l'identification de la structure dans laquelle il exerce ;
- la date de la prescription ;

- **La tarification de la part obligatoire** est réalisée en appliquant les règles de tarification permettant le calcul de remboursement des différentes prestations par les organismes d'AMO. Ces règles permettent de déterminer la base de remboursement et le taux de remboursement au moyen du service SRT et de calculer ainsi le montant remboursable par l'AMO.

- **La tarification de la part complémentaire** est réalisée par le progiciel selon les informations recueillies par le pharmacien à partir de tout support de droit AMC. Lorsqu'il utilise la carte Vitale, il fait appel au service STS qui détermine les droits au remboursement de la part complémentaire.

- **La zone d'échange facture** est composée d'un ensemble de groupes de données relatives au patient, au professionnel de santé, à la prestation et à sa tarification. Ces groupes de données sont comme des blocs assemblés et transmis au module SSV afin de procéder à la mise en forme de la facture. Une présentation des groupes de la zone d'échange de facture utilisés lors de la facturation des produits de santé est disponible en annexe 6.

B.1.2.2 LA MISE EN FORME DES FACTURES ET DES LOTS

Les différents groupes de données de la zone d'échange sont exploités par le progiciel et le module SSV afin d'assurer la mise en forme des factures. La fonction **SSV_FormaterFacture** détermine s'il s'agit d'une FSE et/ou d'une DRE ainsi que le mode de sécurisation de la facture après vérification du code porteur du professionnel de santé.

Quelles soient électroniques ou non, les feuilles de soins transmises aux caisses doivent comporter le codage des produits de santé facturés. Lorsqu'elle est établie sur format papier, ce code est communiqué en collant la vignette pharmaceutique. Si les données de facturation sont transmises par voie électronique, le code est transmis par le biais de la **norme d'échanges** en cas de télétransmission d'une FSE ou d'une feuille de soins SESAM « dégradée ».

Cette norme d'échange est la **norme « B2 inter-régimes »** élaborée en commun par les différents organismes d'assurance maladie afin d'exprimer les données de facturation sous forme codifiée, dans le respect du secret médical en reflétant exactement la facturation retracée sur le support papier. Afin de garantir une interopérabilité des systèmes utilisés pour la facturation, l'élaboration des FSE et des DRE repose sur l'utilisation des mêmes informations issues de la zone d'échange et utilise ce même standard¹⁶⁶.

¹⁶⁶ Les DRE sont en réalité élaborées selon la norme intitulée DRE/DR ou simplement norme DRE dont le principe est basé sur celui de la norme B2 afin de garantir l'interopérabilité des systèmes.

Les factures électroniques générées par le pharmacien au cours d'une journée de travail sont télétransmises sous forme de fichiers de lots de factures. Il est ainsi créé un fichier par organisme destinataire de chaque grand régime. Tout comme il existe différents modèles de feuilles de soins conformes aux modèles CERFA selon la catégorie du professionnel de santé concerné, la norme B2 permet d'exprimer différentes informations selon le mode d'exercice. Nous nous concentrerons donc sur la **norme B2 de type PH** utilisée par les progiciels de facturation officinaux agréés par le centre national de dépôt et d'agrément.

Le principe de constitution d'un fichier B2 repose sur un assemblage hiérarchisé d'informations dont chaque niveau est représenté par un **Type** (88):

- les factures sont regroupées en **lots** (fonction **SSV_FormaterLot**) pour un même code organisme destinataire d'un même code grand régime. Chaque lot regroupe de 1 à n factures bornées par un enregistrement Type 2 (début) puis Type 5 (fin) dont le contenu est constitué de 1 à n lignes représentées dans les enregistrements de Type 4. Les factures sont classées à l'intérieur de chaque lot dans l'ordre croissant de leur numéro d'édition, la référence doit être impérativement différente d'un lot à l'autre et évolutive de 001 à 999 pour une FSE et de AAA à ZZZ une DRE.

- chaque **fichier** borné par un enregistrement de Type 000 en début et de Type 999 en fin est créé par la fonction **SSV_FormaterFichier**. Un fichier est constitué d'un ou plusieurs lots bornés par un enregistrement Type 1 (début) et Type 6 (fin). L'architecture globale de chaque fichier peut être représentée ainsi (88):

Type 000 *Début de fichier*

Type 1 *Début de lot*

Type 2 *Début de facture*

Types 4 et 4n *Ligne de facture*

Type 5 *Fin de facture*

Type 6 *Fin de lot*

Type 999 *Fin de fichier*

Certains Types sont facultatifs et permettent de véhiculer des informations complémentaires relatives à la facturation (Types 2S...). La codification de chaque ligne de facture (Types 4) de la norme B2/PH fait appel à des types spécifiques permettant la facturation des produits de santé codifiés par un code CIP (Types 4P, 4R) et la facturation des produits de la LPP (Type 4F). L'ensemble des informations susceptibles d'être exprimées par chaque Type à la norme B2/PH est précisé dans l'annexe 7.

S'il est ainsi possible de comprendre l'architecture des fichiers transmis, qu'en est-il de la sauvegarde du secret médical ?

Les informations véhiculées dans les enregistrements de type 4P, 4R et 4F font l'objet d'un archivage particulier susceptible d'être interrogées par les services administratifs des organismes d'assurance maladie ou par le service médical placé auprès d'eux. Toutefois, conformément à l'article L.161-29 du code de la sécurité sociale, seul le service médical est habilité à procéder à un chaînage complet, n° immatriculation, date de naissance du bénéficiaire, actes ou produits dispensés avec un code spécifique. Ces informations ne sont donc pas transmises aux organismes de protection complémentaire (88).

- **La signature des FSE et des DRE** emploie des modes de sécurisation identiques. L'article R.161-43 du code de la sécurité sociale rappelle que les feuilles de soins doivent être signées à la fois par le patient et par le professionnel de santé. Il précise en outre que lorsqu'elles sont électroniques « *les signatures sont données par la lecture* » de la carte Vitale et de la carte CPS. « *Le procédé technique mis en œuvre doit garantir le maintien, dès l'obtention de la signature du bénéficiaire, de l'intégrité des données constitutives de la feuille de soins jusqu'à transmission de celle-ci aux fins de remboursement* » ;

Il existe principalement deux modes de sécurisation des flux de télétransmission selon la situation :

- Le mode de sécurisation **SESAM-Vitale** qui nécessite soit la présence simultanée des cartes CPS et Vitale dans le lecteur, soit une sécurisation en 2 temps dite **désynchronisée** (la première sécurisation est réalisée en présence de la carte Vitale seule puis la deuxième en présence de la carte CPS seule). Ce dernier mode est surtout utilisé par les professionnels en visite médicale ou en cas de problème technique.

- Le mode de sécurisation **SESAM-Vitale dégradé**, dans lequel, la carte Vitale étant absente, la sécurisation est réalisée par la carte CPS seule.

- **Le chiffrement des données sensibles de la facture** est réalisé, comme nous l'avons vu, par le logiciel lecteur au moyen de techniques de cryptographie symétrique : 3DES en mode CBC (clé de session de 128 bits) (25).

- **L'inscription des références de la facturation sur l'ordonnance papier¹⁶⁷ ou « ticket vitale » pour les pharmaciens** comporte les références permettant le rapprochement de l'ordonnance avec la FSE de l'exécutant et garantissant aux assurés sociaux une bonne information sur le coût des produits de santé qui leur sont délivrés, telles que :

- la date d'exécution et l'identification du pharmacien chargé de la délivrance ;
- le nom, le prénom et le NIR (ou la date de naissance) du bénéficiaire des soins ;
- l'identification de la caisse d'assurance maladie obligatoire de l'assuré ;
- le montant de la somme effectivement payée par l'assuré pour l'achat de chacun des produits ou articles délivrés¹⁶⁸ ;
- le montant total des produits délivrés ainsi que la part prise en charge par le régime d'assurance maladie obligatoire du patient.

Afin d'optimiser la volumétrie des données transportées, les fichiers de factures (FSE et DRE) peuvent être compressés au format ZIP¹⁶⁹ avant télétransmission. Nous verrons par la suite de quelle façon le fichier SMTP d'envoi est créé et sécurisé au format S/MIME. Chaque fichier est enregistré par le logiciel de facturation sur le poste de travail jusqu'au 1^{er} ARL (accusé

¹⁶⁷ D'après l'article R.161-45 du code de la sécurité sociale.

¹⁶⁸ Article L.162-36 du code de la sécurité sociale.

¹⁶⁹ Les spécifications relatives aux archives ZIP sont fournies par PKWARE : <http://www.pkware.com/support/zip-app-note>. L'algorithme de compression à utiliser est référencé dans la RFC 1952 « *GZIP file format specification version 4.3* » ou supérieure.

de réception logique) positif d'un lot contenu dans le fichier, afin de prévoir les cas possibles de réémission.

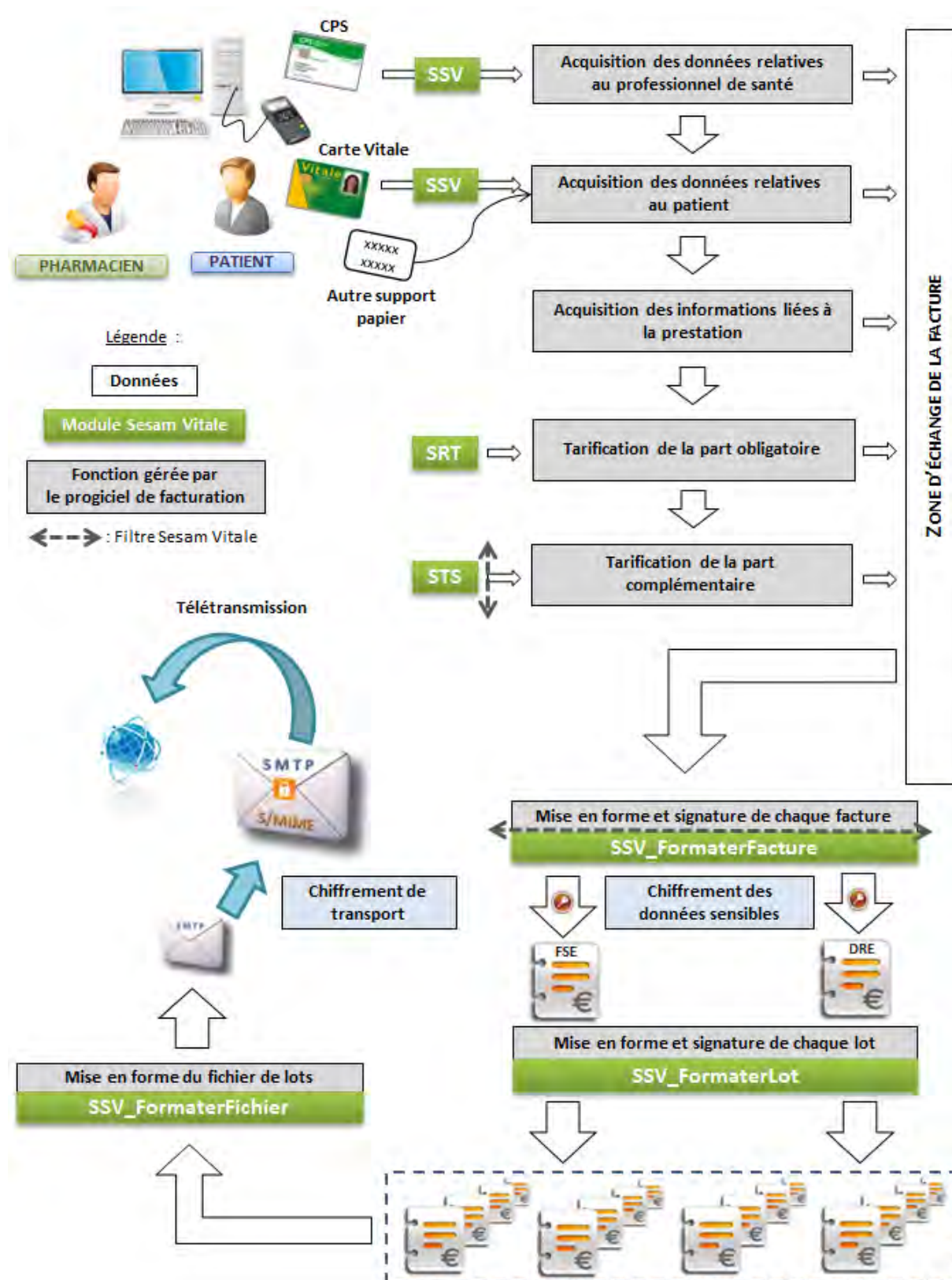


Figure 21 : Principales étapes de la préparation des factures électroniques (FSE/DRE) par le progiciel de facturation d'un logiciel de gestion d'officine (25).

B.1.3. LA NUMERISATION DES PIÈCES JUSTIFICATIVES

Conclu le 14 novembre 2011, l'avenant n°3 de la convention pharmaceutique a permis de franchir une étape décisive en généralisant la dématérialisation des ordonnances à toutes les pharmacies françaises. En allégeant les tâches administratives, ce système offre une opportunité d'accroître la disponibilité des pharmaciens tout en facilitant le traitement des dossiers par l'assurance maladie (86). Afin de faciliter les relations avec les professionnels de santé, simplifier leurs tâches administratives et gagner en efficience, le système de numérisation des pièces justificatives leur permet de dématérialiser certains documents en les numérisant. Comme nous l'avons vu dans la première partie, les pièces justificatives dématérialisées à l'officine peuvent être diverses mais elles sont majoritairement représentées par l'ordonnance originale numérisée à laquelle sont associées les données de facturation du ticket Vitale. Ce projet intitulé **SCOR** est généralisé à l'ensemble du territoire depuis la décision de la Caisse nationale d'assurance maladie du 15 janvier 2013¹⁷⁰ d'extension du projet initié en 2011. Dans l'attente de la généralisation de leur télétransmission, elles sont gravées des CD-ROM et transmises aux organismes d'AMO par voie postale selon un ramassage périodique organisé.

Les informations de la FSE en relation avec une pièce justificative sont récupérées par le progiciel au moyen du module SSV. Ainsi, à chaque pièce numérique au format PDF est lié le numéro de la FSE associée, son mode de sécurisation ainsi que les critères de regroupement en lots. Le progiciel précise la nature de la pièce justificative, sa date de création et lui associe un identifiant unique.



Figure 22 : L'association d'une FSE et d'une pièce justificative.

L'identifiant de chaque pièce justificative est un code reflétant :

- l'identifiant de facturation du professionnel de santé auteur de la pièce justificative ;
- l'identifiant de facturation du professionnel de santé émetteur de la pièce justificative ;
- la nature de la pièce justificative et la date de numérisation ;
- les codes régime, caisse gestionnaire et centre gestionnaire de l'organisme destinataire ;
- un « compteur » à neuf caractères numériques permettant d'identifier de façon unique l'identifiant de la pièce justificative sur le poste de travail du professionnel de santé.

¹⁷⁰ Décision du 15 janvier 2013 portant sur la généralisation et l'extension de la télétransmission des pièces justificatives de la facturation (SCOR).

B.1.3.1 CONSTITUTION D'UN DOSSIER DE PIECES JUSTIFICATIVES

Après l'exécution d'une prestation en lien avec la réalisation d'une FSE, le pharmacien numérise chaque pièce justificative papier, pour établir un fichier PDF par type (nature) de pièces justificatives. Chaque fichier PDF contient donc une seule pièce justificative à laquelle est associé un identifiant. Un dossier de justificatifs contient un seul et unique index, un ou plusieurs fichiers PDF de justificatifs ainsi qu'un ou plusieurs identifiants de pièces justificatives transmis dans un lot précédent.

Le fichier index à la norme SEH (système d'échanges harmonisés des organismes d'assurance maladie obligatoire)¹⁷¹ est généré par le progiciel du pharmacien en utilisant le module SSV et contient les informations suivantes :

- le numéro de facture ;
- les codes régime, caisse gestionnaire et centre gestionnaire ;
- le cas échéant, le code de renouvellement ;
- le total des montants facturés ;
- le total remboursable par l'organisme d'AMO et d'AMC ;
- le numéro d'immatriculation de l'assuré (NIR), sa date et son rang de naissance.



Figure 23 : Le dossier de pièces justificatives (PJ).

Dans cet exemple, l'identifiant de la PJ C est envoyé seul, la PJ C ayant déjà été transmise précédemment à l'organisme d'AMO.

B.1.3.2 MISE EN LOT DES DOSSIERS DE PIECES JUSTIFICATIVES

Suite à la mise en lot des FSE, le progiciel réalise la mise en lot des dossiers de justificatifs qui y sont liés. Parallèlement, le progiciel élabore un entête SEH (non chiffré) pour chaque lot récapitulant l'ensemble des documents inclus.

¹⁷¹ Le protocole d'échange SEH entre les professionnels de santé « prescrits » et les AMO [Contrat d'échange SEH SCOR] est disponible sur le site de l'assurance maladie (<http://www.ameli.fr>).

L'entête SEH est un fichier au format XML contenant plusieurs libellés renseignant sur (89):

- l'identification du lot de justificatifs :

- le champ « *exercice* » : identifiant de facturation du pharmacien ;
- le champ « *compostage* » permettant d'identifier de façon unique un lot, de la forme AAAAMMJJHHMMSSnnnnn (date et heure de création du lot + compteur de 5 caractères) ;

- l'horodatage du lot de justificatifs : Date et heure d'élaboration de l'index au format AAAA-MM-JJTHH:MMSS (où AAAA-MM-JJ représente la date, « T » a une fonction de séparateur et HH :MM : SS représente l'heure d'élaboration de l'index);

- le nombre de fichiers présents dans le lot ;

- l'index de lots de justificatifs ;

- le nombre de lots de justificatifs pour un lot de FSE.

Le nom physique du fichier d'entête SEH est alors constitué des champs « *exercice* » et « *compostage* » selon la structure : « *E-Exercice-ENTSCANORDO-Compostage.xml* ». Un **fichier** du lot de justificatif est élaboré par le progiciel à partir de l'entête SEH et des dossiers de justificatifs d'un seul et unique lot. Chaque fichier de lot est ensuite compressé dans une archive ZIP (le fichier « *Exercice-ENTSCANORDO-Compostage.zip* ») puis enregistré par le progiciel pour une réutilisation éventuelle. C'est ce fichier qui sera ultérieurement envoyée en pièce jointe d'un message SMTP à l'organisme d'AMO conformément aux modalités prévues par le cahier des charges.

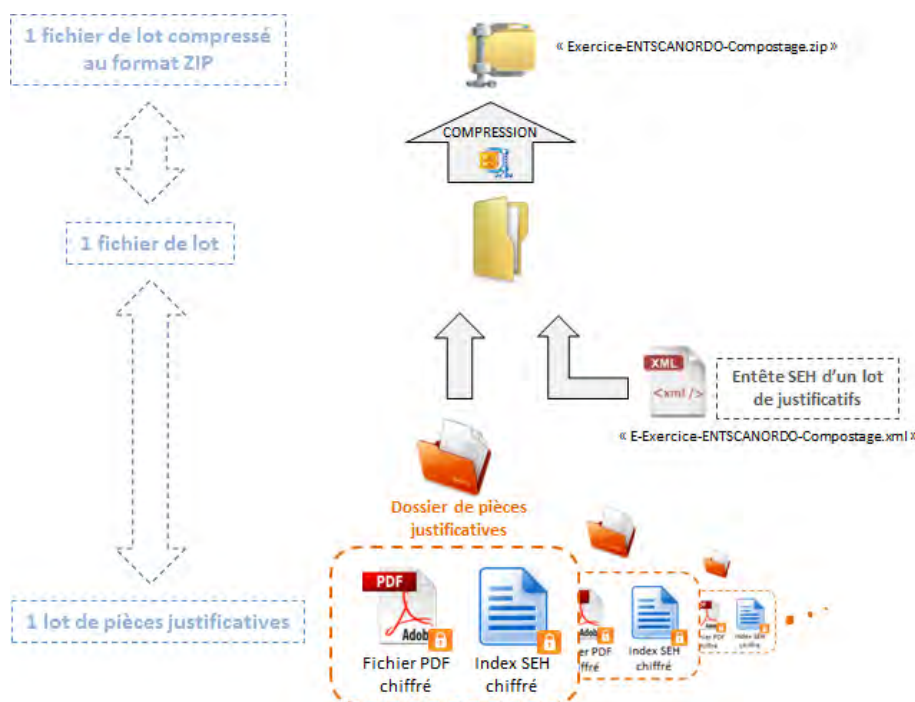


Figure 24 : Constitution d'un fichier de lot de pièces justificatives compressé.

B.1.4. LES FLUX DE TELETRANSMISSION

La télétransmission des factures électroniques constitue le moteur des relations régissant les rapports entre les pharmaciens et l'assurance maladie et permet de véhiculer 1,17 milliards de FSE et 11 millions de DRE par an. Le réseau SESAM-Vitale constitue ainsi le vecteur de transmission privilégié des échanges dématérialisés entre les professionnels de santé et l'assurance maladie. Rappelons que dans l'attente de la généralisation de leur télétransmission, les pièces justificatives numérisées sont quant à elles provisoirement gravées sur CD-ROM et transmises périodiquement à l'assurance maladie par voie postale¹⁷² (39).

B.1.4.1 LES FLUX DE FACTURATION ET DE PIECES JUSTIFICATIVES

La télétransmission des fichiers de lots de FSE, de DRE ou de pièces justificatives compressés aux différents organismes d'assurance maladie concernés est réalisée sous forme d'un message SMTP dont la sécurisation selon le protocole S/MIME par les certificats électroniques fournis par l'ASIP Santé permet de préserver la confidentialité de leur contenu.

B.1.4.1.a Constitution et sécurisation des flux

Un message SMTP est envoyé pour chaque fichier de lot de FSE, de DRE ou de pièces justificatives. Le contenu de ce message renseigne les différents champs présentés dans le tableau ci-dessous, auquel le fichier est associé en pièce jointe :

PROFIL DES MESSAGES SMTP DE TELETRANSMISSION			
CHAMP	FSE	DRE	PJ
Expéditeur « From »	Adresse e-mail du professionnel de santé émetteur		
Destinataire « To »	AMO : XYYYY@YYY.XX.rss.fr AMC : WWW@ZZZZ.fr XX : code grand régime YYY : code organisme destinataire W et Z : définis lors de la mise en forme des lots.		Régime général : 01.YY@01.scor.rss.fr Autre régime : XX@XX.scor.rss.fr YY : Code région caisse XX : Code régime
Sujet « Subject »	SVvvvvvv/exercice/compostage	DRvvvvvv/exercice/compostage	SOvvvvvv/exercice/compostage
	vvvvvv : version du cahier des charges « <i>exercice</i> » : identifiant de facturation du professionnel de santé « <i>compostage</i> » : permettant d'identifier de façon unique un lot, de la forme AAAAMMJHHMMSSnnnnn (date et heure de création du lot + compteur de 5 caractères)		
Type de contenu « Content-Type »	Type et le sous-type de l'objet transporté ; la valeur de ce champ est "Application/EDI-consent" quel que soit l'envoi		
Description du contenu « Content-Description »¹⁷³	Décrit le type de norme utilisé		
	« FSE/B2 »	« DRE/DR »	« SEH »

Tableau 19 : Profil des messages SMTP de télétransmission des FSE, des DRE et des pièces justificatives (PJ) numériques (25) (41).

¹⁷² 124 officines participaient à la télétransmission des pièces justificatives en 2012 (pour un million de flux SCOR) contre 5 pharmacies en 2011 (pour 1700 flux SCOR) (39).

¹⁷³ En cas de compression du fichier avant envoi, un sous-champ valorisé à « Z » est ajouté. Par exemple : FSE/B2/Z pour un fichier SMTP de FSE compressé.

Par ailleurs, tout professionnel de santé équipé d'un logiciel lecteur en version 3 bénéficie des fonctions de chiffrement assurant la confidentialité de données sensibles télétransmises¹⁷⁴. Le chiffrement de transport n'est cependant qu'optionnel pour l'obtention de l'agrément par les éditeurs de logiciels¹⁷⁵.

Lorsque les flux chiffrés transitent par un organisme concentrateur technique, ils sont déchiffrés par cet organisme qui effectue ses propres traitements et les re-chiffre avant de les transmettre aux organismes d'assurance maladie (87).

Le chiffrement du contenu de chaque message est réalisé à l'aide d'une clé de session utilisant l'algorithme 3DES (128 bits) en mode CBC. Cette clé de session est elle-même chiffrée avec la clé publique RSA 1024 bits du destinataire du message (certificat serveur de type S/MIME de l'organisme d'assurance maladie)¹⁷⁶. Cette clé publique associée à un certificat X.509 version 3 est certifiée par l'autorité de certification (l'ASIP Santé) qui atteste que la clé publique est bien liée à cet organisme d'assurance maladie¹⁷⁷. Après avoir vérifié la non-inclusion de ce certificat dans la liste de révocation des certificats (CRL), le logiciel procède au chiffrement et à la signature de chaque fichier¹⁷⁸.

B.1.4.1.b L'adressage des flux

Les processus d'élaboration des factures électroniques et des pièces justificatives étant distincts, leur envoi demeure désynchronisé. La télétransmission des pièces justificatives s'effectue donc séparément de la des FSE et DRE. Comme nous l'avons vu, tout pharmacien peut télétransmettre ses factures et pièces justificatives aux organismes d'assurance maladie via le réseau SESAM-Vitale ou en ayant recours à un organisme concentrateur technique. Ce dernier peut recevoir du pharmacien des flux :

- de FSE seules, de FSE enrichies (comprenant une part complémentaire) ;
- de DRE seules ou de DRE assorties de FSE ;
- comprenant un fichier unique, composé à la fois de lots de FSE et de DRE, l'organisme concentrateur technique procède alors à un éclatement des flux pour les adresser aux organismes d'AMO et d'AMC concernés ;

¹⁷⁴ Dans le cas où la transmission du lot de justificatifs est effectuée par CDROM, les fichiers PDF et les index sont non chiffrés.

¹⁷⁵ D'après le site du CNDA (<http://cnda-vitale.fr>).

¹⁷⁶ Il utilise, le cas échéant, la clé publique de l'OCT auquel il a recourt.

¹⁷⁷ Comme pour les professionnels de santé, les certificats des AMO sont disponibles via l'annuaire du GIP-CPS à l'adresse <http://annuaire.gip-cps.fr/>

¹⁷⁸ En revanche, les flux retours des organismes d'assurance maladie ne sont quant à eux pas chiffrés.

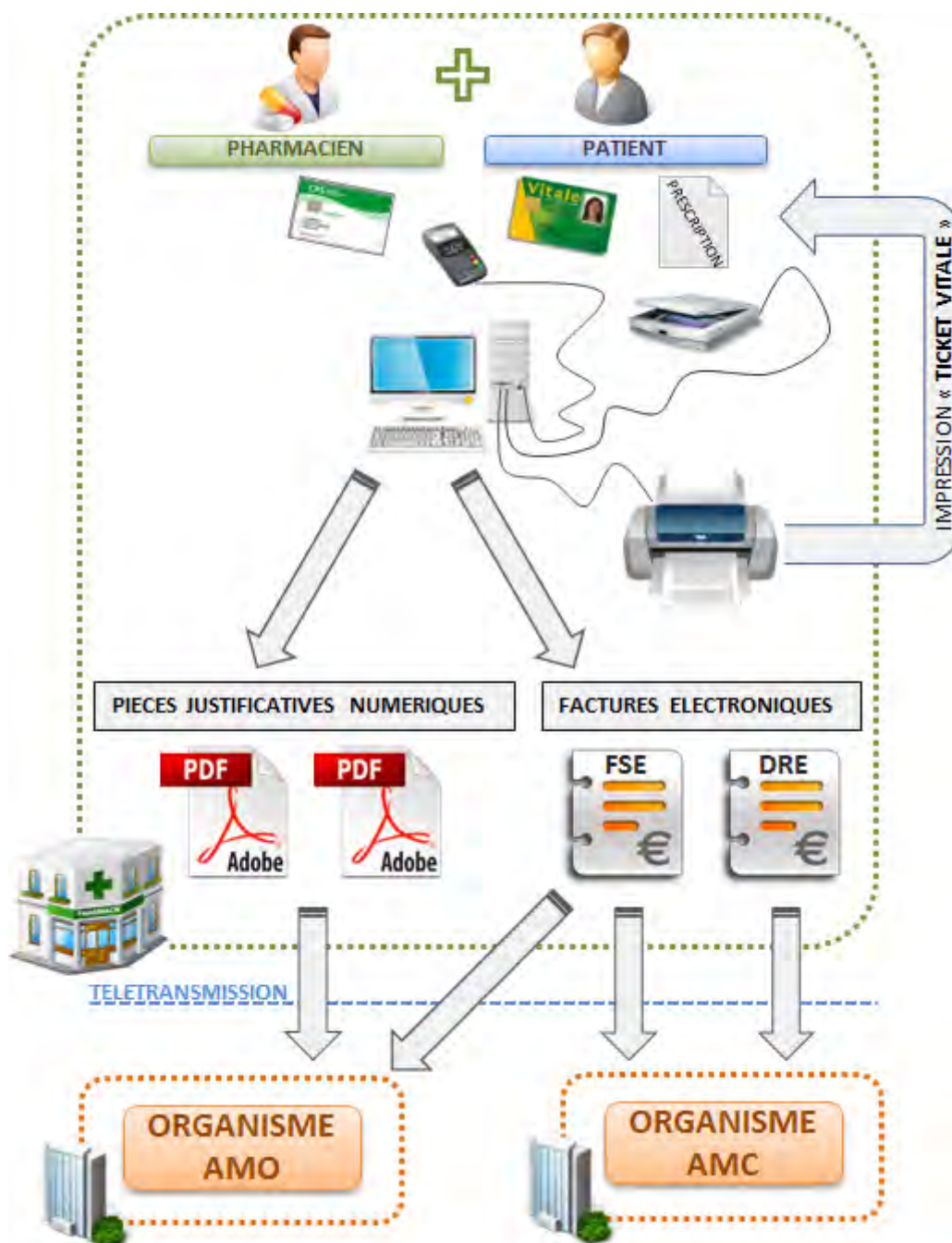


Figure 25 : La télétransmission des factures électroniques et des pièces justificatives numériques aux organismes d'assurance maladie.

La généralisation de ce système de télétransmission au cours des années 1990 a ainsi fourni le premier souffle de l'élan vers la dématérialisation des échanges au sein des systèmes d'information de santé et constitue la raison d'être de la carte Vitale. Ces échanges ne sont cependant pas unilatéraux et permettent un suivi complet du processus de remboursement des frais avancés par une pharmacie et notamment la résolution de litiges (rejets).

B.1.4.2 AUTRES FLUX DE TELETRANSMISSION

B.1.4.2.a Les flux d'administration du système SESAM-Vitale

- **Les données de suivi du parc** véhiculées par le biais des FSE, sont émises par le poste de travail du pharmacien à destination du GIE SESAM-Vitale et permettent d'avoir un état du parc des progiciels agréés, des lecteurs et des fournitures SESAM-Vitale.
- **Les flux de mise à jour du poste de travail du professionnel de santé** émis par le GIE SESAM-Vitale permettent notamment la mise à jour des tables utilisées pour la facturation.
- **Les flux de mise à jour des tables de conventions** sont émis par les signataires de conventions et contiennent les fichiers de conventions et de regroupement normés.
- **Les flux de mise à jour de la liste d'opposition incrémentale (LOI)** émis par le GIE SESAM-Vitale contiennent les incréments (dLOI) applicables sur la liste d'opposition incrémentale (LOI). Il s'agit des numéros de cartes Vitale en opposition dont la liste est mise à jour quotidiennement sur le poste de travail du pharmacien.
- **Les flux de mise à jour des cartes Vitales.**

B.1.4.2.b Les flux retour

Comme nous l'avons vu, le réseau SESAM-Vitale permet de véhiculer d'autres flux électroniques que ceux utilisés pour la facturation. On distingue ainsi des « flux retour » et des flux d'administration du système SESAM-Vitale assurant le suivi et la gestion du dispositif de télétransmission. Les flux émis par les organismes d'AMO et d'AMC à destination des pharmaciens transitent donc également par le réseau SESAM-Vitale.

On distingue :

- **Les accusés de réception logiques (ARL)**¹⁷⁹ indiquant au pharmacien que le lot de factures ou de pièces justificatives qu'il a émis a bien été reçu par l'organisme d'AMO ou d'AMC ;
- **Les rejet/signalement/paiement (RSP)** sont des flux à la norme NOEMIE (norme ouverte d'échanges entre la maladie et les intervenants extérieurs) indiquant le statut du traitement de la facture (paiement, rejet, ou signalement) ;
- **Les messages de service** sont des flux émis par les systèmes d'accueil des AMO, des AMC ou par l'opérateur de messagerie du réseau SESAM-Vitale signalant une irrégularité portant sur un message SMTP ou une indisponibilité du service.

¹⁷⁹ Le progiciel doit sauvegarder l'ARL positif associé, pendant 90 jours au moins (article R.161-47 du code de la sécurité sociale).

Chapitre 2 : L'AIDE A LA DISPENSATION ET AU SUIVI THERAPEUTIQUE DES PATIENTS

Les logiciels utilisés par les pharmaciens n'assuraient au départ qu'un rôle de mémoire comptable de la délivrance des produits pharmaceutiques et non de mémoire de leur dispensation. La dispensation désigne l'acte pharmaceutique dont les principes fondamentaux résident dans le devoir d'analyser et le pouvoir de décider. Toute dispensation ne se solde pas pour autant par une délivrance. En évaluant le contenu et le contexte de la requête d'un patient, l'analyse pharmaceutique d'un pharmacien peut conduire à une modification d'office ou concertée de la prescription initiale, voire à un refus de délivrance (3).

Les logiciels de gestion d'officine offrent aujourd'hui d'incroyables capacités d'analyses basées sur l'intégration de bases de données médicamenteuses dont le contenu est validé par la Haute Autorité de santé. Le pharmacien peut ainsi vérifier la composition exacte, les indications précises, les posologies et modalités d'administration, les précautions d'emploi, les contre-indications, les interactions, les effets indésirables, les propriétés pharmacocinétiques et pharmacodynamiques pour chaque médicament. Organisées en base de données structurées, ces informations peuvent être confrontées entre elles à la recherche d'interactions médicamenteuses, mais encore, avec les données relatives à un patient (âge, poids, taille, sexe, grossesse, allergies, contre-indications, historique de délivrance...).

Afin d'intégrer l'officine de manière interactive dans le parcours de santé de tout patient, les pharmaciens disposent d'un panel d'outils numériques destinés à améliorer le suivi des patients ainsi qu'à valoriser et sécuriser l'acte pharmaceutique : l'« opinion pharmaceutique » (OP) et le « dossier de suivi pharmaco-thérapeutique » (DSPT) mis en œuvre localement à l'officine et le dossier pharmaceutique accessible par le pharmacien via internet.

Afin d'assouvir les besoins d'échange et de partage d'informations des professionnels de santé, de nouveaux moyens de communication par messagerie électronique ont vu le jour. La multiplication de ces outils parfois peu sécurisés et largement employés par les professionnels de santé, conduisent à transmettre des données confidentielles « en clair ». C'est pourquoi l'ASIP Santé s'est investie dans le développement d'un système de messagerie sécurisé de santé (MSSanté) à l'échelle nationale leur permettant un échange sécurisé d'informations sensibles, de manière asynchrone mais potentiellement réalisé en direct.

Nous étudierons par ailleurs les conditions de mise en œuvre de la vente en ligne de médicaments par les officines françaises ainsi que les bonnes pratiques liées à ce nouveau mode de dispensation. Enfin, nous évaluerons les bénéfices potentiels de la dématérialisation dans l'accomplissement des nouvelles missions confiées au pharmacien d'officine par la loi HPST et la convention pharmaceutique.

B.2.1. LA DEMATERIALISATION DES REGISTRES COMPTABLES

L'une des particularités de la profession pharmaceutique consiste en l'obligation de tenue de registres comptables destinés à assurer la traçabilité des produits et substances délivrées. Le décret du 5 février 2007 relatif aux substances vénéneuses a permis de clarifier les modalités relatives à l'édition et à la conservation de ces registres au format électronique. Ainsi, les registres et enregistrements informatisés doivent être conservés pendant une durée de dix ans et tenus à la disposition des autorités de contrôle. Ils doivent pouvoir être édités sur papier, chaque page devant comporter le nom et l'adresse de l'officine, et être classés par patient, par médicament et par ordre chronologique¹⁸⁰. Le support informatique utilisé doit garantir la pérennité et l'intégrité des enregistrements qui doivent être dupliqués sur deux supports distincts.

B.2.1.1 L'ORDONNANCIER ELECTRONIQUE¹⁸¹

Toute délivrance d'un médicament, autre qu'une préparation, relevant de la réglementation des substances vénéneuses doit être transcrite sur un registre ou enregistrée informatiquement. Cet ordonnancier est unique pour les produits de santé appartenant aux listes I et II ainsi que pour les médicaments stupéfiants. Chaque enregistrement comporte un numéro d'ordre différent ainsi que :

- le nom et l'adresse du prescripteur ;
- le nom et l'adresse du malade ou du détenteur de l'animal ;
- le cas échéant la mention « usage professionnel » ;
- la date de délivrance ;
- la dénomination ou la formule du médicament ;
- les quantités délivrées ;
- le nom de l'établissement et le nom du prescripteur s'il s'agit d'un médicament à prescription hospitalière ;
- la spécialité du prescripteur s'il s'agit d'un médicament dont la prescription est réservée à certains médecins spécialistes.

S'il s'agit d'un médicament soumis à la réglementation des stupéfiants, il est également nécessaire d'indiquer : le nom et l'adresse du porteur de l'ordonnance lorsque celui-ci n'est pas le malade ainsi que les références de la pièce d'identité du porteur de l'ordonnance. Ces enregistrements doivent pouvoir être édités sur papier et être classés par patient, par médicament et par ordre chronologique. Toute personne habilitée à procéder à la dispensation de produits de santé à l'officine est habilitée à remplir ce registre.

B.2.1.2 LE REGISTRE SPECIAL DES STUPEFIANTS¹⁸²

Toute entrée et sortie de substances de la catégorie des stupéfiants est consignée dans un registre spécial, immédiatement après chaque opération. La balance des entrées et des sorties est ensuite portée au registre une fois par mois et l'inventaire du stock est effectué une fois par an. Ce registre est indispensable pour la comptabilité et la traçabilité des médicaments stupéfiants. Pour les entrées sont indiquées : la provenance, la désignation et la quantité de stupéfiants reçus tandis que toute sortie doit être assortie d'informations renseignant l'identité du patient ainsi que la désignation et les quantités délivrées de spécialités pharmaceutiques ou préparations répondant au régime des stupéfiants. Seul le pharmacien titulaire de l'officine est habilité à remplir ce registre qui doit être conservé au moins 10 ans.

¹⁸⁰ Article R.5132-9 du code de la santé publique.

¹⁸¹ Article R.5132-10 du code de la santé publique.

¹⁸² Article R.5132-36 du code de la santé publique.

B.2.2. LE DOSSIER DE SUIVI PHARMACO-THERAPEUTIQUE (DSPT)

Le pharmacien d'officine étant un acteur prépondérant dans la prévention des incidents ou accidents iatrogènes, la convention pharmaceutique réitère son devoir de suivi pharmaceutique des patients. En effet, certains médicaments présentent de forts risques d'effets indésirables et nécessitent par conséquent un suivi, voire une adaptation régulière de la posologie. Afin de tenir compte des spécificités de chacun, le DSPT permet de renseigner de nombreuses données utiles à la dispensation des produits de santé telles que l'âge, le poids, des facteurs de risque, des mesures tensionnelles, des antécédents, des résultats d'analyses...

Le tableau ci-dessous permet de mettre en évidence les principaux atouts liés à l'informatisation du dossier d'un patient :

CARACTERISTIQUES FONCTIONNELLES	TYPE DE DOSSIER	
	PAPIER	INFORMATISE
Mise à disposition et partage des données entre professionnels de santé		
Intégration des données	+	+++
Lisibilité du dossier	+	++
Complétude	+	+++
Accès	Séquentiel	Simultané
Disponibilité de l'information	Locale	Globale
Accès à distance	0	+++
Chainage des épisodes de soin	+	+++
Sécurité et protection		
Sécurité de l'information	+	+++
Confidentialité	++	+
Traitement automatique et aide à la décision		
Rappels et alarmes	0	+++
Suggestions diagnostiques et thérapeutiques	0	++
Traitement de données multimédia	0	++
Réutilisation des données		
Evaluation des pratiques professionnelles	+	+++
Recherche clinique et épidémiologique	+	+++
Formation et éducation		
Formalisation de la démarche de soin	+	+++
Adhésion du patient au protocole de soin	+	++
Lien avec des bases de connaissances	0	+++

Tableau 20 : Comparaison fonctionnelle entre le dossier relatif à un patient sous forme papier et dématérialisée (90).

B.2.2.1 PRINCIPALES FONCTIONS DU DSPT

Le dossier d'un patient est, selon F. Roger France, « *la mémoire écrite de toutes les informations concernant un malade, constamment mises à jour et dont l'utilisation est à la fois individuelle et collective* » (91). Il est le reflet de l'évolution de l'état de santé d'un patient et/ou de ses traitements. L'informatisation de ce dossier doit contribuer à faciliter le partage de données entre professionnels de santé, à diminuer les temps d'accès et d'acheminement des données de santé, à répondre aux besoins de sécurité et de traçabilité et éviter les erreurs de prescription ou de dispensation (3).

Afin d'améliorer la qualité et la sécurité de la dispensation des produits de santé (particulièrement le médicament), mieux informer et conseiller les patients, le DSPT permet d'enregistrer certaines données conformément à la déclaration simplifiée n° 52 de traitement automatisé de données personnelles. Le DSPT s'inscrit également dans une démarche de continuité des soins en assurant un suivi des actes de dispensation successifs (sur prescription ou non) au sein d'une même officine et au profit d'un même patient tout en prenant en compte les « opinions pharmaceutiques » précédemment élaborées.

Constitué avec l'accord du patient, le DSPT est la collection des données issues des opinions pharmaceutiques, rapportées à un patient et avec son accord. Elles constituent l'ensemble des informations de source pharmaceutique, médicale (informations communiquées par le médecin ayant trait à une dispensation ou à un profil), biologique (résultats pertinents d'analyse) et administrative (identification), utiles à la dispensation. Correctement utilisé, le DSPT promet de nombreux bénéfices en optimisant la sécurité, la qualité, l'efficacité, le confort et l'économie du soin de chaque stratégie thérapeutique. Les collections successives de données utiles permettent ainsi au pharmacien de bénéficier d'un niveau d'information de plus en plus élevé avec le temps pour affiner ses analyses et ses décisions (3).

Il est ainsi possible de schématiser la structure du DSPT en quatre volets principaux (92) :

- **le profil administratif du patient** renseignant l'ensemble des données d'identification, les coordonnées ainsi que les informations sur les régimes et les contrats d'AMO et éventuellement d'AMC ;
- **le profil physiologique du patient** (taille, poids, IMC...) ;
- **le profil pathologique du patient** (type de pathologie, allergies...) ;
- **l'historique des prescriptions** permettant de mettre en évidence une incompatibilité avec une dispensation antérieure.

Les sources d'information permettant d'alimenter ces différents volets peuvent être variées et donc multiples. Il peut s'agir d'informations communiquées oralement par le patient ou son médecin ou encore acquises à partir de supports d'identification (carte Vitale, carte de mutuelle, attestation de droits, documents numérisés...). Couplé à une base de données médicamenteuse, le DSPT constitue un outil puissant permettant de considérer l'ensemble des données utiles à l'accomplissement d'une dispensation et du suivi local¹⁸³ d'un patient en toute sécurité.

¹⁸³ Par opposition au dossier pharmaceutique qui permet un suivi des délivrances effectuées sur l'ensemble du territoire.

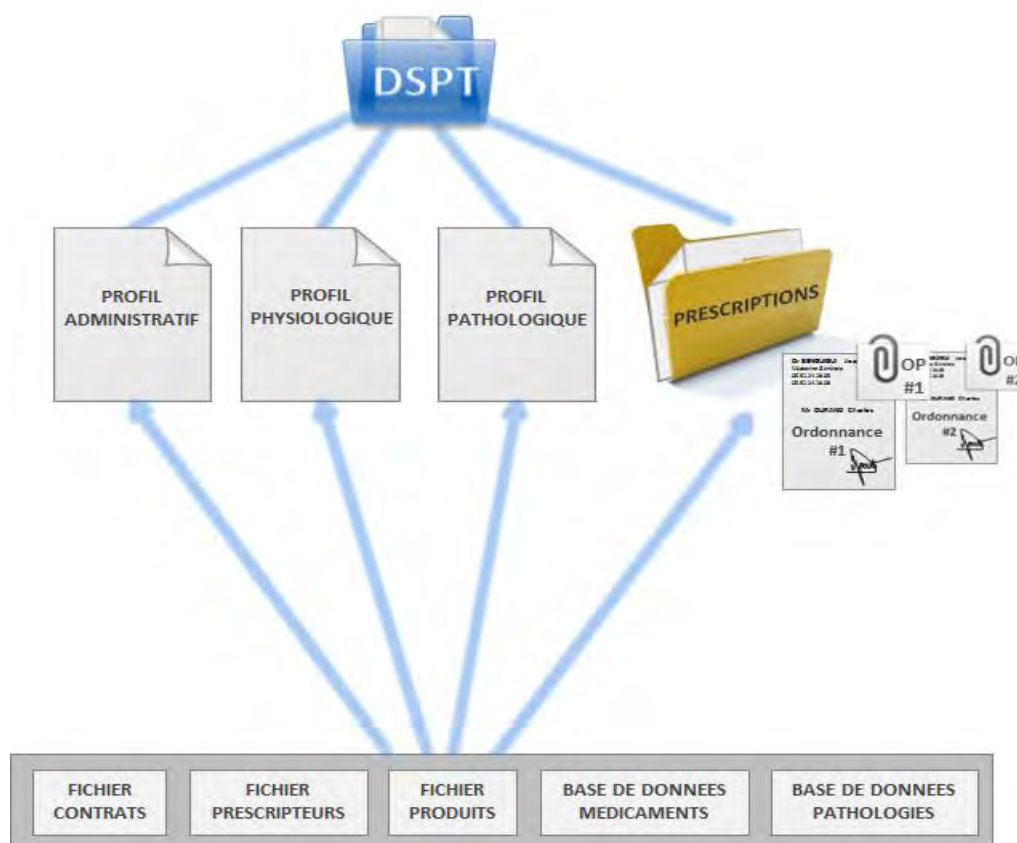


Figure 26 : Interactions des principaux volets du DSPT avec les fichiers et les bases de données du logiciel de gestion d'officine.

Afin d'associer le bon dossier au bon patient et garantir une interopérabilité des systèmes, le logiciel de gestion d'officine calcule l'INS-C selon des traits du patient lus à partir de la carte Vitale et permet « d'appeler » le dossier du patient. Cet appel du dossier peut être réalisé en dehors du cadre d'utilisation de la carte Vitale en effectuant une recherche au moyen des différents traits du patient enregistrés dans son DSPT.

B.2.2.1.a Gestion du dossier du patient

Le DSPT met à disposition du pharmacien l'ensemble des informations du patient utiles à la dispensation et éventuellement, à la facturation des produits de santé. Les données administratives garantissent à la fois une identification du patient nécessaire à la dispensation mais apporte aussi l'ensemble des informations nécessaires à l'élaboration d'une facture électronique. Les données physiologiques et pathologiques garantissent quant à elles une adéquation du traitement au profil du patient ainsi qu'un suivi de leur évolution dans le temps.

Les données administratives relatives au patient sont généralement acquises au moyen de supports d'identification (tels qu'une carte Vitale, une carte de mutuelle ou une attestation de droits), il s'agit (9) :

- de son identité : nom, prénom, date de naissance, sexe ;
- de ses coordonnées : adresse postale et numéro de téléphone ;

- du numéro de sécurité sociale (NIR) et des taux de prise en charge (régime d'exonération, durée de validité des droits) ainsi que la période d'ouverture des droits ;

- des informations relatives à un contrat d'AMC éventuel (numéro d'adhérent, taux de prise en charge) ;

- des informations sur la profession ou les habitudes de vie du patient dans la mesure où elles sont utiles à la dispensation ;

- des informations relatives au prescripteur : nom, adresse, numéro d'identification, spécialité, situation conventionnelle. Ces données peuvent être saisies dans la fiche informatisée relative au prescripteur par retranscription des informations au moyen du clavier mais le numéro d'identification peut parfois être acquis à partir d'un code barre unidimensionnel imprimé sur l'ordonnance. Ce système très apprécié des pharmaciens permet à la fois un gain de temps tout en limitant les risques d'erreurs de saisie (source de rejets des factures par les organismes d'assurance maladie).

Les données du profil physiologique du patient sont le plus souvent obtenues à partir d'informations communiquées oralement par le patient ou son médecin, ou encore mentionnées sur une ordonnance. Il s'agit d'information sur l'état de santé physiologique du patient comme des informations anthropomorphiques (âge, taille, poids, IMC), des constantes biologiques ou encore des informations sur le statut vaccinal du patient. En effet, tout patient acceptant de communiquer ses résultats d'analyses biologiques à son pharmacien pourra bénéficier d'un suivi de l'évolution de ces constantes en fonction du temps.

Les données du profil pathologique du patient sont généralement renseignées suite à une communication du prescripteur, de mentions portées sur l'ordonnance, de compte-rendu d'examens ou encore par le patient lui-même. Dans ce dernier cas, le pharmacien devra toutefois être vigilant à l'exactitude des informations confiées par le patient et les faire confirmer par le prescripteur si besoin. Dans ce domaine, la classification internationale des maladies (CIM)¹⁸⁴ permet de codifier l'ensemble des pathologies, affections, allergies... dont sont susceptibles de souffrir les patients.

Si les données administratives du patient ne varient que rarement et ont peu d'impact sur la qualité de la dispensation, il reste parfois difficile pour les pharmaciens de collecter les informations nécessaires à l'établissement de leurs profils physiologique et pathologique. De plus, pour être pertinentes, ces données doivent être régulièrement mises à jour mais le phénomène de « nomadisme pharmaceutique » conduisant de nombreux patients à changer régulièrement d'officine ne permet pas toujours la tenue du DSPT de manière efficace. Comme nous le verrons, la mise en œuvre du dossier pharmaceutique permet de réaliser un suivi pharmaco-thérapeutique quelle que soit l'officine choisie par le patient.

B.2.2.1.b Gestion des délivrances

Le DSPT permet d'assister le pharmacien dans les différentes étapes majeures d'analyse d'une prescription ou d'une demande spontanée d'un produit de santé. Une liste exhaustive des dispensations antérieures (qu'il s'agisse de produits de santé prescrits ou non) permet ainsi de retracer chaque vente et éventuellement de remonter jusqu'au vendeur, au numéro de lot du produit ou à une prescription particulière.

¹⁸⁴ Classification statistique internationale des maladies et des problèmes de santé élaborée par l'Organisation mondiale de la santé.

En effet, chaque fichier de prescription archivé renseigne, outre la date de prescription :

- des informations relatives au prescripteur : nom, prénom, spécialité, numéro d'identification, coordonnées (adresse, téléphone, fax, e-mail) ;
- des informations relatives aux médicaments, produits de santé ou dispositifs médicaux dispensés : dosage, posologie, date de l'ordonnance et durée de la prescription ;
- l'historique des médicaments dispensés, les traitements en cours et les médecins traitants (9).

Comme nous l'avons vu, les bases de données médicamenteuses contenues dans les logiciels de gestion d'officine mettent l'ensemble des monographies des produits de santé recensés, à disposition des pharmaciens. Elles permettent ainsi de disposer rapidement d'informations pertinentes permettant d'affiner la dispensation (52):

- dans le cadre systématique d'une recherche d'interactions de produits de santé entre eux, prescrits ou non, dispensés de façon concomitante ou non, sur une même ordonnance ou à l'occasion d'une dispensation simultanée de produits prescrits et non prescrits, ou vis-à-vis de l'historique de délivrance ;
- dans le cadre d'une recherche d'interactions ciblées entre l'utilisation d'un produit de santé et le profil thérapeutique d'un patient (par exemple, le traitement d'une maladie chronique) ;
- dans le cadre d'une recherche d'une incompatibilité avec le profil physiologique ou pathologique du patient.

Lors de toute détection d'incompatibilités relatives à une dispensation, le pharmacien a la possibilité d'émettre une « opinion pharmaceutique » liée à chaque dispensation. La dématérialisation du formulaire papier d'opinion pharmaceutique par le logiciel de gestion d'officine permet au DSPT de réaliser la collection des données issues des dispensations précédentes, rapportées à un patient et avec son accord. Elles constituent l'ensemble des informations de source pharmaceutique, médicale (communiquées par le prescripteur), biologique et administrative (identification), utiles à la dispensation.

B.2.2.2 L'OPINION PHARMACEUTIQUE

Au travers du nombre et de la précision des informations recueillies auprès des prescripteurs et du patient, les opinions pharmaceutiques, véritables vecteurs de constitution et de communication du DSPT, permettent au pharmacien de disposer d'un niveau d'information de plus en plus élevé en fonction du temps, lui permettant d'affiner ses analyses et ses décisions.

B.2.2.2.a Définition et objectifs

L'opinion pharmaceutique est un avis motivé dressé sous l'autorité d'un pharmacien, portant sur la pertinence pharmaceutique d'un ou d'un ensemble de traitements le concernant. Consigné dans l'officine, il est communiqué par un document normalisé au prescripteur et/ou au patient lorsqu'il invite à la révision, ou lorsqu'il justifie le refus ou la modification d'office de sa prescription (52).

L'acte de dispensation de produits de santé ne consiste pas en une simple délivrance, il fait intervenir les connaissances du pharmacien pour l'analyse pharmaceutique de la prescription. Il engage ainsi sa responsabilité (pénale, civile, disciplinaire) lorsqu'un préjudice lié à son activité est subi par un patient. Qu'ils soient prescrits ou non, la dispensation de produits de santé par un pharmacien d'officine peut se solder par :

- **la délivrance** : lorsque l'analyse pharmaceutique des données du patient (analyse d'une prescription, données médicales après interrogatoire) satisfait aux conditions de dispensation du produit en question ;
- **la délivrance après levée d'un doute** thérapeutique ou réglementaire : ce doute est généralement levé par communication téléphonique avec le médecin prescripteur ;
- **la délivrance en situation d'urgence** avec modification de la prescription ;
- **la délivrance après modification du traitement** après accord du prescripteur ou du patient sans ordonnance ;
- **le refus de délivrance** total ou partiel des produits de santé.

Ces décisions qui découlent de l'analyse pharmaceutique ne laissent en général aucune trace de l'intervention du pharmacien où seule la délivrance est formalisée de manière comptable au travers de la facturation et par l'inscription dans les différents registres.

Véritable instrument de coopération interdisciplinaire, l'opinion pharmaceutique clarifie l'engagement de la responsabilité des professionnels de santé tout en valorisant leur intervention. Elle rend l'acte pharmaceutique intelligible et lui assure :

- **lisibilité** : préciser la réflexion, évaluer les actes, alerter sur des cas particuliers...
- **mémoire** : assurer le témoignage de l'acte et le suivi du patient ;
- **traçabilité** : retrouver l'auteur d'une dispensation, d'une prescription...
- **opposabilité** : justifier d'un acte face au patient, face au médecin ou aux juridictions...

B.2.2.2.b Mise en œuvre de l'opinion pharmaceutique

Si l'élaboration d'une opinion pharmaceutique était initialement rédigée sur papier, l'évolution des logiciels métiers a permis d'intégrer cette fonction en la rendant facilement accessible et rapidement éditable de manière informatique.

Les pharmaciens ainsi que le personnel régulièrement habilité à effectuer une dispensation sous leur contrôle effectif, peuvent donc formellement rendre compte d'un acte qui ressort de leur compétence grâce à un document normalisé qui décrit les informations qu'ils doivent recenser. Le recueil de ces informations doit être réalisé avec une méthodologie rigoureuse et doivent être retranscrites fidèlement.

Ce document normalisé comprend 10 champs :

1/ La date d'intervention ;

2/ L'identification formelle des acteurs : patient, auteur de la dispensation, prescripteur (s'il y a lieu), produits de santé mis en cause. L'identification électronique du patient par sa carte Vitale et du pharmacien par sa carte CPS permet d'établir, *a priori*, l'identité des acteurs sans ambiguïté ;

3/ Les éléments connus du profil physiopathologique du patient : pathologies traitées, état de grossesse, hypersensibilité, antécédents médicaux... qui permettent de dévoiler certaines contre-indications ou l'incohérence d'une prescription ;

4/ La nature du problème : Dans son cahier des charges, le conseil central A de l'ordre des pharmaciens propose une liste des situations les plus courantes auxquelles les pharmaciens peuvent être confrontés. Le problème doit être clairement identifié et explicité en termes intelligibles ;

5/ Eventuellement, l'intention thérapeutique du prescripteur : prescription hors-AMM, posologie particulière...

6/ L'argumentaire du pharmacien et ses propositions éventuelles : fondé sur la synthèse des données recueillies précédemment, il lui permet de justifier sa décision et proposer éventuellement une alternative au prescripteur ;

7/ La décision prise par le dispensateur : de dispenser ou non la totalité des produits de santé ;

8/ La mention de la transmission éventuelle de l'information : au patient, au prescripteur, à un centre de pharmacovigilance ou aux autorités légalement autorisées ;

9/ La validation obligatoire par un pharmacien : la signature (manuscrite ou électronique) du pharmacien responsable de la dispensation (ou à défaut du titulaire de l'officine) est obligatoire ;

10/ Le numéro de facture correspondant aux produits délivrés.

Une fois validée, l'opinion pharmaceutique est enregistrée dans le système informatique de l'officine et peut alors être consultée par le personnel régulièrement habilité.

B.2.2.2.c Communication de l'opinion pharmaceutique

Consignée dans l'officine, l'opinion pharmaceutique est couverte par le secret médical et peut être communiquée au praticien prescripteur et/ou au patient lorsque le pharmacien l'invite à modifier ou réviser son traitement. Seule sa communication formelle est une condition de son opposabilité légale.

Communication de l'opinion pharmaceutique au prescripteur : Dès lors que le pharmacien l'estime utile ou si le règlement l'impose. L'article R.4225-61 du code de la santé publique prévoit que lors d'un refus de dispensation dans l'intérêt de la santé du patient, le pharmacien doit en informer le prescripteur et en porter mention sur l'ordonnance.

En pratique, la communication formelle de l'opinion pharmaceutique vient donc en complément de l'alerte téléphonique au médecin.

Communication de l'opinion pharmaceutique au patient : Chaque patient a un droit d'accès permanent aux informations personnelles le concernant. Cependant, lors d'une délivrance non conforme (refus ou modification), sa communication doit rester limitée aux devoirs d'assistance et de conseil. Le contenu intégral de l'opinion pharmaceutique dépasse le cadre de cette information, et le pharmacien doit alors ainsi veiller à lui communiquer les informations les plus pertinentes et intelligibles tout en veillant à ne pas altérer la confiance qu'il porte en son médecin.

Tout pharmacien ne doit pas perdre de vue que l'objectif est de délivrer une information adaptée au contexte de chaque patient et non de l'effrayer inutilement sur la dangerosité des produits de santé. Il est donc primordial de savoir sélectionner les informations utiles à un patient pour un contexte donné et de s'assurer de la bonne compréhension des informations. Tout pharmacien doit donc délivrer une information claire et concise en choisissant un vocabulaire en adéquation avec le niveau de compréhension de son patient afin de délivrer un conseil personnalisé et adapté à chaque contexte.

En se proposant comme support de substitution dédié au stockage des connaissances du pharmacien, l'outil informatique ne doit bien évidemment pas remplacer son savoir-faire et ses connaissances, ni aliéner la liberté de son jugement. Il s'agit d'un outil destiné à faciliter le travail du pharmacien dans l'exercice de sa profession dont les bénéfices attendus par les patients, les pharmaciens ainsi que les organismes d'assurance maladie doivent être garants d'une amélioration de la sécurité, de la qualité et de l'efficacité de la dispensation des produits de santé tout en simplifiant les démarches administratives liées à leur facturation.

Comme nous le verrons, la généralisation de l'utilisation d'une messagerie sécurisée de santé par les pharmaciens et les prescripteurs et la mise en œuvre d'un système d'e-prescription permettraient de faciliter la mise en œuvre de l'opinion pharmaceutique en facilitant leurs correspondances et leur coopération.

B.2.3. LE DOSSIER PHARMACEUTIQUE

C'est avec la volonté de « *favoriser la coordination, la qualité, la continuité des soins et la sécurité de la dispensation* » que la loi n°2007-127 du 30 janvier 2007 introduit la possibilité pour les pharmaciens d'officine de créer un dossier pharmaceutique « *pour chaque bénéficiaire de l'assurance maladie, avec son consentement* ». Cette loi lui confère ainsi une assise légale et confie au Conseil national de l'ordre des pharmaciens, la responsabilité de sa mise en œuvre. Le décret 2008-1326 du 15 décembre 2008 a ensuite permis de définir les modalités de mise en œuvre de ce dossier, après avis de la CNIL et de l'ordre des pharmaciens, en modifiant la partie réglementaire du code de la santé publique créant ainsi la section « dossier pharmaceutique » comprenant aujourd'hui les articles R.1111-20-1 à R.1111-20-11. Cette réglementation fut de nouveau modifiée par le décret du 5 octobre 2012¹⁸⁵ qui étend désormais les missions du dossier pharmaceutique aux pharmaciens exerçant dans les pharmacies à usage intérieur.

Les textes de la loi de 2007 portant sur la création du dossier pharmaceutique furent transférés par la loi n° 2009-879 du 21 juillet 2009 portant réforme de l'hôpital et relative aux patients, à

¹⁸⁵ Décret n° 2012-1131 du 5 octobre 2012 relatif à la consultation et à l'alimentation du dossier pharmaceutique par les pharmaciens exerçant dans les pharmacies à usage intérieur.

la santé et aux territoires puis finalement modifiés en 2012 ce qui explique que le décret d'application de 2008 paraît antérieur à la loi portant sur la création du dossier pharmaceutique.

L'article L.1111-23 du code de la santé publique précise que *« sauf opposition du patient quant à l'accès du pharmacien à son dossier pharmaceutique et à l'alimentation de celui-ci, tout pharmacien d'officine est tenu d'alimenter le dossier pharmaceutique à l'occasion de la dispensation. Les informations de ce dossier utiles à la coordination des soins sont reportées dans le dossier médical personnel »*. Dans l'attente d'une intégration du dossier pharmaceutique au dossier médical personnel, cet article offre la possibilité aux médecins de certains établissements de santé de consulter le dossier pharmaceutique de leurs patients depuis 2011 : *« à titre expérimental et pour une durée de trois ans (...) et dans le cadre de la prise en charge des patients »*¹⁸⁶.

L'une des particularités du dossier pharmaceutique par rapport aux autres projets du domaine de l'e-santé, est que la profession elle-même s'est largement investie dans sa conception, son déploiement, sa réglementation et sa mise en œuvre. Initié sous la présidence de Jean Parrot¹⁸⁷ et passionnément défendu par l'actuelle présidente du Conseil national de l'ordre des pharmaciens, Madame Isabelle Adenot, ce projet fut tout d'abord coordonné par un comité de pilotage en collaboration avec la Direction des technologies de santé de l'ordre, permettant à 80% des pharmacies d'officine de proposer le dossier pharmaceutique à leur patient en 2011.

B.2.3.1 PRESENTATION ET OBJECTIFS

Géré par voie électronique¹⁸⁸, le dossier pharmaceutique recense les informations relatives aux médicaments (code CIP, quantité et date de dispensation) dispensés à un patient **avec ou sans prescription médicale au cours 4 derniers mois**¹⁸⁹. Si l'article L.1111-23 du code de la santé publique prévoit que le dossier pharmaceutique recense l'ensemble des produits et objets définis à l'article L.4211-1 du code de la santé publique, il ne contient en pratique actuellement que les médicaments, le tri se faisant automatiquement par le système informatique officinal.

Ce projet d'envergure ayant bénéficié d'un soutien sans faille de la profession a toutefois nécessité un investissement humain et financier à la hauteur des ambitions du Conseil national de l'ordre des pharmaciens. Cet outil accessible via internet dans toute officine raccordée au dispositif, doit permettre de renforcer la lutte contre l'iatrogénie médicamenteuse et garantir un relais des alertes sanitaires. Les quatre grands objectifs visés par le dossier pharmaceutique consistent ainsi à (93) :

- **Sécuriser la dispensation** en limitant les risques de survenue **d'évènements iatrogènes**, conséquences d'une mauvaise prescription, du non-respect de contre-indications, d'une interaction, d'une posologie excessive ou d'un traitement trop long¹⁹⁰. L'objectif principal de cet outil voulu performant est de limiter la survenue de ces évènements grâce à un meilleur suivi du patient et une meilleure coopération entre professionnels de santé. En proposant au

¹⁸⁶ Loi n° 2011-2012 du 29 décembre 2011 relative au renforcement de la sécurité sanitaire du médicament et des produits de santé, article 23.

¹⁸⁷ Président du Conseil national de l'ordre des pharmaciens de 1993 à 2009.

¹⁸⁸ Article R.1111-20-1 du code de la santé publique

¹⁸⁹ Articles R.1111-20-2 et R.1111-20-11 du code de la santé publique.

¹⁹⁰ Le nombre annuel d'hospitalisations en lien avec un évènement indésirable médicamenteux est estimé à 140 000 pour 13 000 décès (94).

pharmacien de visualiser un large aperçu des dispensations effectuées au patient, le dossier pharmaceutique permet ainsi de limiter les redondances de traitements (94).

- **Améliorer la gestion des retraits de lots et des alertes sanitaires** diffusées dans les plus brefs délais à toutes les officines via le réseau informatique du dossier pharmaceutique. Il permet au pharmacien de recevoir quotidiennement les alertes sanitaires ainsi que les rappels et retraits de lots de médicaments, s'affichant directement à l'écran, et de prendre les mesures adaptées à la situation. Le pharmacien responsable du laboratoire concerné communique l'information validée par l'Agence nationale de sécurité du médicament, à l'hébergeur du dossier pharmaceutique, permettant d'alerter toutes les officines raccordées, 24 heures sur 24 et 7 jours sur 7 (94).

- **Orienter l'acte pharmaceutique vers le patient** et non plus vers le médicament grâce à une large vision des traitements dispensés au patient par les différentes officines qu'il fréquente. Ceci permet d'optimiser son traitement et de mettre en évidence une éventuelle surconsommation de médicaments. Si le « nomadisme pharmaceutique » entraîne parfois une redondance de dispensations et donc une surconsommation de médicaments, celle-ci peut néanmoins résulter d'une aggravation de l'état de santé du patient, d'un traitement insuffisant, d'une mauvaise observance, d'un mauvais usage des médicaments, ou encore d'interactions médicamenteuses devant alerter le pharmacien sur la nécessité de réévaluer la stratégie thérapeutique avec le prescripteur.

- **Renforcer la place du pharmacien dans le système de soins** en considérant les données relatives aux médicaments dispensés sans ordonnance dont l'utilisation n'est pas dénuée de risques. Le monopole des pharmaciens pour la dispensation de tels produits étant actuellement menacé, le dossier pharmaceutique permet de réaffirmer l'importance d'une analyse pharmaceutique dans sa globalité, exclusivement disponible en pharmacie, confirmant l'apport indispensable des compétences scientifiques des pharmaciens.

Il s'agit donc d'un véritable outil professionnel qui vise à sécuriser la dispensation des médicaments et améliorer le suivi thérapeutique des patients. Il valorise l'acte pharmaceutique et entretient la relation de confiance entre le patient et son pharmacien. Voué à être prochainement intégré au DMP, le dossier pharmaceutique permettra alors de faciliter la coopération entre les pharmaciens et les prescripteurs autour du traitement d'un patient.

B.2.3.2 LES ETAPES CLES DE LA VIE D'UN DOSSIER PHARMACEUTIQUE

Conformément à la loi informatique et libertés, chaque pharmacien est tenu de déclarer la mise en œuvre d'un traitement de données personnelles auprès de la CNIL et doit en informer les patients au moyen d'une affiche prévue à cet effet. Cependant, comme nous l'avons vu, la déclaration simplifiée n°52 ne couvre pas les opérations de traitement des données relatives au dossier pharmaceutique. Un mandat de télé-déclaration spécial (annexe 8) doit donc être faxé à la société Celtipharm, mandatée par l'ordre, afin de déclarer l'officine comme proposant ce service.

Il est nécessaire qu'avant toute création d'un nouveau dossier pharmaceutique, le pharmacien s'entretienne avec le patient afin de lui en expliquer de manière claire et explicite le principe, les finalités, les modalités de mise en œuvre ainsi que ses droits. Pour cela il lui remet une brochure d'informations disponible sur le site internet de l'ordre des pharmaciens¹⁹¹ et dans le kit de démarrage du dossier pharmaceutique obtenu auprès de l'ordre. Ce kit contient

¹⁹¹ <http://www.ordre.pharmacien.fr/>

également une affiche de la CNIL destinée à l'information des patients concernant les modalités d'utilisation du dossier pharmaceutique ainsi qu'une charte et un exemplaire du mandat de télé-déclaration.

Chaque intervention sur le dossier pharmaceutique (création, consultation, alimentation, rectification, édition d'une copie ou clôture) à la demande du bénéficiaire ou de son représentant légal, est datée et comporte l'identification du pharmacien ayant effectué cette intervention¹⁹². Cependant ils n'ont accès qu'aux traces des seules interventions effectuées dans leur officine¹⁹³.

B.2.3.2.a La création d'un dossier pharmaceutique

La création et la gestion d'un dossier pharmaceutique ne peut se faire que sous « *le contrôle et la responsabilité des pharmaciens d'officine ou exerçant dans une pharmacie à usage intérieur* » ainsi que « *les professionnels de santé habilités par la loi à les seconder dans la dispensation des médicaments* »¹⁹⁴ (préparateurs en pharmacie, étudiants en pharmacie à partir de la troisième année d'études).

Géré par voie électronique, le dossier pharmaceutique peut être créé dans toute officine directement via le logiciel de gestion d'officine du pharmacien, en présence et avec le consentement¹⁹⁵ exprès, libre et éclairé du patient muni de sa carte Vitale et d'une pièce d'identité. Sauf situations particulières telles que les mineurs de moins de seize ans ou les personnes sous tutelle, seul le patient muni de sa carte Vitale est autorisé à créer et utiliser ce dossier. Lorsque le bénéficiaire devient majeur, le dossier pharmaceutique subsiste dès lors que le pharmacien a recueilli son consentement.

Lors de la création du dossier pharmaceutique d'un patient, une attestation de création papier mentionnant son autorisation expresse et ses droits de rectification et de clôture du dossier lui est remise par le pharmacien¹⁹⁶ (annexe 9). La remise de ce document au patient atteste de son information et de son consentement quant à la création du dossier pharmaceutique par le pharmacien et son hébergement par la société Santeos, hébergeur tiers sélectionné par l'ordre des pharmaciens et agréé par le ministre en charge de la santé.

La création, comme l'alimentation et la consultation du dossier pharmaceutique par le pharmacien est réalisée par l'utilisation conjointe de sa carte CPS et de la carte Vitale du bénéficiaire. Il crée le dossier pharmaceutique d'un patient directement via le module proposé par son logiciel de gestion d'officine et renseigne en premier lieu des informations d'identification (nom, prénom, date de naissance, sexe et rang de naissance du patient)¹⁹⁷.

B.2.3.2.b L'alimentation du dossier pharmaceutique

Lors de toute dispensation de médicament, avec ou sans prescription, les pharmaciens peuvent proposer à leur patient d'alimenter leur dossier pharmaceutique. Au cours de la dispensation, le logiciel de gestion d'officine propose d'alimenter le dossier pharmaceutique en renseignant la date de dispensation, l'identification (code CIP) et la quantité de produits dispensés au bénéficiaire avec ou sans prescription médicale¹⁹⁸. Ne sont accessibles par le

¹⁹² Article R.1111-20-2 du code de la santé publique.

¹⁹³ Article R.1111-20-11 du code de la santé publique.

¹⁹⁴ Article R.1111-20-8 du code de la santé publique.

¹⁹⁵ Article R.1111-20-1 du code de la santé publique.

¹⁹⁶ Article R.1111-20-3 du code de la santé publique.

¹⁹⁷ Article R.1111-20-2 du code de la santé publique.

¹⁹⁸ Article R.1111-20-2 du code de la santé publique.

dossier pharmaceutique ni le nom de l'officine, ni le prix du médicament, ni le nom du médecin prescripteur. Le patient peut néanmoins s'opposer à l'inscription d'un ou plusieurs de ses médicaments dans ce dossier, le pharmacien lui remettant alors une attestation de refus d'alimentation du dossier pharmaceutique (annexe 10).

Une fois la dispensation enregistrée et le dossier pharmaceutique alimenté, il n'est plus possible pour le pharmacien de l'effacer. Il peut cependant rédiger un commentaire en format libre signalant une éventuelle erreur de dispensation apparaissant à l'écran lors d'une consultation ultérieure. Cette procédure a été mise en place en prévision de la prochaine fusion du dossier pharmaceutique avec le DMP afin qu'un autre professionnel de santé (pharmacien ou prescripteur) ne soit pas responsable d'une décision qu'il aurait prise au vu du dossier pharmaceutique avant sa modification.

B.2.3.2.c La consultation du dossier pharmaceutique

Au cours de la dispensation, le pharmacien consulte le dossier pharmaceutique de son patient afin de déceler et lui signaler les éventuels risques de redondances de traitements ou d'interactions médicamenteuses pouvant entraîner des effets iatrogènes connus et le cas échéant, refuser d'effectuer toute ou partie de la délivrance¹⁹⁹.

Les données du dossier pharmaceutique restent disponibles pendant quatre mois à compter de la date à laquelle elles ont été saisies puis sont archivées par l'hébergeur pendant une durée complémentaire de trente-deux mois afin de permettre au pharmacien de prendre les mesures nécessaires en cas d'alerte sanitaire relative à un médicament. Au terme de la durée totale de trois ans, l'hébergeur détruit les données, ainsi que les différentes traces d'interventions sur le dossier²⁰⁰.

La consultation du dossier pharmaceutique autorisée aux personnes habilitées à le créer a récemment été élargie aux médecins de certains établissements de santé, avec l'accord exprès du patient. Celui-ci peut néanmoins s'opposer à ce qu'un professionnel de santé consulte son dossier, une attestation de refus de consultation du dossier pharmaceutique lui est alors remise (annexe 11).

B.2.3.2.d L'édition et la clôture du dossier pharmaceutique

L'édition du dossier pharmaceutique sur support papier doit être possible à tout moment. En l'absence de plateforme sécurisée accessible par les patients sur internet comme pour le DMP, le pharmacien doit remettre une copie de l'intégralité des dispensations des quatre derniers mois inscrites dans le dossier pharmaceutique²⁰¹ (annexe 12) si celui-ci en fait la demande.

La clôture du dossier pharmaceutique peut être réalisée à tout moment et dans n'importe quelle officine raccordée au dispositif, sur demande du patient²⁰². Une attestation de clôture (annexe 13) lui est remise, puis est aussitôt transmise à l'hébergeur qui clôt le dossier dans les plus brefs délais, la totalité des données étant supprimées. Enfin, s'il n'a fait l'objet d'aucun accès durant une période de trois ans, le dossier pharmaceutique est automatiquement clos et supprimé chez l'hébergeur.

¹⁹⁹ Article R.1111-20-5 du code de la santé publique.

²⁰⁰ Article R.1111-20-11 du code de la santé publique.

²⁰¹ Article R.1111-20-9 du code de la santé publique.

²⁰² Article R.1111-20-4 du code de la santé publique.

B.2.3.3 L'ARTICULATION DU DOSSIER PHARMACEUTIQUE AVEC LE DMP ET LE WEB-MEDECIN

Si la montée en charge des systèmes informatisés du domaine de la santé fut rapide, les différents systèmes de gestion électronique des dossiers de patients se sont développés de manière anarchique.

Le projet d'intégration d'un volet « santé » dans la carte Vitale de chaque patient, voué à remplacer le traditionnel carnet de santé et à contenir des données de santé fut avorté en 2007 avec le projet de développement d'un dossier informatisé, dont l'hébergement est réalisé par un organisme tiers agréé et dont l'accès est réalisé par internet. Ce **dossier médical personnel (DMP)** sensé réunir toutes les données de santé des patients au moyen d'une seule et unique interface accessible via internet fut ainsi le précurseur du dossier pharmaceutique.

Instauré par la loi du 13 août 2004²⁰³, le DMP fut tout d'abord conduit par le groupement d'intérêt public du dossier médical personnel (GIP-DMP) pendant une phase d'expérimentation allant jusqu'au 31 décembre 2006 pour être finalement suspendu jusqu'en 2009 en raison des difficultés techniques rencontrées lors de son déploiement. Il fallut attendre la conférence du 9 avril 2009 de Madame Roselyne Bachelot-Narquin, ministre de la santé et des sports, pour proposer un plan de relance du DMP en prévoyant un lancement du dossier pour 2010 (95). C'est dans cette dynamique que le GIP-DMP et le GIP-CPS chargé de la gestion des cartes CPS disparaissent pour laisser place à l'ASIP Santé dont les fonctions sont élargies au développement des systèmes d'information partagés de santé en s'intégrant dans une démarche d'interopérabilité. Suite à l'avis favorable de la CNIL²⁰⁴, le grand départ du DMP élaboré par les sociétés Atos Origin et La Poste sur l'ensemble du territoire, fut donné le 2 décembre 2010. Depuis, tout patient peut demander à son médecin la création de son DMP pourvu que ce dernier dispose d'un logiciel compatible avec son utilisation, l'ASIP Santé parle ainsi de « DMP-Compatibilité »²⁰⁵.

Créé avec le consentement du patient, celui-ci peut demander à ce que certaines informations n'apparaissent pas dans son DMP ou en exiger la clôture à tout moment²⁰⁶. **Il est directement consultable en ligne par le patient** ainsi que par les professionnels de santé qu'il y autorise. Le DMP est destiné à renseigner l'ensemble des données de santé du patient recueillies « *à l'occasion de chaque acte ou consultation, les éléments diagnostiques et thérapeutiques nécessaires à la coordination des soins de la personne prise en charge* »²⁰⁷ (antécédents, allergies, comptes rendus médicaux, résultats d'examens radiologiques ou biologiques, traitements...).

Si le patient peut se connecter seul à son DMP²⁰⁸ en s'authentifiant avec un couple identifiant/mot de passe qui lui ont été remis lors de la création de son DMP, un professionnel de santé ne peut accéder au DMP de son patient qu'en présence conjointe de sa carte CPS et de la carte Vitale. Afin d'en renforcer la confidentialité, les données du DMP sont chiffrées et toute connexion ou modification du DMP est gardée en mémoire (76).

²⁰³ Loi n° 2004-810 du 13 août 2004 relative à l'assurance maladie.

²⁰⁴ Délibération n°2010-449 du 2 décembre 2010 portant autorisation des traitements de données personnelles mis en œuvre par les professionnels et établissements de santé nécessaires à la première phase de déploiement généralisé du dossier médical personnel.

²⁰⁵ La liste des logiciels DMP compatibles est disponible sur le site dédié au DMP (<http://www.dmp.gouv.fr/>).

²⁰⁶ Le dossier n'est alors plus alimenté mais les informations restent enregistrées chez l'hébergeur pendant une durée de 10 ans avant suppression définitive. Une suppression définitive sans délai est néanmoins possible sur demande du patient.

²⁰⁷ Article L.1111-15 du code de la santé publique.

²⁰⁸ Via la plateforme d'accès au DMP (<http://www.dmp.gouv.fr/>).

La sécurité des données du DMP est un élément fondamental du projet car de nombreuses compagnies d'assurance ou mutuelles pourraient avoir un intérêt à prendre connaissance de telles informations. Si cette interdiction paraît justifiée pour de tels organismes il peut être surprenant de constater que celle-ci s'applique également aux médecins du travail²⁰⁹, preuve d'une défiance très sévère à l'égard de ces médecins²¹⁰.

Afin de promouvoir et constater l'avancement du projet, l'ASIP Santé permet d'observer une carte d'évolution du nombre de DMP créés par région ainsi que le nombre d'établissements de santé adhérant au dispositif sur la plateforme en ligne dédiée au DMP. Environ 310 000 DMP ont été créés depuis son lancement grâce à l'implication de plus de 4000 professionnels de santé et plus de 231 établissements de santé à l'échelle nationale. Michel Gagneux, président de l'ASIP Santé, évoquait lors de la conférence parlementaire sur l'e-santé du 14 novembre 2012 que le DMP n'en était pourtant qu'à sa phase d'amorçage. Il est vrai que, comparé aux 25,8 millions de dossiers pharmaceutiques créés à ce jour (pour 22 195 officines soit 97,5%) (96), le DMP qui devait montrer la voie dans la dématérialisation des dossiers médicaux s'est rapidement fait doubler par l'outil performant élaboré par l'ordre des pharmaciens.

Malgré son retard, le DMP est pourtant voué à intégrer les données du dossier pharmaceutique afin de proposer une plateforme d'accès unique comme le prévoit l'article L. 1111-23 du code de la santé publique en précisant que « *les informations de ce dossier utiles à la coordination des soins sont reportées dans le dossier médical personnel* ». C'est ainsi que médecins et pharmaciens sont destinés à travailler, dans leur cadre de leur champ de compétences, autour du dossier d'un même patient grâce à un même outil dématérialisé.

Créé par la loi réformant l'assurance maladie du 13 août 2004, le dispositif du « **Web-médecin** » ou « **historique des remboursements** » est un service proposé par la caisse nationale d'assurance maladie permettant aux médecins, à l'occasion d'un acte médical, d'accéder à l'ensemble des soins, médicaments et examens qui ont été remboursés à leurs patients au cours des douze derniers mois. Il s'agit d'un listing de l'ensemble des informations nécessaires à l'identification des actes, produits ou prestations pris en charge par l'assurance maladie ainsi que les éléments constitutifs du protocole de soins de patients atteints d'affection de longue durée (ALD). Ce dispositif présente cependant de nombreuses limites puisqu'un médecin peut effectivement vérifier que son patient s'est vu prescrire un médicament mais ne peut en connaître la quantité ou encore constater qu'il s'est vu prescrire une analyse biologique, sans pouvoir prendre connaissance directement du résultat. En raison de ce caractère allégé donc à la fois plus pratique et moins coûteux cet outil fut annoncé comme une alternative possible au DMP en 2007²¹¹ mais son utilisation demeure encore marginale (97).

Si le consentement du patient est obligatoire pour la création et la consultation de son DMP²¹² ou de son dossier pharmaceutique²¹³, il n'est en revanche pas requis pour la création de son web-médecin établi par l'assurance maladie. Seule la consultation de cet historique requiert le consentement de la personne concernée²¹⁴.

²⁰⁹ Article L.1111-18 du code de la santé publique.

²¹⁰ Les médecins du travail s'étaient déjà vu interdire l'accès au carnet de santé par arrêté ministériel du 18 octobre 1996 en raison de leur rôle exclusivement préventif et non curatif.

²¹¹ Rapport du GIP-DMP du 14 octobre 2007.

²¹² Article L.1111-15 du code de la santé publique.

²¹³ Article L.1111-23 du code de la santé publique.

²¹⁴ Article L.162-4-3 du code de la sécurité sociale.

	WEB-MEDECIN	DOSSIER MEDICAL PERSONNEL	DOSSIER PHARMACEUTIQUE
Principaux objectifs	Faciliter les choix thérapeutiques des médecins.	Favoriser la coordination, la qualité et la continuité des soins.	Sécuriser la dispensation, transmettre les alertes sanitaires et les rappels de lots de médicaments.
Périmètre des données	Actes médicaux, examens diagnostics, médicaments remboursables par l'assurance maladie	Toute donnée de santé relative au patient (antécédents, allergies, résultats d'examens, traitements...	Les médicaments remboursables ou non, prescrits ou non (CIP, DCI, nom de présentation, quantité et date de délivrance).
Personnes habilitées à créer le dossier	L'assurance maladie	L'ASIP Santé par l'intermédiaire d'un dossier rempli par le patient	Un pharmacien ou un préparateur en pharmacie.
Personnes habilitées alimenter le dossier	L'assurance maladie	Les professionnels de santé autorisés par le patient avec la carte Vitale du patient et sa CPS	Un pharmacien ou un préparateur avec sa CPS et la carte Vitale du patient.
Personnes habilitées à consulter le dossier	• L'assurance maladie • Les médecins libéraux ayant signé une convention avec l'assurance maladie.	• Le patient lui-même (plateforme en ligne) • Tout professionnel de santé autorisé par le patient	• Le patient lui-même (remise d'une copie imprimée) • Un pharmacien (officine et PUI) ou un préparateur avec sa CPS et la carte Vitale du patient. • Les Médecins de certains établissements de santé
Recueil du consentement du patient pour la création du dossier	Non	Oui	Oui
Recueil du consentement pour consulter et alimenter le dossier	Oui	Oui	Oui

Tableau 21 : Comparaison de trois dossiers de santé : web-médecin, dossier médical personnel et dossier pharmaceutique (76).

B.2.3.4 LE RESEAU DU DOSSIER PHARMACEUTIQUE : VECTEUR D'ALERTE SANITAIRES ET DE RETRAITS DE LOTS

La généralisation du dossier pharmaceutique sur l'ensemble du territoire repose sur le déploiement d'un réseau performant et hautement sécurisé garant de la qualité de ce système et de la confidentialité des données. En marge de son déploiement à l'officine, le dossier pharmaceutique a évolué vers de nouveaux horizons en permettant également de diffuser les alertes sanitaires et les retraits de lots de médicaments dans les plus brefs délais. En effet, ce système présente l'avantage de fonctionner « en temps réel, nuits et jours de garde inclus » (98).

Les annonces de retrait du marché de médicaments régulièrement mises en lumière par les médias ne sont pas sans renforcer l'inquiétude générale des patients quant au circuit complexe qu'est celui du médicament. La diffusion en temps réel des alertes sanitaires et de retraits de

lots via la plate-forme du dossier pharmaceutique permet donc aux pharmaciens d'informer les patients le plus rapidement possible et d'anticiper efficacement leurs questions et leurs craintes, affirmant ainsi le rôle central du pharmacien au sein du circuit de distribution du médicament.

B.2.3.4.a La diffusion d'alertes sanitaires

C'est le 7 juillet 2010 que la Madame Isabelle Adenot décida pour la première fois de relayer aux pharmaciens une alerte sanitaire émanant de la Direction générale de la santé via le réseau du dossier pharmaceutique. Cette alerte mettait en évidence une augmentation du risque de fièvre hémorragique avec syndrome rénal suite à une infection par *hantavirus* dans le quart nord-est de la France. Cette alerte fut diffusée en moins d'une heure aux 1433 officines adhérant au dossier pharmaceutique dans les 6 régions du nord-est de la France concernées. Sur ces 1433 officines, 1415 ont pu réceptionner cette alerte dans les heures qui ont suivi, soit 98,8 % d'entre elles. Depuis, l'ordre utilise ainsi le canal du dossier pharmaceutique pour relayer, 24 heures sur 24 et 7 jours sur 7, les alertes sanitaires les plus urgentes émanant de la Direction générale de la santé (DGS-urgent).

L'objectif de ce dispositif n'est pas de diffuser toutes les alertes sanitaires mais seulement les plus importantes afin de ne pas submerger les pharmaciens d'informations. En effet, la diffusion de ces alertes est contrôlée, l'accord préalable du président de l'ordre est obligatoire pour toute diffusion d'alerte et demeure réservée à des alertes sanitaires graves et urgentes susceptibles d'avoir un impact sur l'exercice professionnel du pharmacien (99).

Concrètement, lorsque l'opérateur (pharmacien, préparateur...) s'identifie sur un poste de travail de l'officine, l'alerte s'affiche directement à l'écran du logiciel de gestion d'officine et ne disparaît que lorsque toutes les informations ont été cochées comme lues (écran bloquant). Elle s'affiche une seule fois pour un opérateur donné et non pour un poste. Un accusé de réception est alors retourné au serveur du dossier pharmaceutique afin de suivre la diffusion du message sur le territoire en temps réel.

B.2.3.4.b Les rappels et retraits de lots de médicaments

C'est dans cette même logique que la diffusion des alertes de rappels et de retraits de lots de produits de santé aux pharmaciens utilise la plate-forme du dossier pharmaceutique depuis le 3 novembre 2011. Jusqu'alors, les rappels et retraits de lots de médicaments du circuit officinal étaient régis par une convention entre le Conseil national de l'ordre des pharmaciens, les entreprises du médicament (LEEM) et la Chambre syndicale de la répartition pharmaceutique. Une fois validée par l'AFSSAPS (ex ANSM), l'alerte était transmise par fax aux grossistes répartiteurs, lesquels relayaient l'information auprès de toutes les officines au moyen d'un bordereau glissé dans un bac de livraison de médicaments.

La dématérialisation de ce bordereau en alerte électronique rend ainsi l'infrastructure du dossier pharmaceutique incontournable pour la transmission de ces retraits de lots. Il a pu être observé lors de la phase test du dossier pharmaceutique, que 90% des alertes étaient lues dans les 15 minutes qui suivent sa diffusion et que 95% des messages arrivaient à destination dans un délai d'une heure. Ce système permet donc de s'affranchir du délai de 24 à 48h de l'ancien système de diffusion et de mener ainsi une opération coordonnée aussi rapidement que possible.

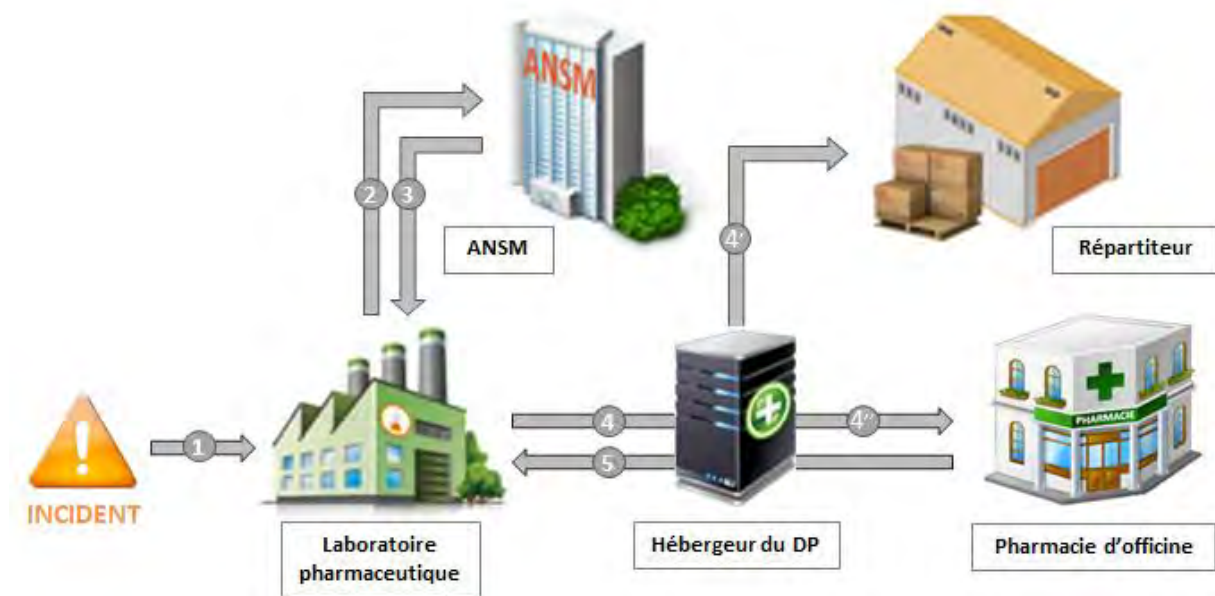


Figure 27 : Le dossier pharmaceutique au cœur du processus de rappel et de retrait de lots des médicaments.

En pratique, le pharmacien responsable²¹⁵ du laboratoire exploitant concerné communique directement l'information, validée par l'Agence nationale de sécurité du médicament, à l'hébergeur du dossier pharmaceutique. Celui-ci diffuse l'alerte à destination des organismes de répartition dans un format normalisé via le serveur du dossier pharmaceutique afin d'immobiliser les lots incriminés. Les officines reçoivent l'alerte sous forme d'un écran bloquant apparaissant sur l'écran du logiciel de gestion d'officine. Les retours émis par les pharmacies transitent en sens inverse afin d'en procéder à l'analyse et de dresser un bilan quant à la diffusion de l'alerte²¹⁶ (100).

Le réseau du dossier pharmaceutique est donc devenu incontournable dans la transmission des alertes permettant les rappels et retraits de lots par les fabricants. Il permet donc un suivi du parcours du médicament tout au long de son circuit de distribution, gage d'une traçabilité renforcée, en suivant le parcours d'un produit de sa fabrication à l'utilisateur final. **Cette traçabilité descendante** permet d'identifier toutes les étapes de la production à la dispensation du médicament et de prévenir les risques liés à un défaut de fabrication. Elle permet donc de connaître l'endroit exact où est situé un produit donné afin d'intervenir rapidement en effectuant des rappels de produits ou de lots et les retirer du circuit.

La traçabilité descendante des médicaments est réalisée en établissant une politique organisationnelle rigoureuse reposant sur une hiérarchisation logistique. Pour les produits de santé, les réflexions entre les partenaires de santé ont permis de décrire cinq niveaux hiérarchiques d'identification des produits. Une entité physique unitaire dénommée « unité commune de dispensation » (UCD) utilisée dans le circuit hospitalier correspond au plus bas niveau de cette hiérarchie (par exemple un comprimé). C'est à partir de cette unité identifiable par un code Datamatrix qu'il est possible de décrire tous les conditionnements ou états du produit, par multiplication (boîte de x comprimés) ou division (1/4 de comprimé). L'unité d'achat (boîte) est comme nous l'avons vu, marquée sur son conditionnement extérieur au

²¹⁵ Dont le statut et les missions sont détaillées par l'article R.5124-36 du code de la santé publique

²¹⁶ Les dernières officines encore non reliées au dossier pharmaceutique ainsi que les distributeurs en gros reçoivent une télécopie de l'alerte.

moyen d'un code Datamatrix renseignant son code CIP13, son numéro de lot de fabrication et sa date de péremption. Afin de faciliter la manipulation et le stockage des boîtes, celles-ci sont généralement regroupées en unité de stockage (de 7 boîtes par exemple) enveloppée d'un suremballage en plastique identifié au moyen d'un code-barres linéaire de type GS1-128. Les unités logistiques (cartons) et d'expédition (palettes) sont elles aussi marquées d'un code de type GS1-128 puisque la surface d'impression du code est étendue²¹⁷. La composition des unités logistiques (mise en carton) est une étape clé de la distribution du produit. Elle doit prendre en compte l'ensemble des contraintes logistiques liées au transport et au stockage et doit tenter de garantir une homogénéité maximale en termes de lots de fabrication. En effet, les boîtes étant identifiées par un numéro de lot, il est nécessaire que chaque unité logistique contienne un minimum de lots de fabrication différents (idéalement un seul) afin d'en faciliter la saisie informatique et la traçabilité.

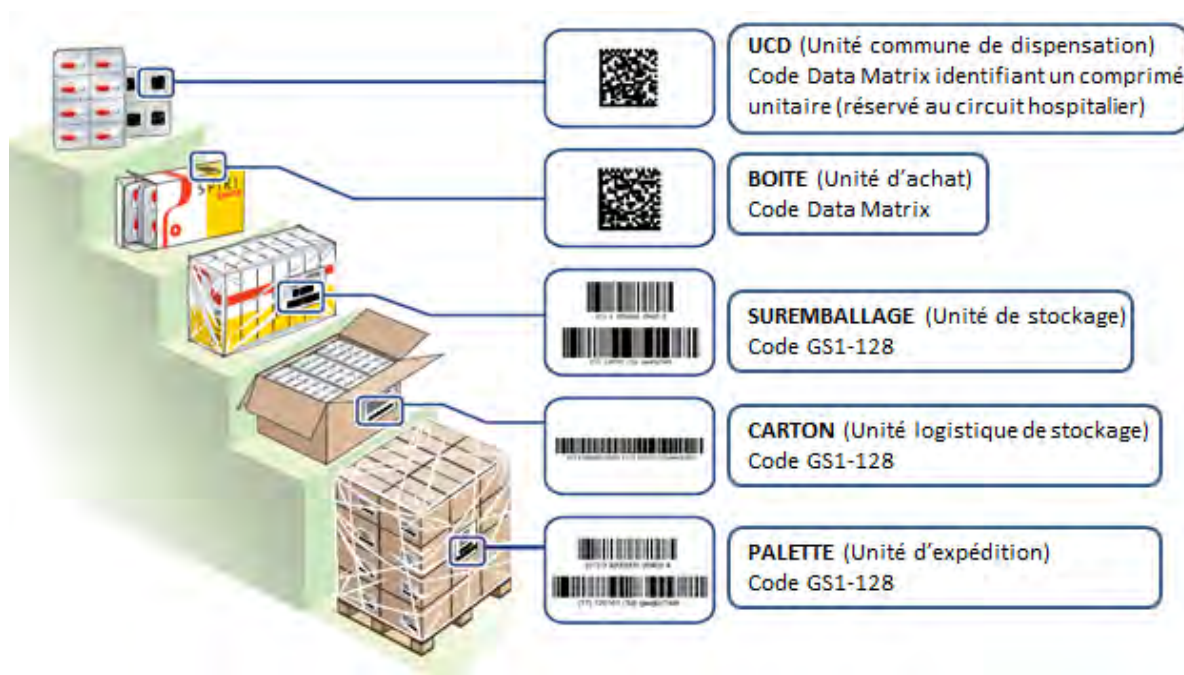


Figure 28: Les différents niveaux de conditionnement du médicament (101).

Grâce à cette identification précise de chaque conditionnement, il est ainsi possible à partir d'un lot incriminé, de connaître quels cartons et palettes de produits sont concernés et donc de remonter jusqu'aux officines impliquées. En l'état actuel du développement du dossier pharmaceutique, il n'est pas encore possible d'enregistrer le numéro de lot des médicaments dispensés. Cette fonction d'intégration des données du Datamatrix du conditionnement extérieur des médicaments sera prochainement intégrée au dossier pharmaceutique de manière à prolonger la procédure de retrait jusqu'au domicile du patient (102). Le pharmacien dûment informé du numéro de lot incriminé doit donc faire appel aux bases de données de son logiciel métier afin d'appeler l'ensemble des dossiers patients informatisés ayant fait l'objet d'une telle dispensation. Le pharmacien peut ainsi contacter les patients auxquels il aurait pu délivrer ce produit afin d'en avoir la confirmation et retirer ce produit du circuit de distribution en le remplaçant par un produit conforme.

²¹⁷ Il s'agit de codes 1D de type GTIN à 13 caractères différents pour chaque niveau d'emballage.

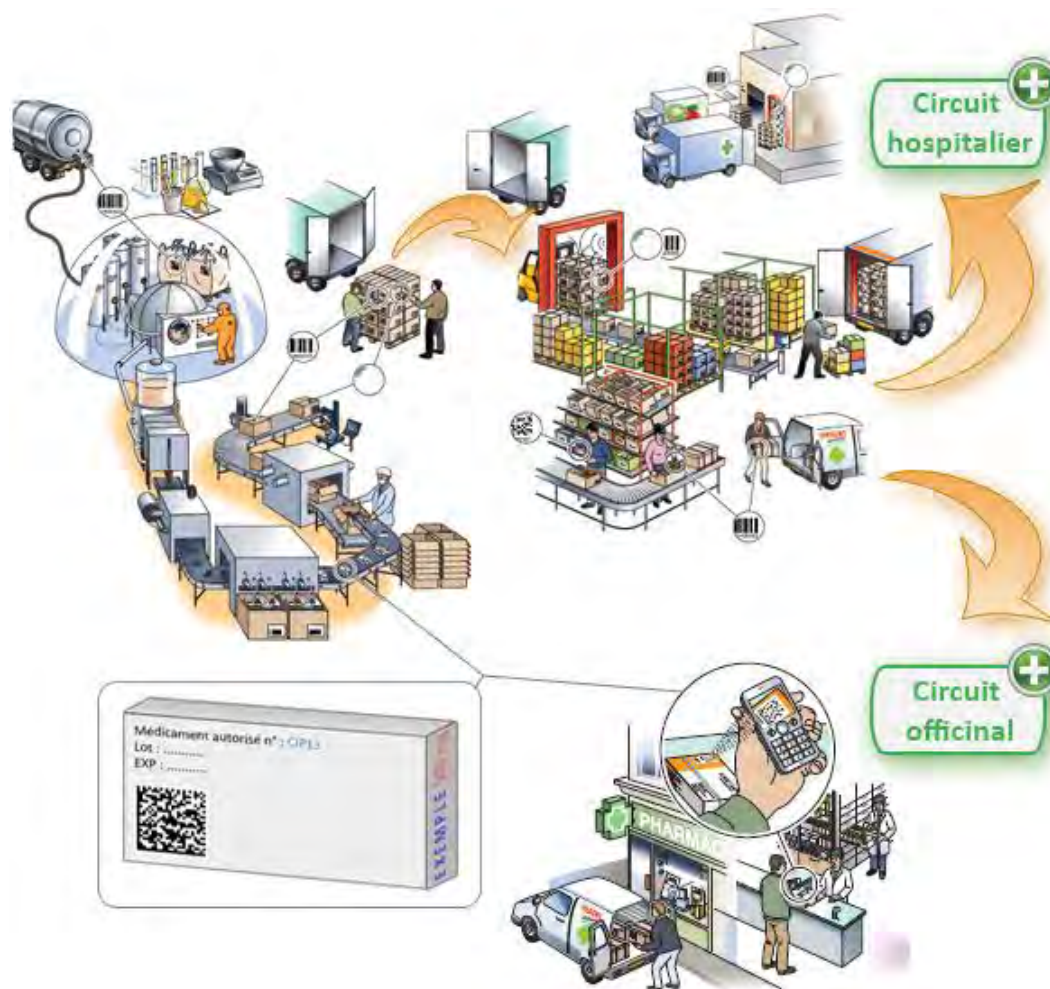


Figure 29 : L'identification des produits de santé au cœur du circuit du médicament.

La directive européenne sur les médicaments falsifiés²¹⁸ publiée le 1^{er} juillet 2011, visant à renforcer le contrôle des chaînes de distribution des médicaments et protéger les consommateurs contre les médicaments falsifiés, impose une évolution de l'identification des médicaments à prescription obligatoire à la boîte et non plus au lot, obligeant la France à faire évoluer son système de traçabilité selon cette méthode dite de **sérialisation**. C'est pourquoi l'avis du ministère de la santé du 29 janvier 2013 prévoit que le marquage du conditionnement extérieur des produits de santé soit « *interopérable avec les modalités d'échanges de l'identifiant européen unique par boîte à compter de 2017* ». Les enjeux organisationnels et financiers de la **sérialisation** de tels produits étant colossaux, la nécessité de développer un cadre de compatibilité et d'interopérabilité des systèmes est essentielle. Ainsi, le système de remplacement de la vignette pharmaceutique, vouée à disparaître, doit considérer la variabilité des informations relatives au prix et à la prise en charge des médicaments entre les différents pays. Ces informations étant variables d'un pays à l'autre, leur inclusion dans le Datamatrix rendrait la facturation de tels produits impossible (20).

A l'inverse, **la traçabilité ascendante** permet de remonter d'un produit fini vers les matières premières utilisées pour sa production. Elle s'avère donc très utile en cas de problème sur un produit pour connaître les causes d'un produit défectueux et pour éviter que cela ne se reproduise. Au-delà de la défectuosité constatée d'un produit, la traçabilité ascendante s'intègre dans la démarche de vigilance des produits de santé. En effet, toute fiche de

²¹⁸ Directive 2011/62/EU du Parlement européen et du Conseil du 8 Juin 2011,

déclaration de pharmacovigilance²¹⁹ renseigne l'identification des médicaments dispensés ainsi que leur numéro de lot. La pharmacovigilance a donc un rôle clé à jouer dans cette démarche de traçabilité par le regroupement d'événements indésirables imputables à un même lot de médicaments par exemple. Il sera d'ailleurs très prochainement possible de réaliser une télé-déclaration de pharmacovigilance afin de s'affranchir des inconvénients de l'envoi du formulaire papier par voie postale²²⁰. Dans ce domaine, le site pharmavigilance.fr lancé en avril 2012 par l'ordre des pharmaciens permet d'ores et déjà d'informer le grand public de l'importance des vigilances relatives aux produits de santé et de faciliter les déclarations.

B.2.3.5 LA SECURISATION DU DOSSIER PHARMACEUTIQUE

Les conditions juridiques de la protection des données du dossier pharmaceutique permettent de respecter les droits du patient tels qu'ils sont prévus par la loi informatique et liberté garantissant leur protection face aux risques liés au traitement automatisé de leurs données.

Les dossiers pharmaceutiques sont hébergés chez un hébergeur unique de données de santé à caractère personnel agréé comme le prévoit le code de la santé publique. C'est pour le moment la société SANTEOS qui est en charge de cette activité jusqu'à ce que la société DOCAPOST ne reprenne le flambeau à l'été 2013. Cet hébergeur est sélectionné par le Conseil national de l'ordre des pharmaciens qui passe avec lui un contrat précisant notamment les conditions techniques nécessaires pour assurer la qualité et la continuité du service rendu, la conservation, la sécurité, la confidentialité et l'intégrité des données, ainsi que leur interopérabilité avec le dossier médical personnel²²¹.

L'accès au dossier pharmaceutique d'un patient est protégé par la nécessité d'utiliser conjointement la carte Vitale du patient et la carte CPS²²² d'un pharmacien. De plus, toutes les informations composant le dossier pharmaceutique sont enregistrées, conservées et transférées dans des conditions de sécurité garanties par des moyens de chiffrement afin d'en préserver la confidentialité tout au long de leur traitement²²³.

B.2.3.5.a L'identification de l'officine

Lors de chaque tentative de connexion au serveur du dossier pharmaceutique, le numéro FINESS géographique²²⁴ permettant une identification physique de l'officine est transmis à l'hébergeur par le logiciel de gestion d'officine.

Cette étape d'identification de l'officine présente un double intérêt :

- garantir la traçabilité des interventions des différentes officines sur le dossier pharmaceutique d'un patient ;
- apporter des informations techniques complémentaires à l'ordre telles que la version du logiciel ou encore le type de connecteur utilisé.

²¹⁹ Disponible sur le site de l'Agence nationale de sécurité du médicament (<http://ansm.sante.fr>).

²²⁰ Il est cependant possible de transmettre le formulaire papier au centre régional de pharmacovigilance par fax ou en le numérisant et en l'envoyant par courrier électronique.

²²¹ Article R.1111-20-10 du code de la santé publique.

²²² Article R.1111-20-5 du code de la santé publique relatif à l'utilisation du dossier pharmaceutique.

²²³ Article R.1111-20-11 du code de la santé publique.

²²⁴ Par opposition au numéro FINESS juridique, ou numéro de facturation, utilisé pour la télétransmission des factures électroniques.

B.2.3.5.b Constitution et sécurisation des flux de données

Afin d'être correctement interprétées par les différents systèmes informatiques, les données doivent être retranscrites par le module du dossier pharmaceutique du logiciel officinal dans un format bien précis. Les données alphanumériques saisies dans le dossier pharmaceutique doivent donc être formatées, par exemple un champ de huit caractères numériques au format aaaammjj pour la date de naissance ...

Pour permettre à tous les éditeurs d'intégrer un module fiable et standardisé à leurs logiciels, **la norme HL7 (*Health Level 7*)** fut choisie pour le développement informatique du dossier pharmaceutique. Ce standard reconnu par l'ISO est bien connu des éditeurs qui l'utilisent depuis deux décennies. Particulièrement dédié à la transmission des données de santé, cette norme permet de définir la façon dont les paquets de données sont constitués et transmis afin d'être interprétables sans ambiguïté par les différents systèmes, en toute interopérabilité.

Contrairement à certains pays européens qui ont développé un véritable réseau national privé permettant la télétransmission de données de santé, les milliards de bits de données qui transitent chaque jour au travers des mailles du réseau du dossier pharmaceutique utilisent le réseau internet comme vecteur de transmission en raison de sa fiabilité et de sa rapidité. Il est cependant nécessaire de pouvoir s'assurer de l'authentification réciproque de chaque correspondant et de préserver l'intégrité et la confidentialité des données échangées avec le serveur du dossier pharmaceutique.

L'authentification forte du professionnel de santé est rendue possible par saisie du code porteur associé à sa carte CPS et l'utilisation de son certificat électronique d'authentification.

Comme nous l'avons vu, cet échange utilise le protocole de communication HTTP classique mais enrichi de fonctions de sécurité particulières (HTTPS). Ce protocole de transport est sécurisé selon la version 3 du protocole SSL (*Secure Sockets Layer*) ou HTTPS/SSLv3.0 permettant de créer comme un tunnel clos où seuls les ordinateurs à l'entrée et à la sortie (l'officine et l'hébergeur) peuvent lire le message (76). L'ASIP Santé permet ainsi aux pharmaciens d'utiliser un certificat serveur, dit « certificat SSL » qui permet la sécurisation d'une voie d'échange avec un serveur, ceci pendant toute la durée de la connexion. La sécurisation consiste en l'**authentification réciproque** du serveur (certificat SSL) et de l'utilisateur (certificat d'authentification CPS), ainsi que la **confidentialité** et l'**intégrité** des données échangées (77).

B.2.3.5.c La sécurité de l'hébergeur

Comme nous l'avons vu, les données contenues dans le dossier pharmaceutique sont amenées à être conservées jusqu'à 36 mois chez l'hébergeur, période durant laquelle il est impératif d'en contrôler l'accès, et préserver l'intégrité. Il est possible de dissocier ces données en deux catégories : les données relatives à l'identification du patient d'une part, et les données relatives à l'historique des dispensations, d'autre part.

Si les données sont chiffrées lors de leur transport, elles le demeurent également chez l'hébergeur où elles sont ainsi dissociées et stockées sur deux bases cryptées « étanches » :

- l'annuaire des patients fournit les identifiants (numéro de dossier pharmaceutique) en clair ;
- la base de dispensation contenant les données relatives aux traitements ainsi qu'une version chiffrée du numéro de dossier pharmaceutique.

La mise en correspondance des données issues de ces deux bases est réalisée lors de chaque connexion au dossier pharmaceutique d'un patient à partir des données d'identification afin d'y rattacher les données relatives aux dispensations, le lien entre les deux étant assuré comme nous l'avons vu, par le calcul d'un identifiant mettant en œuvre une fonction de hachage : le numéro de dossier pharmaceutique ou NDP. Afin de renforcer la sécurité et garantir la continuité du service, toutes les données sont dédoublées par l'hébergeur et stockées sur deux sites géographiquement séparés (103).

B.2.3.5.d La traçabilité des échanges

Afin de conserver toute trace de connexion ou d'utilisation du dossier pharmaceutique, chaque intervention effectuée est sauvegardée. Ainsi, toute création, consultation, alimentation, clôture, impression de l'historique, refus de consultation ou d'alimentation est horodatée et tenue à jour dans un fichier de l'officine couvrant la période des trente derniers jours. Il comprend notamment (76) :

- le type de données envoyées;
- l'identifiant unique du message et la taille du message (en kilo-octets);
- la date et l'heure d'envoi du message par l'officine (au format aaaammjjhhmmss) ;
- la date et l'heure de réception du message de réponse par l'officine (même format) ;
- la durée totale de la correspondance.

L'ensemble de ces données est ainsi sauvegardé afin de conserver une trace de chaque intervention sur le dossier pharmaceutique pouvant par exemple faire office de preuve.

B.2.4. LE PARTAGE DE DONNEES ENTRE PROFESSIONNELS DE SANTE

Le fax et les messageries électroniques sont devenus de véritables outils de travail au service des professionnels de santé mais ne représentent *a priori* pas un moyen de communication sûr pour transmettre des données confidentielles. En effet, une simple erreur de manipulation (adresse erronée, erreur de numérotation du fax destinataire...) peut conduire à divulguer des informations couvertes par le secret médical à des destinataires non habilités. Différents outils de messageries sécurisées de santé privées ont ainsi été développés afin de sécuriser les correspondances électroniques entre professionnels de santé, mais l'ASIP Santé souhaite désormais généraliser cet outil à l'échelle nationale en proposant une plateforme de messagerie unique : la MSSanté.

B.2.4.1 LA TELECOPIE

La télécopie consiste à dématérialiser la transmission d'un document papier par le biais d'une ligne téléphonique. La CNIL recommande certaines précautions concernant son usage outil :

- l'appareil doit être situé dans un local « médical », physiquement contrôlé et accessible uniquement au personnel médical et paramédical ;
- l'impression des messages doit être subordonnée à l'introduction d'un code d'accès personnel ;

- lors de l'émission des messages, le fax doit afficher l'identité du fax destinataire afin d'être assuré de son identité ;
- doubler l'envoi par fax d'un envoi des documents originaux au destinataire ;
- pré-enregistrer les destinataires potentiels dans le carnet d'adresses de l'appareil.

La télécopie est parfois utilisée en situation d'urgence pour la transmission d'ordonnances entre un prescripteur et une officine afin de permettre une dispensation rapide de produits de santé à un patient n'étant pas en mesure de présenter une prescription valide. Cette méthode est aussi parfois utilisée pour la transmission de documents complémentaires nécessaires à une dispensation (résultats d'analyses, protocoles thérapeutiques...) et pour anticiper la préparation des ordonnances dans le cadre des relations d'une officine avec une maison de retraite.

B.2.4.2 LES MESSAGERIES SECURISEES DE SANTE

Les messageries électroniques tendent à remplacer de plus en plus souvent la télécopie pour la transmission de documents entre professionnels de santé. Il existe de nombreux services de messagerie « grand public » disponibles sur internet mais la CNIL rappelle aux professionnels de santé « l'obligation éthique » d'utiliser un service de messagerie hautement sécurisé (63).

La messagerie sécurisée de santé est née du constat que ces messageries destinées au grand public ne constituaient pas un moyen sûr pour transmettre des données de santé nominatives. Une simple erreur de manipulation ou encore la non-confidentialité du réseau internet pourraient ainsi conduire un tiers non autorisé à prendre connaissance d'informations relevant du secret médical. Les récentes révélations sur les outils *Prism* et *Upstream* impliquant *a priori* certains services de clients de messagerie en ligne grand public, ne font que renforcer l'inquiétude quant à la confidentialité des données échangées par les professionnels de santé massivement utilisateurs de ces systèmes.

Le 25 octobre 2012, les conseils d'éthique et de déontologie de l'ASIP Santé ont proposé certaines recommandations aux professionnels de santé concernant l'usage actuellement très répandu des messageries mises à la disposition du public par les fournisseurs d'accès internet traditionnels. Ces services de messagerie ne permettent pas d'assurer les conditions satisfaisantes en matière de cryptage et de sécurisation de données sensibles telles que les données de santé. Leur utilisation par les professionnels de santé conduit ainsi à faire circuler des informations confidentielles en clair par des courriels non cryptés, alors que des services de messagerie sécurisée de santé (MSS) sont à leur disposition depuis plusieurs années (104). En effet, l'association APICEM proposait depuis 1996 la première MSS privée dédiée aux professionnels de santé. S'il existe actuellement une dizaine de prestataires de MSS, la solution APICRYPT développée par l'APICEM demeure la plus couramment utilisée et compte environ 30 000 utilisateurs.

Il est donc recommandé aux professionnels de santé qui persistent à transmettre les données couvertes par le secret médical via des messageries peu sécurisées de crypter les documents à l'aide d'un programme de chiffrement (type PGP) et de les envoyer au destinataire prévu en pièce jointe du message en lui communiquant le mot de passe nécessaire au décryptage du fichier par un moyen de communication différent (téléphone, SMS...) (104).

Afin de développer un service unique et durable, le GIP-CPS publia dès 2001 un référentiel d'homologation des messageries sécurisées de santé qui présentait le cahier des charges des

normes d'interopérabilité. Ce projet resta en suspens avec la fin de l'existence du GIP puis fut repris par l'ASIP Santé (105). La mise en ligne au mois de mai 2013 d'une première version du dossier des spécifications fonctionnelles et techniques relatif au développement du système **MSSanté** a ainsi fourni le premier élan nécessaire à la conception d'outils MSSanté-compatibles par les éditeurs de logiciels. C'est dans ce contexte que l'ASIP Santé met au point depuis plusieurs mois avec l'ensemble des ordres professionnels et les organisations professionnelles libérales et hospitalières un système de messageries sécurisées de santé qui repose sur trois principes :

- Proposer un cadre de développement des services de messageries sécurisées ;
- Créer un espace de confiance basé sur une communauté d'utilisateurs clairement identifiés (les professionnels de santé libéraux ou exerçant dans un établissement de santé) ;
- Mettre à disposition un annuaire national certifié de tous les utilisateurs basé sur le répertoire partagé des professionnels de santé (RPPS) (106).

Le déploiement de la MSSanté impose un niveau de sécurité au moins égal à celui qui régit les échanges par correspondance « papier » entre professionnels de santé. Les conditions à réunir sont donc (104) :

- Développer un service facile d'utilisation afin ne pas paralyser la production et la qualité des soins tout en garantissant un niveau de sécurité maximal ;
- Le recours à un hébergeur de données de santé agréé, l'usage de cette messagerie se traduisant par un hébergement temporaire des données échangées. Il en découle une obligation de disposer de l'agrément d'hébergeur de données de santé et de recueillir le consentement des patients, en application de l'article L.1111-8 du code de la santé publique. Le conseil d'éthique et de déontologie de l'ASIP Santé estime cependant qu'il n'est pas réaliste d'exiger un consentement à l'occasion de chaque échange ou pour chaque nouveau destinataire. La remise d'un document papier ou électronique rappelant également les droits du patient serait suffisant pour matérialiser ce consentement ;
- L'utilisation de la carte CPS pour la transmission de données par voie électronique afin de garantir une authentification forte des correspondants et d'attester de l'intégrité des données ;
- Garantir la confidentialité des données lors des échanges (chiffrement de transport) selon un procédé de chiffrement et l'utilisation de canaux de transmission sécurisés ;
- Elaborer un historique et un archivage des correspondances ;
- Intégrer les correspondances au DMP ;
- Elaborer un annuaire national disponible en ligne et alimenté par l'ASIP Santé.

La mise en œuvre d'un tel système est assumée par des opérateurs homologués enregistrés dans une « liste blanche » et disposant de certificats électroniques d'authentification délivrés par l'IGC-CPS.

Techniquement, il s'agirait d'un client de messagerie intégré au logiciel professionnel et directement accessible, permettant un échange de messages selon deux modalités selon le choix de l'opérateur :

- En utilisant les protocoles de messagerie standards (SMTP, IMAP) dont la transmission est sécurisée par le protocole TLS ou SSL et l'authentification est assurée par la carte CPS ;
- Par l'intermédiaire d'un service-web, c'est-à-dire une interface accessible via internet, après authentification de la carte CPS et renseignement d'un couple identifiant / mot de passe.

La campagne de recrutement d'utilisateurs a débuté depuis le mois d'avril par le biais de la version bêta du site mssante.fr, les premières homologations de clients de messageries devraient avoir lieu au mois de novembre 2013, tandis que le lancement officiel du projet devrait avoir lieu au mois de mars 2014 (106).

Comme nous le verrons, l'une des perspectives majeures pour notre système d'e-santé consiste en l'élaboration d'un outil d'e-prescription, véritable « passerelle électronique » sécurisée entre professionnels de santé. Un tel outil intégrant un service de messagerie sécurisée, l'e-prescription pourrait donc fournir l'élan nécessaire pour la généralisation de l'emploi de la MSSanté par les professionnels de santé.

B.2.5. LE E-PHARMACIEN AU CŒUR DES ORIENTATIONS STRATEGIQUES DE SANTE

Qu'il s'agisse de leurs logiciels professionnels ou de dossiers médicaux partagés, les professionnels de santé et particulièrement les pharmaciens, bénéficient d'outils puissants capables de les assister dans leur quotidien. Ce quotidien est cependant fréquemment bouleversé par de nouvelles orientations stratégiques visant principalement à améliorer la qualité, la sécurité et l'efficacité de notre système de santé.

La loi portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires du 21 juillet 2009 dite loi HPST, a ainsi marqué un véritable tournant pour la profession en enrichissant l'exercice du pharmacien d'officine de nouvelles missions. Dans la continuité de cette loi, la convention pharmaceutique régissant les rapports entre les pharmaciens et l'assurance maladie a par ailleurs introduit le principe d'entretiens individuels permettant d'améliorer la qualité des soins et du suivi des patients recevant un traitement anticoagulant et valorisant les rôles du pharmacien dans l'exercice de son art.

Compte-tenu de ses nouvelles attributions, nous verrons comment la dématérialisation peut, ou pourrait, assister les pharmaciens afin d'atteindre ses objectifs.

Si la dématérialisation des données et plus particulièrement de leur transmission présente de nombreux avantages, un pas de géant fut récemment franchi en permettant aux pharmaciens titulaires d'une officine de proposer un site de vente en ligne de médicaments, après autorisation. Le constat amer que laisse la mise en application dans l'urgence de cette mesure, montre que notre système de santé n'était peut-être pas suffisamment prêt à intégrer un tel dispositif. Considérant les risques liés à la vente en ligne de médicaments et le flou persistant sur le champ d'application de cette mesure, l'information des patients utilisateurs de tels sites, représente l'un des enjeux majeurs pour leur développement.

B.2.5.1 LES NOUVELLES MISSIONS DU PHARMACIEN D'OFFICINE

Les nouvelles missions confiées aux pharmaciens d'officines par la loi HPST constituent de véritables opportunités de valoriser leurs rôles et réaffirmer leur légitimité en tant que professionnels de santé. Cette loi crée ainsi l'article L.5125-1-1 du code de la santé publique précisant l'intitulé de chacune des huit missions qui lui sont confiées. Compte-tenu des orientations stratégiques en matière d'e-santé, il paraît primordial de prévoir une intégration de la dématérialisation des informations et des échanges dans l'accomplissement de ces missions. En recentrant la toile de l'e-santé sur le patient, le développement des échanges dématérialisés doit permettre d'améliorer la qualité de leur suivi et une meilleure coordination des soins. Il est ainsi prévu que les pharmaciens :

1° Participent aux soins de premier recours, définis en substance par l'article L.1411-11 du code de la santé publique. Il précise que l'accès aux soins de premier recours ainsi que la prise en charge continue des malades sont définis dans le respect des **exigences de proximité, qui s'apprécie en termes de distance et de temps de parcours, de qualité et de sécurité.**

Ces soins concernent :

- La prévention, le dépistage, le diagnostic, le traitement et le suivi des patients ;
- La dispensation et l'administration des médicaments, produits et dispositifs médicaux, ainsi que le conseil pharmaceutique ;
- L'orientation dans le système de soins et le secteur médico-social ;
- L'éducation pour la santé.

Si l'e-santé ne permettra jamais de combler les « déserts médicaux » en matière d'accessibilité aux soins, particulièrement d'urgence, elle rapproche les patients des professionnels de santé, ainsi que les professionnels de santé entre eux, contribuant ainsi à améliorer l'accessibilité et la qualité des soins de premiers recours. Le logiciel de gestion d'officine et le dossier pharmaceutique proposent comme nous l'avons vu, d'incroyables capacités d'aide à la dispensation et au suivi des patients mais il faut reconnaître que les pharmaciens n'en exploitent que rarement le potentiel. En effet, les logiciels proposent bien souvent différents modules paramétrables susceptibles de soumettre des informations aux pharmaciens relatives au dépistage et à la prévention de la survenue de maladies ou d'effet indésirable lié à l'utilisation d'un médicament, compte tenu du contexte (âge, antécédents, épidémie, toxicomanie, grossesse...) ainsi qu'à l'éducation pour la santé sur de nombreuses thématiques.

Par ailleurs, le nouveau site dédié au médicament publié par le Ministère des affaires sociales et de la santé depuis le 1^{er} octobre 2013²²⁵ vient enrichir le panel de services reconnus d'informations sur la santé, garantissant un accès autonome des patients à une source sûre de données dédiée aux médicaments. Cette plateforme en ligne publie le « résumé des caractéristiques du produit » de chaque médicament et en clarifie le circuit afin de lever certaines inquiétudes et estomper la méfiance des patients, consommateurs de ce système. Au-delà de ce rôle de base de données en ligne accessible par tous, ce site offre de nombreuses rubriques d'informations sur les médicaments, leur bon usage, les acteurs de leur circuit, les contrôles et leurs autorités, mais aussi concernant leur vigilance. Il comporte en effet une rubrique dédiée à la vigilance des produits de santé et particulièrement la pharmacovigilance,

²²⁵ Disponible à l'adresse <http://medicaments.gouv.fr>

en rappelant ses principes fondamentaux et en fournissant des liens directs permettant d'accéder aux différents formulaires de déclaration d'effet indésirable sous forme dématérialisée²²⁶.

Enfin, la possibilité récente pour certains pharmaciens titulaires d'une officine physique bien réelle, de proposer un site internet dédié à la vente en ligne de médicaments doit également contribuer à favoriser l'information et l'éducation des patients sur la santé.

2° Participant à la coopération entre professionnels de santé. Dans ce domaine, le développement des dossiers médicaux partagés (DMP et dossier pharmaceutique) conjugué au à celui des messageries sécurisées de santé permettent de rapprocher les professionnels de santé autour d'informations communes au sujet de leurs patients. Comme nous le verrons, le nouveau rôle de « pharmacien correspondant » pourrait également permettre de réaffirmer la place du pharmacien dans notre système de santé, notamment en développant ses interactions et donc sa coopération, avec les médecins. La finalisation du DMP qui devait permettre de renseigner des résultats d'analyses pourrait également permettre d'élargir ce cercle de coopération avec les laboratoires d'analyses et de biologie médicale.

3° Participant à la mission de service public de la permanence des soins. La publication des coordonnées de la pharmacie de garde via le site internet d'une officine permet, par exemple, d'améliorer l'information des patients qui n'ont par exemple plus à se déplacer jusqu'à l'officine. Il peut s'agir d'un avantage certain pour les patients dont la mobilité est réduite.

4° Concourent aux actions de veille et de protection sanitaire organisées par les autorités de santé notamment par l'intermédiaire des procédures d'alertes sanitaires et de rappels de lots émises via le dossier pharmaceutique. Les pharmaciens disposent par ailleurs de nombreuses plateformes en ligne leur permettant de participer aux missions de l'Institut national de veille sanitaire²²⁷ ou encore, de réaliser des déclarations de pharmacovigilance en ligne.

5° Peuvent participer à l'éducation thérapeutique et aux actions d'accompagnement d'un patient afin de le rendre plus autonome en facilitant son adhésion aux traitements prescrits et en améliorant sa qualité de vie²²⁸. Le contenu de ces programmes et actions d'accompagnement est conforme à un cahier des charges national défini par arrêté et mis en œuvre localement par le biais des Agences régionales de santé²²⁹. De nombreux supports peuvent être utilisés lors de séances individuelles ou collectives d'éducation thérapeutique mais la diversité des TIC offre un large panel de supports multimédia utilisant à la fois des images, des sons, des animations et des vidéos permettant une bonne compréhension des informations par les patients.

Afin de sensibiliser les patients sur la nécessité d'une bonne observance à leur traitement, de les aider et réaliser un suivi, le logiciel LGPI développé par Pharmagest Interactive a innové en proposant de multiples services dont le pilulier électronique intelligent, le DO-Pill Secure™. Il s'agit d'un pilulier doté de puces électroniques préalablement rempli avec l'aide du pharmacien émettant un signal visuel et/ou sonore au moment de prise des comprimés et permettant de transmettre automatiquement les informations relatives à chaque prise (heure,

²²⁶ La communication de ce formulaire au centre régional de pharmacovigilance de référence peut ensuite être réalisée par voie postale ou électronique.

²²⁷ <http://www.invs.sante.fr/>

²²⁸ Article L.1161-1 du code de la santé publique.

²²⁹ Article L.1161-2 du code de la santé publique.

jour, retard oubli...). Ce système innovant permet ainsi un suivi extrêmement rigoureux de l'observance d'un patient, par exemple dans un contexte de troubles mnésiques.

Les développements convergents de la domotique et des gérontechnologies permettent plus largement d'améliorer le confort de vie de patients à mobilité réduite comme certaines personnes âgées mais encore de lutter contre leur fragilité :

- Par une meilleure appréhension de la diminution des capacités physiques et de la perte de mobilité ;
- En limitant leur isolement social par le rétablissement de liens sociaux que la personne n'a plus la capacité physique ou psychique d'entretenir ;
- En accompagnant les personnes souffrant de troubles cognitifs (107).

6° Peuvent assurer la fonction de pharmacien référent pour un établissement accueillant des personnes âgées ou qui leur apportent à domicile une assistance dans les actes quotidiens de la vie, des prestations de soins ou une aide à l'insertion sociale²³⁰. Lorsqu'il s'agit par exemple d'une maison de retraite, les ordonnances établies par le prescripteur au moment de leurs visites sont transmises sous forme dématérialisée par télécopie ou e-mail au pharmacien référent de l'officine. Celui-ci collecte les médicaments nécessaires à chaque dispensation et chaque processus de facturation est mis en pause. Lorsqu'il dispense les médicaments au sein de l'établissement, il les confie à l'infirmier responsable à qui il communique les informations et conseils associés aux traitements. Le pharmacien récupère les originaux des ordonnances et les cartes Vitale des patients et termine le processus de facturation de chaque ordonnance après avoir vérifié la correspondance exacte entre l'ordonnance faxée et celle effectivement remise. La dématérialisation de la transmission de la prescription permet donc de faciliter l'exercice de la fonction de pharmacien référent d'une maison de retraite et laisse présager des nombreux bénéfices qu'un système d'e-prescription pourrait offrir à notre système de santé.

7° Peuvent être désignés comme correspondants au sein de l'équipe de soins par le patient depuis la parution du décret du 5 avril 2011²³¹. A ce titre, ils peuvent, à la demande du médecin ou avec son accord, renouveler périodiquement des traitements chroniques, ajuster, au besoin, leur posologie et effectuer des bilans de médications destinés à en optimiser les effets. Un protocole détermine le nombre de renouvellements autorisés et leur durée²³² et chaque prescription précise les posologies minimales et maximales, la durée totale du traitement comprenant les renouvellements ainsi que la nature éventuelle des prestations à associer selon le produit prescrit. Ce protocole peut prévoir un bilan de médication réalisé par le pharmacien, comprenant l'évaluation de l'observance et de la tolérance du traitement ou d'autres éléments plus spécifiques précisés par le prescripteur. Le pharmacien recense les effets indésirables et identifie les interactions avec d'autres traitements en cours dont il a connaissance puis communique le bilan réalisé au prescripteur. Le pharmacien mentionne le renouvellement sur l'ordonnance ou la présence d'une feuille qui lui est annexée, notifiant un ajustement de posologie, datée et signée par le pharmacien, avec le timbre de l'officine, ainsi que le nom du médicament concerné et la nouvelle posologie. Le pharmacien informe ensuite le médecin de l'adaptation posologique et reporte éventuellement l'ensemble de ces informations dans le dossier pharmaceutique du patient²³³.

²³⁰ Article L.312-1 du code de l'action sociale et des familles.

²³¹ Décret n° 2011-375 du 5 avril 2011 relatif aux missions des pharmaciens d'officine correspondants.

²³² La durée totale de la prescription et des renouvellements ne peut excéder douze mois.

²³³ Article R.5125-33-5 du code de la santé publique.

Comme nous le verrons, **la mise en œuvre d'un service d'e-prescription en France pourrait constituer une véritable opportunité de valoriser les missions du « e-pharmacien correspondant »** comme c'est par exemple le cas aux Etats-Unis au travers du système *Surescripts*TM. Un tel système permettant aux médecins et aux pharmaciens de communiquer au sujet d'une prescription et notamment d'actualiser le statut de délivrance d'une dispensation, il s'agirait d'une opportunité idéale d'affirmer ce rôle de pharmacien correspondant, avec l'aide des TIC.

8° Peuvent proposer des conseils et prestations destinés à favoriser l'amélioration ou le maintien de l'état de santé des personnes.

Ces nouvelles missions du pharmacien d'officine furent suivies de la mise en œuvre d'un nouveau mode de rémunération plus en adéquation avec son activité. Le rapport de l'inspection générale des affaires sociales intitulé « Pharmacies d'officine : rémunération, mission, réseau » publié en juin 2011 soulignait l'inadéquation des modalités de rémunération et d'exercice de l'activité officinale au contexte économique actuel d'une part et aux missions de santé publique qui relèvent de cette profession d'autre part. La rémunération fondée sur une marge par boîte vendue fait du prix des produits et de leur évolution un déterminant de la dispensation, ce qui relève d'une approche réductrice de l'activité officinale.

C'est dans la continuité de la loi HPST et afin de promouvoir la qualité de la dispensation et valoriser l'engagement des pharmaciens d'officine dans des missions de santé publique que la convention nationale organisant les rapports entre les pharmaciens titulaires d'officine et l'assurance maladie intègre un nouveau dispositif. Celui-ci définit ainsi de nouveaux modes de rémunération destinés notamment à valoriser la qualité de l'exercice pharmaceutique et les missions de conseil et d'accompagnement du pharmacien d'officine.

La première pierre de cet édifice consiste dans le suivi par les pharmaciens d'officine, de patients traités par anticoagulants oraux au long cours. Les principaux objectifs de cette mesure visent ainsi à diminuer l'incidence de survenue d'évènements iatrogènes et améliorer l'observance des patients. Ces entretiens portent pour le moment sur les patients traités par un médicament anticoagulant anti-vitamine K (AVK) et seront prochainement étendus au suivi des patients asthmatiques.

Concrètement, il s'agit d'un entretien individuel entre le patient et son pharmacien réalisé dans un local adapté afin d'en préserver la confidentialité, au cours duquel il exerce son rôle de conseil pour l'initiation, l'observance et le suivi du traitement.

Ce suivi régulier fait l'objet d'une rémunération annuelle de quarante euros, en fonction du respect des engagements individuels de santé publique, c'est à dire :

- réaliser un entretien à l'instauration du traitement et au moins deux entretiens par an ;
- s'assurer de la réalisation de l'INR ;
- en cas de besoin prendre contact avec le prescripteur avec le consentement du patient.

Au cours de cet entretien, le pharmacien dispose d'une « fiche de suivi patient » qu'il complète au fur et à mesure de l'entretien afin de remplir l'ensemble des objectifs. Les logiciels de gestion d'officine tels que LGPI intègrent ainsi désormais un module de suivi des patients permettant au pharmacien de conduire ses entretiens, compléter et sauvegarder les informations qui y sont relatives, directement dans le dossier du patient.

Alors que les familles de quatre personnes traitées par Pradaxa^{® 234}, décédées début 2013, ont porté plainte contre le laboratoire allemand *Boehringer Ingelheim* qui le commercialise, il apparaît désormais urgent de généraliser et poursuivre les efforts entrepris pour améliorer le suivi des patients traités par tous types d'anticoagulants.

Enfin, il est intéressant de constater l'engouement de certains patients, notamment ceux atteints de pathologies chroniques, pour la dématérialisation de leurs données de santé. Ainsi, il n'est plus rare d'être confronté à certains patients utilisant par exemple des carnets de suivi de la glycémie, de la pression artérielle ou de l'INR sur *smartphone* au moyen d'applications. L'application iBGStar[®] Diabète Manager développée par le laboratoire Sanofi-Aventis permet par exemple de connecter un lecteur de glycémie électronique directement au téléphone, dont les résultats sont enregistrés et exploités par une application associée. Le patient diabétique peut ainsi de connaître l'évolution des valeurs de sa glycémie dans le temps au moyen de graphiques et de tableaux mis en forme automatiquement. Il peut éventuellement imprimer des relevés de mesures ou les transmettre à un professionnel de santé par messagerie électronique.

L'application gratuite « Ma pharmacie mobile » créée en 2011 par la société Pharmagest permet aux pharmaciens adhérents, quel que soit leur logiciel, d'accompagner leurs patients au quotidien dans leur traitement avec des rappels de prise de médicaments ou encore d'envoyer des alertes de pharmacovigilance. Par ailleurs, cette application permet aux patients de localiser les pharmacies adhérentes à proximité et de transmettre une photographie de leur ordonnance via le réseau mobile afin que le pharmacien anticipe la préparation de la dispensation. Elle lui permet enfin d'interagir avec son pharmacien via la rubrique « mes demandes de conseil » afin de lui poser des questions relatives à son traitement, enrichies d'éventuelles photos (108).

D'autres applications à vocation plus publicitaire ont également vu le jour sous l'impulsion de certains groupements tels que PHR (« ipharmacien ») ou Giphar. Il est cependant important de clarifier la position de ces applications en terme de publicité de l'officine, puisque le groupe « Plus Pharmacie » a été condamné en janvier 2012 par le tribunal de grande instance de Paris pour la diffusion de son application illicite car elle ne permettait de localiser que les pharmacies sous ce label (109).

De nombreux outils et applications numériques permettent donc aujourd'hui d'éduquer et d'impliquer plus facilement les patients dans le suivi de leur maladie et de leur traitement, gage d'adhésion aux protocoles de soins et d'un suivi thérapeutique de qualité.

²³⁴ Le Pradaxa[®], inhibiteur direct de la thrombine, est un médicament anticoagulant de nouvelle génération présentant certains avantages par rapport aux AVK (régime alimentaire moins strict, suivi biologique allégé...), mais dont il n'existe pour le moment pas « d'antidote ». Compte tenu des risques liés à leur utilisation, il convient de rappeler qu'il n'existe aucun argument pour changer le traitement d'un patient équilibré sous AVK.

B.2.5.2 LA VENTE EN LIGNE DE MEDICAMENTS PAR LES OFFICINES EN FRANCE

Depuis le 2 janvier 2013, les pharmaciens établis en France, titulaires d'une pharmacie d'officine, peuvent vendre des médicaments sur Internet sous certaines conditions. Il est important de noter que cette démarche a été plus subie que choisie par les autorités françaises compte tenu de l'obligation de transposer, dans les délais, la directive européenne²³⁵ relative à la prévention de l'introduction dans la chaîne d'approvisionnement légale de médicaments falsifiés.

Les règles de bonnes pratiques relatives à la conception et l'exploitation d'un tel site sont définies par l'arrêté du 20 juin 2013 relatif aux bonnes pratiques de dispensation des médicaments par voie électronique, entré en vigueur le 12 juillet 2013. Depuis, l'activité de dispensation au détail de médicaments des officines n'est donc plus strictement cantonnée aux locaux de l'officine. Elle peut être mise en œuvre à distance par voie électronique, conformément aux dispositions de l'ordonnance du 19 décembre 2012 relative au renforcement de la sécurité de la chaîne d'approvisionnement des médicaments, à l'encadrement de la vente de médicaments sur internet et à la lutte contre la falsification de médicaments et de son décret d'application du 31 décembre 2012.

L'extension de la surface de vente d'une officine sur « la toile » marquant un véritable tournant dans l'exercice de la profession, reste une pratique cependant très encadrée et nécessite avant tout une **autorisation préalable de l'agence régionale de santé** compétente territorialement.

Un médicament sur deux acheté via internet étant une contrefaçon selon l'Organisation mondiale de la santé, leur vente en ligne est donc source de risques pour la santé des patients. Ces risques étant parfaitement décrits par le nouveau site du ministère chargé de la santé dédié aux médicaments mais encore par la thèse de Philippe Stivanin²³⁶ sur la vente électronique de médicaments et la protection des patients, nous nous contenterons de décrire les modalités d'application de cette nouvelle mesure, conformément à l'arrêté du 20 juin 2013.

Depuis, les principales inquiétudes de l'ordre des pharmaciens et des agences régionales de santé portent sur deux points principaux :

- L'exploitation frauduleuse de sites illégaux liés à des noms de domaines tombés dans le domaine public. L'ordre a ainsi déjà déposé onze plaintes après avoir constaté l'existence de sites hébergés dans des pays étrangers proposant la vente en ligne de médicaments en usurpant l'identité d'une officine française bien réelle ;
- Le non-respect des règles relatives à la conception, l'hébergement et l'exploitation de tels sites par les pharmaciens qui soumettent leurs dossiers aux agences régionales de santé chargées d'en valider la conformité.

²³⁵ Directive européenne 2011/62/UE instituant un code communautaire relatif aux médicaments à usage humain, en ce qui concerne la prévention de l'introduction dans la chaîne d'approvisionnement légale de médicaments falsifiés,

²³⁶ STIVANIN Philippe. Vente électronique de médicaments et protection des patients.- 152p. Thèse : Pharmacie : Toulouse 3 : 2011 ; 2011TOU32106.

B.2.5.2.a Bonnes pratiques liées au commerce électronique de médicaments

Le site internet de la pharmacie doit être considéré comme le prolongement virtuel d'une officine autorisée et ouverte au public. Afin de garantir un même niveau de qualité et de sécurité qu'au comptoir, la dispensation des médicaments par voie électronique est réalisée selon les mêmes principes, conformément aux règles de bonnes pratiques, c'est-à-dire :

- En préservant, l'indépendance professionnelle du pharmacien et le respect du secret professionnel ;
- En présentant l'activité officinale de façon neutre et objective afin de ne pas solliciter sa clientèle par des procédés contraires à la dignité de la profession ;
- En se conformant à son devoir de conseil lorsqu'il délivre un médicament ne requérant pas de prescription médicale ;
- En préservant son devoir de refuser la délivrance d'un médicament lorsqu'il estime que l'intérêt de la santé du patient l'exige ;
- En s'abstenant d'émettre un quelconque diagnostic et en incitant le patient à consulter un praticien qualifié lorsque cela paraît nécessaire ;
- En respectant les règles relatives à la publicité de l'officine et en n'incitant pas les patients à la consommation abusive de médicaments.

La publicité des médicaments ne doit pas être trompeuse ni porter atteinte à la protection de la santé publique. Elle doit présenter le médicament de façon objective et favoriser son bon usage. Le pharmacien doit s'abstenir de tout acte de concurrence déloyale et ne doit pas solliciter la clientèle par des procédés et moyens contraires à la dignité de la profession.

B.2.5.2.b Médicaments faisant l'objet du commerce électronique

Les débuts balbutiants de la vente en ligne de médicaments par les officines françaises sont en partie liés à une définition initiale imprécise du périmètre des médicaments susceptibles de faire l'objet de e-commerce en France. L'article 7 de l'ordonnance du 19 décembre 2012 créant l'article L.5125-34 du code de la santé publique prévoyait initialement que seuls les médicaments de médication officinale pouvant être présentés en accès direct au public de l'officine et ayant obtenue une autorisation de mise sur le marché puissent faire l'objet d'une l'activité de commerce électronique²³⁷, soit environ 350 produits. Cependant, par ses décisions du 14 février 2013 et du 17 juillet 2013, le Conseil d'Etat a déclaré cet article non conforme au droit européen sur le sujet, autorisant ainsi la vente en ligne de tous les médicaments non soumis à prescription médicale obligatoire, soit environ 4500 produits.

La présentation de chaque médicament doit être réalisée de façon objective, claire et non trompeuse et doit **seulement** comprendre :

- La dénomination de fantaisie du médicament **et** sa dénomination commune ;
- La ou les indications thérapeutiques de l'autorisation de mise sur le marché ;

²³⁷ Ainsi que certains médicaments homéopathiques et certains médicaments à base de plantes visés aux articles L.5121-13 et L.5121-14-1 du code de la santé publique.

- La forme galénique et le nombre d'unités de prise ;
- Le prix en euros toutes taxes comprises est affiché de manière claire, lisible et non ambiguë pour le patient. Il doit être précisé qu'il ne comprend pas les frais de livraison qui seront clairement indiqués au moment de la commande. Le prix doit être affiché de manière identique pour chaque médicament, sans artifice de mise en valeur (caractères gras, couleurs...) afin d'éviter toute promotion ou mise en avant d'un médicament particulier.
- Une mention spéciale indiquant que les informations relatives aux précautions d'emploi (interactions médicamenteuses, contre-indications, mises en garde spéciales, effets indésirables...) ainsi que la posologie sont détaillées par la notice du médicament disponible en format PDF et imprimable.
- Un lien hypertexte vers le « résumé des caractéristiques du produit » du médicament disponible sur le site de l'Agence nationale de sécurité du médicament et des produits de santé ou, le cas échéant, sur le site de l'Agence européenne du médicament ;
- Les photos du conditionnement devant représenter le médicament tel qu'il est proposé à la vente en officine. Toutes les photos doivent être de la même taille et présenter le médicament de manière claire et non ambiguë.

Ils doivent être classés par catégorie générale d'indication (douleurs, fièvre, nausées, toux...) puis de substances actives. A l'intérieur de chaque catégorie, le classement est établi par ordre alphabétique, sans artifice de mise en valeur, afin d'éviter toute forme de promotion ou d'incitation à une consommation abusive des médicaments.

B.2.5.2.c Identification administrative du site de l'officine

Le commerce électronique des médicaments est réalisé à partir d'un site internet, adossé à une pharmacie d'officine autorisée bien réelle, et dont la création a été autorisée par le directeur général de l'agence régionale de santé compétente. Conformément aux dispositions de la loi informatique et libertés et de la loi du 21 juin 2004 pour la confiance dans l'économie numérique, certaines mentions légales doivent être obligatoirement être publiées sur le site internet de l'officine. Lorsqu'un patient sollicite les services d'un tel site, il doit en effet pouvoir être en mesure de l'identifier comme celui d'une officine physique régulièrement autorisée.

INFORMATIONS OBLIGATOIRES	INFORMATIONS NON-OBLIGATOIRES
- La raison sociale de l'officine et le numéro de licence - Les noms et prénoms du ou des pharmaciens et leur numéro RPPS - Les adresses postale et électronique de l'officine ainsi que les numéros de téléphone et de télécopie - La dénomination sociale et les coordonnées de l'hébergeur du site internet - Le nom et l'adresse de l'agence régionale de santé compétente	- Le numéro individuel d'identification relatif à l'assujettissement à la taxe sur la valeur ajoutée (TVA) - Le numéro d'inscription au registre du commerce et des sociétés - Le code APE (47.73 Z pour « Commerce de détail de produits pharmaceutiques en magasin spécialisé ») - Le numéro SIRET

Tableau 22 : L'identification administrative du site internet de commerce en ligne d'une pharmacie d'officine.

Afin d'informer et rassurer les patients consultant un tel site internet, celui-ci doit également comporter différents logos enrichis d'un lien hypertexte :

- le logo commun à tous les Etats membres de l'Union européenne, qui a trait au commerce électronique des médicaments ;
- Le logo du Conseil de l'ordre des pharmaciens permettant notamment l'accès à la liste des sites de commerce en ligne de médicaments régulièrement autorisés par l'agence régionale de santé ;
- Le logo de l'Agence nationale de sécurité du médicament avec un lien permettant une déclaration d'effets indésirables par le patient et jouer un rôle de relais des alertes sanitaires;
- Le logo du ministère chargé de la santé.

L'accès à ces informations doit être « *facile, direct et permanent* »²³⁸ sur l'ensemble des pages du site grâce à un lien renvoyant à une page dédiée s'intitulant « Qui sommes-nous ? ».

La multiplication de sites illégaux de vente ligne usurpant l'identité d'officines françaises bien réelles reste à ce jour une véritable problématique. En attribuant à chaque pharmacie un sous-nom de domaine lié à pharma-france.fr, l'ordre des pharmaciens souhaite ainsi lutter contre la pratique de « *cybersquatting* » consistant en l'usurpation de l'identité d'une officine par l'utilisation d'un nom de domaine disponible.

B.2.5.2.d Règles techniques de conception

S'il ne peut en déléguer l'exploitation, la conception et la maintenance du site internet de commerce électronique de médicaments d'une officine peut être réalisée par le pharmacien lui-même (titulaire ou adjoint), mais il peut solliciter les services d'une entreprise sous-traitante sous certaines conditions. Certaines règles doivent cependant être respectées afin de garantir une compréhension parfaite ainsi qu'une bonne orientation du patient au cours de sa navigation.

Un tel site doit donc être rédigé en langue française et éventuellement traduit en plusieurs langues. D'un point de vue conceptuel, le site nécessite toutefois un certain savoir-faire en matière de programmation puisqu'il doit proposer différentes fonctions automatisées. De simples connaissances en langage HTML ne permettent donc *a priori* pas de concevoir un tel site dont le fonctionnement doit reposer sur l'utilisation de bases données (par exemple MySQL) et de langages plus complexes tels que le PHP ou le Javascript. Un système automatisé doit ainsi permettre à chacun la création d'un compte personnel suite à un processus d'inscription²³⁹ au cours duquel le visiteur renseigne son nom, son prénom, sa date de naissance et son adresse électronique. Cette formalité permet à la personne d'accéder par la suite à un espace privé intitulé « Mon compte » recensant notamment les commandes passées ainsi que l'intégralité de ses échanges avec le pharmacien.

Un onglet spécifique doit en outre identifier clairement la partie du site réservée à la vente de médicaments, afin de les distinguer des autres produits éventuellement commercialisés. Au

²³⁸ Article 19 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

²³⁹ Ce processus doit pouvoir être réversible et chacun doit pouvoir se désinscrire à tout moment.

sein de cette partie, seuls sont autorisés les liens hypertextes vers les sites institutionnels des autorités de santé et vers le site du Conseil national de l'ordre des pharmaciens²⁴⁰.

En raison de leur difficile contrôle, les forums de discussion en ligne sont proscrits et les lettres d'information ne doivent comporter, s'agissant du médicament, que des informations émanant des autorités sanitaires. Par ailleurs, la recherche de référencement dans des moteurs de recherche ou des comparateurs de prix contre rémunération est formellement interdite. Enfin, la date de mise à jour de toutes les informations présentes sur le site est indiquée sur chaque page du site internet par la mention « Page mise à jour le... ».

B.2.5.2.e L'e-dispensation

La dispensation de produits de santé et plus particulièrement s'agissant de médicaments ne peut être résumée à une simple délivrance. Par ses facultés d'analyse et ses conseils, le pharmacien permet ainsi de réaliser chaque dispensation en toute sécurité, en délivrant une information adaptée au contexte. Il n'est ainsi possible pour un pharmacien autorisé, de vendre des médicaments en ligne que si un échange interactif pertinent est rendu possible avant la validation de la commande. Une réponse **automatisée** à une question posée par le patient n'est donc pas suffisante pour assurer une information et un conseil adaptés au cas particulier de chaque patient.

Ainsi, lors de la première commande réalisée par un patient, celui-ci doit remplir un questionnaire en ligne afin que le pharmacien puisse attester de l'adéquation de la commande à l'état de santé du patient et qu'il puisse déceler d'éventuelles incompatibilités. Outre les informations recueillies au cours de l'inscription du patient sur le site, il prend ainsi connaissance de son âge, son poids, son sexe, ses traitements en cours, ses antécédents allergiques et, le cas échéant, son état de grossesse ou d'allaitement. Avant validation de la commande, le patient atteste de l'exactitude de ces informations et les met éventuellement à jour, puis le pharmacien procède à une validation du questionnaire, justifiant qu'il a pris connaissance des informations fournies par le patient. Afin de répondre aux attentes et aux questions des patients et transmettre un conseil pertinent et adapté à chaque dispensation, un système permettant un dialogue par courriel ou sous forme d'une boîte de dialogue en ligne doit être proposé par le site de l'officine. Le système choisi doit permettre de préserver la confidentialité des échanges entre le pharmacien et son patient. Tous ces échanges sont enregistrés, tracés, et imprimables directement par le patient.

La vente de médicaments en ligne par une officine française mettant en œuvre un traitement automatisé de données à caractère personnel, les patients doivent être informés de la mise en œuvre des traitements et de leurs droits d'accès et de rectification des données²⁴¹. Les pharmaciens doivent par ailleurs procéder à une déclaration normale de leur site auprès de la CNIL et doivent avoir impérativement recours, comme nous l'avons vu, à un hébergeur de données de santé agréé. Elles sont stockées dans des bases de données garantissant la confidentialité, l'intégrité et la pertinence des informations collectées pendant une durée de trois ans.

Au moment de la commande, le patient doit être informé que dans le cadre de la dispensation par voie électronique, son dossier pharmaceutique ne peut être alimenté par le pharmacien. Il lui est toutefois indiqué que celui-ci peut être renseigné *a posteriori*, dès lors qu'il se rend à

²⁴⁰ Les liens hypertextes vers les sites des entreprises pharmaceutiques sont, par ailleurs, strictement interdits sur l'ensemble du site.

²⁴¹ Ils ne disposent en revanche pas d'un droit d'opposition concernant la création de leur compte et du questionnaire qu'ils remplissent.

l'officine physique qui lui a délivré le médicament dans les quatre mois suivant la validation de la commande. Avant le paiement en ligne, le patient âgé d'au moins seize ans doit accepter les conditions générales de vente, assimilées à un contrat électronique, en cochant la case « j'accepte » du formulaire.

La pharmacie d'officine demeurant un lieu de **dispensation au détail de médicaments**, la quantité maximale de médicaments commandés doit être conforme à la durée du traitement indiquée dans le résumé des caractéristiques du produit et ne peut excéder un mois de traitement à la posologie usuelle, ou la quantité maximale nécessaire au traitement d'épisodes aigus. Aucune quantité minimale d'achat ne peut en revanche être exigée.

Une fois transmise et validée par le patient, le pharmacien assure personnellement la délivrance des médicaments dont les informations sont enregistrées dans le logiciel officinal et la commande est préparée au sein des locaux de l'officine, dans un espace adapté à cet effet. Le patient pourra ensuite venir chercher ses médicaments en personne, directement à l'officine ou se faire envoyer ou livrer par le pharmacien comme le prévoit le code de la santé publique lorsque le patient est dans l'impossibilité de se déplacer, notamment en raison de son état de santé, de son âge ou de situations géographiques particulières²⁴². Dans le cas d'un envoi par voie postale, les délais de traitement de la commande et le montant des frais de ports doivent être clairement indiqués au patient au moment de la commande. Les médicaments sont ainsi placés dans un paquet scellé, opaque au nom du seul patient, et dont la fermeture est telle que le destinataire puisse s'assurer qu'il n'a pas pu être ouvert par un tiers²⁴³. Le pharmacien veille à ce que les conditions de transport soient compatibles avec la bonne conservation des médicaments puis sont envoyés sous sa responsabilité.

Enfin, la vente en ligne de médicaments par une officine française autorisée présente un avantage singulier lié à ce nouveau type d'interaction du pharmacien avec ses patients. En effet, il ne s'agit pas d'une simple transaction commerciale en ligne mais bel et bien d'une dispensation de médicaments, incluant une analyse pharmaceutique de la requête d'un patient. Malgré toute la bonne volonté des pharmaciens, il est en pratique, au comptoir officinal, parfois très difficile de récolter les informations nécessaires à la dispensation de médicaments de médication officinale auprès de patients parfois pressés ou ne souhaitant pas se confier. Ces questionnaires permettent donc de récolter à coup sûr les informations nécessaires pour assurer la sécurité de l'e-dispensation.

L'un des principaux défis à relever afin de sécuriser la vente en ligne des médicaments par des officines françaises consiste à poursuivre les efforts entrepris par l'ordre des pharmaciens en collaboration avec les agences régionales de santé contre la multiplication de sites illégaux. Lorsqu'il souhaite avoir recours au service de vente en ligne de médicaments proposés par une officine, chaque patient peut préalablement consulter l'annuaire recensant les sites régulièrement autorisés à exercer une activité de e-commerce, publié via le site du conseil national de l'ordre des pharmaciens²⁴⁴.

Si les officines françaises peuvent désormais dématérialiser une partie de leur espace de vente, leurs sites de vente en ligne de médicaments ne pourront remplacer pleinement l'interaction physique des patients avec leurs pharmaciens, source de confiance permettant l'établissement d'un dialogue spontané et l'observation éventuelle de certains symptômes.

²⁴² Article R.5125-50 du code de la santé publique.

²⁴³ Article R.5125-47 du code de la santé publique.

²⁴⁴ Cet annuaire est accessible à l'adresse : <http://www.ordre.pharmacien.fr/ecommerce/search> et sous forme d'une liste sur le site nouveau site du médicament du ministère de la santé : <http://medicaments.gouv.fr>

Chapitre 3 : L'E-PRESCRIPTION : PERSPECTIVE D'AVENIR MAJEURE POUR L'E-SANTE EN FRANCE

L'essor de l'informatique des dernières décennies permet aujourd'hui de dématérialiser les différents supports de données utiles à la dispensation des produits de santé ainsi qu'à leur prise en charge par les organismes d'assurance maladie. Les ordonnances délivrées par les professionnels de santé habilités demeurent cependant le support réglementaire de prescriptions médicales en France même s'il est désormais possible de transmettre une prescription par voie électronique sous certaines conditions depuis 2004.

Afin de renforcer la démarche de simplification des tâches administratives, la convention organisant les rapports entre les pharmaciens d'officine et l'assurance maladie du 4 avril 2012 prévoit de poursuivre les démarches engagées pour la modernisation de notre système de santé, en dématérialisant la prescription à la source, conformément aux recommandations de l'inspection générale des affaires sociales dans son rapport de juin 2011 sur les missions de la pharmacie d'officine (110). Dans la continuité du projet de dématérialisation des pièces justificatives, l'assurance maladie en collaboration avec les ordres concernés, planifient ainsi l'élaboration d'un système de transmission d'ordonnances par voie électronique.

Ce projet repose sur l'article 34 de la loi n° 2004-810 du 13 août 2004 relative à l'assurance maladie autorisant la transmission de prescriptions de soins ou de produits de santé par courriel sous certaines conditions :

- le prescripteur doit être clairement identifié,
- l'ordonnance doit être « *établie, transmise et conservée dans des conditions propres à garantir son intégrité et sa confidentialité* »,
- le praticien doit avoir préalablement procédé à l'examen du patient (éventuellement par un acte de télémedecine), sauf à titre exceptionnel en cas d'urgence.

Cette procédure exceptionnellement utilisée actuellement permet généralement de dépanner certains patients en situation d'urgence ou ne s'étant pas aperçu de la fin de validité de leur ordonnance.

C'est le CLIO Santé²⁴⁵ rassemblant des représentants des sept ordres de professions de santé qui a donné le départ du premier élan fédérateur autour de l'e-prescription en France. La note d'orientation publiée en janvier 2012 vise ainsi à définir les orientations stratégiques d'un tel projet sur le territoire français compte tenu des contraintes techniques et juridiques imposées par notre système de santé. Le comité s'est appuyé sur l'étude des systèmes d'e-santé opérationnels à l'étranger afin de mettre en évidence les principales difficultés rencontrées.

Au-delà d'une simple transmission d'une ordonnance par courriel, le CLIO Santé présente le service d'e-prescription comme un **outil complet offrant de multiples fonctions** visant à optimiser la sécurité et la qualité de son exécution en permettant (111) :

- le dépôt de prescriptions électroniques dans une base de données sécurisée (comparable à celle du dossier pharmaceutique) ;
- la recherche d'une prescription enregistrée dans la base de données ;

²⁴⁵ Comité de liaison inter-ordres de santé.

- la mise à jour du statut d'exécution de la prescription (entièrement exécutée, partiellement exécutée, à renouveler...);

- de communiquer par messagerie sécurisée avec le prescripteur lors de problèmes rencontrés lors de l'exécution de la prescription. Ce type de correspondance asynchrone mais « en direct » permettrait aux pharmaciens de ne pas perturber les prescripteurs dans leur exercice par un appel téléphonique ;

- de signer chaque prescription et sécuriser l'utilisation du dispositif grâce à la carte CPS permettant d'assurer la confidentialité et l'intégrité des données traitées ainsi que l'authentification formelle des professionnels de santé impliqués en intégrant un historique des traces.

Son périmètre porte sur les prescriptions de médicaments et de dispositifs médicaux, d'actes de soins ou de rééducation, d'examens radiologiques et d'analyses biologiques (111).

Si de tels systèmes sont actuellement opérationnels à l'étranger, il n'est qu'à l'état de projet en France, sous l'impulsion du CLIO Santé et de la Caisse nationale d'assurance maladie. La France, pionnière en matière d'e-santé est désormais dépassée dans ce domaine par de nombreux pays, notamment européens. Le retard accumulé par la France dans la course européenne à l'e-santé n'est pas insurmontable et pourrait même constituer un atout. En s'inspirant des actions brillamment menées dans certains pays, il serait en effet possible de promouvoir la généralisation du dossier médical personnel et finaliser notre système déjà doté d'un outil d'e-dispensation performant : le dossier pharmaceutique.

L'étude des différents systèmes opérationnels à l'étranger nous permettra de mettre en évidence les principales contraintes rencontrées dans ces pays afin d'émettre certaines suggestions pour la conception d'un système d'e-prescription intégré à notre paysage d'e-santé.

B.3.1. L'ORDONNANCE MEDICALE EN FRANCE

Véritable outil de travail des professionnels de santé, l'ordonnance médicale prescrivant des produits de santé constitue avant tout le support de la stratégie thérapeutique élaborée par un prescripteur pour son patient et doit ainsi renseigner différentes informations réglementairement définies. Pièce justificative transmise par les pharmaciens aux organismes d'assurance maladie, la copie numérisée de l'ordonnance doit en outre comporter les informations permettant le remboursement éventuel des frais engagés.

B.3.1.1 STATUT JURIDIQUE

Lorsqu'elle prescrit des produits de santé, l'ordonnance ne peut être réduite à un ordre de délivrance de produits de santé par un pharmacien. En effet, les informations devant réglementairement être portées sur toute ordonnance doivent garantir au patient une bonne information sur la stratégie thérapeutique adoptée et le montant de la facture correspondante.

La prescription de médicaments ou de tout produit de santé n'est cependant pas réservée aux seuls médecins. Les chirurgiens-dentistes, les sages-femmes, les vétérinaires ainsi que les directeurs de laboratoires d'analyses de biologie médicales sont en effet autorisés à prescrire avec cependant certaines limites selon les corps de métiers²⁴⁶.

²⁴⁶ Article R.5132-6 du code de la santé publique.

Le statut de l'ordonnance en tant que support légal pour la prescription de médicaments est apporté par l'article R.5132-3 du code de la santé publique qui en précise également le contenu réglementaire. Elle doit être rédigée **après examen du patient** « *lisiblement en langue française et datée, pour permettre l'identification du praticien dont elle émane et être signée par lui* ».

Il est intéressant de noter que le code de la santé publique exige un examen clinique du patient préalable à la remise d'une ordonnance, tandis que la loi du 13 août 2004 prévoit que la transmission d'une ordonnance par voie électronique puisse s'en affranchir en situation d'urgence. Il s'agit là d'une particularité de notre code de la santé publique constituant l'un des paramètres juridiques à intégrer pour la mise en œuvre d'un système d'e-prescription en France.

B.3.1.2 LES DIFFERENTS TYPES D'ORDONNANCES

L'une des premières contraintes techniques liées à la dématérialisation des ordonnances à la source consiste en l'existence d'une certaine diversité des supports de prescription. Si les ordonnances simples sécurisées ou non sont bien connues de tous, d'autres moins répandues utilisent des modèles homologués par le Centre d'enregistrement et de révision des formulaires administratifs (CERFA) qu'il est nécessaire de considérer dans le cadre d'étude de développement d'un outil d'e-prescription en France.

Quel que soit le type d'ordonnance, certaines informations doivent réglementairement figurer lors de sa rédaction par le prescripteur. Elles sont destinées au patient pour la bonne compréhension de la stratégie thérapeutique élaborée par le prescripteur, au pharmacien afin d'assurer l'analyse pharmaceutique et la dispensation de l'ordonnance, et aux organismes d'assurance maladie impliqués dans le remboursement des dépenses susceptibles d'être prises en charge.

Si les médicaments dits « de médication officinale » sont disponibles en libre accès dans les pharmacies, les substances vénéneuses appartenant aux listes I et II, ainsi que les stupéfiants, les médicaments d'exceptions et à prescription restreinte doivent être prescrits sur des ordonnances particulières selon des règles bien précises.

Il est ainsi possible de mettre en évidence quatre types d'ordonnances ²⁴⁷ :

- **Les ordonnances simples, non sécurisées** permettent la prescription de médicaments ou de préparations dont le principe actif est inscrit sur les listes I ou II des substances vénéneuses. Elles sont dites non-sécurisées car ces prescriptions peuvent être rédigées sur toute feuille vierge de papier blanc pourvu que les informations devant réglementairement figurer sur une telle ordonnance soient présentes, il s'agit ²⁴⁸ :

- **des données d'identification du prescripteur** : son nom, sa qualité (qualification ou titre), son identifiant, son adresse. Le numéro d'identification du prescripteur peut parfois être également exprimé sous forme d'un code-barres unidimensionnel permettant une saisie rapide et sans erreur ;

- **de la date de la prescription ;**

²⁴⁷ Un document pré-imprimé, et homologué (N° Cerfa : 11264*02 - N° d'homologation ministérielle : S3323c) permet en outre la prescription, la dispensation, l'injection et la prise en charge des vaccins antigrippaux sous certaines conditions.

²⁴⁸ Article R.5132-3 du code de la santé publique.

- **des données d'identification du patient** : nom et prénom, le sexe et l'âge du malade et si nécessaire, sa taille et son poids ;

- **des informations relatives au traitement** : dénomination du médicament ou du produit prescrit, ou le principe actif du médicament désigné par sa dénomination commune, et s'il s'agit d'une préparation, sa formule détaillée. Pour chaque spécialité, la posologie, la durée du traitement ou le nombre d'unités de conditionnement, le mode d'emploi et le cas échéant, le nombre de renouvellements de la prescription doivent être précisés.

- **le cas échéant, de certaines mentions particulières** : « usage professionnel », « non substituable », « non remboursable » ou « hors AMM » ;

- **de la signature manuscrite du prescripteur** qui doit être apposée directement sous la dernière ligne de prescription.

Tout prescripteur peut en outre préciser s'il le souhaite son prénom, son numéro de télécopie, ses jours et heures de consultation, des données d'identification de médecins associés, sa situation vis-à-vis des organismes d'assurance maladie ou encore d'éventuelles distinctions honorifiques reconnues par la République française²⁴⁹.

Si chaque ordonnance est unique, les prescripteurs peuvent utiliser des ordonnances sur lesquelles sont pré-imprimées ses données d'identification. Elles sont ensuite complétées et personnalisées au moment de la consultation d'un patient, de façon manuscrite ou à l'aide d'un logiciel d'aide à la prescription. Le problème de la non-sécurisation de telles ordonnances à maintes fois été soulevé et particulièrement depuis que les prescripteurs rédigent massivement de telles prescriptions directement sur leur ordinateur. Alors que l'ordonnance historiquement manuscrite permettait aux pharmaciens de déceler certaines falsifications ou ajouts postérieurement à sa rédaction, il paraît aujourd'hui enfantin pour toute personne malveillante d'altérer l'intégrité (modifications, ajouts d'informations...), voire de reproduire de fausses ordonnances vierges, à partir d'une ordonnance non sécurisée licite, produite par un logiciel d'aide à la prescription.

• **Les ordonnances sécurisées** sont obligatoires pour la prescription de médicaments classés comme stupéfiants mais peuvent tout à fait être utilisées en lieu et place d'une ordonnance simple. Elles sont fabriquées et pré-imprimées par des sociétés agréées par l'Association française de normalisation (AFNOR) sur du papier blanc naturel sans azurant. Elles sont ornées d'un filigrane ombré figurant un caducée dont la pré-impression est réalisée à l'encre bleue de teinte et d'intensité déterminée également utilisée pour les informations relatives au prescripteur. Chacune d'elles comporte également le numéro d'identification du lot d'ordonnance ainsi qu'un carré pré-imprimé en micro-lettres sans le coin inférieur droit permettant d'inscrire le nombre de lignes de spécialités prescrites (annexe 14).

Pour la prescription de médicaments stupéfiants ou soumis à une telle réglementation, le prescripteur indique en toutes lettres le nombre d'unités thérapeutiques par prise, le nombre de prises et le dosage s'il s'agit de spécialités, les doses ou les concentrations de substances et le nombre d'unités ou le volume s'il s'agit de préparations et dans certains cas, le nom du pharmacien désigné par le patient pour effectuer la délivrance. Lorsqu'un tel traitement est fractionné, le prescripteur mentionne sur l'ordonnance la durée de traitement correspondant à chaque fraction ou éventuellement apposer la mention "délivrance en une seule fois".

²⁴⁹ Article R.4127-79 du code de la santé publique.

- **Les ordonnances bizonnes** constituent un modèle d'ordonnance permettant de distinguer deux parties distinctes de prescription sur l'ordonnance :

- une partie supérieure pour les traitements relatifs à une affection de longue durée (ALD) ouvrant droit à une exonération du ticket modérateur et pris en charge intégralement par l'assurance maladie,

- une partie inférieure pour le traitement de maladies intercurrentes, sans rapport avec ladite ALD et pris en charge aux taux habituels.

Les prescripteurs peuvent se procurer un modèle type homologué et pré-imprimé²⁵⁰ d'ordonnance bizonnes (annexe 15) auprès des organismes d'assurance maladie²⁵¹.

- **Les ordonnances de médicaments d'exception** sont obligatoires pour la prescription de traitements particulièrement onéreux et d'indications précises ou « médicaments d'exception ». Le but est de permettre une traçabilité et un contrôle de leur prescription par les organismes d'assurance maladie de manière rigoureuse au moyen d'un modèle d'ordonnance « cerfatisé » à quatre volets autocopiants²⁵² (annexe 16).

S'il est difficile de concevoir que les ordonnances papiers puissent totalement disparaître, il est en revanche tout à fait probable d'envisager que seules les ordonnances simples et sécurisées perdurent sous forme matérielle. Les ordonnances bizonnes et de médicaments d'exception répondant à des modèles normalisés sont avant tout destinées à faciliter le contrôle des dépenses engagées par l'assurance maladie dans un contexte de prescription particulier. Il est donc possible de concevoir que la dématérialisation de ces types d'ordonnances puisse avoir un impact majeur sur les rapports des professionnels de santé avec l'assurance maladie en contrôlant au plus près l'efficacité économique des procédures de prescription et de dispensation.

B.3.1.3 ROLES DE L'ORDONNANCE VIS A VIS DE SES DESTINATAIRES

Les rôles d'une ordonnance sont multiples au regard de ses différents destinataires. Il s'agit du support de prescription autorisant un pharmacien à délivrer des produits de santé et permettant au patient de connaître et se remémorer la stratégie thérapeutique établie. Ainsi muni d'une ordonnance, tout patient peut librement choisir le pharmacien qu'il souhaite pour assurer la délivrance des produits prescrits. Le pharmacien exécutant reporte les informations liées à la dispensation et relatives au coût du traitement, sur l'ordonnance et en télétransmet une copie numérisée à la caisse d'assurance maladie concernée.

B.3.1.3.a Outil de coopération interdisciplinaire

Lors de l'accueil à l'officine d'un patient muni d'une ordonnance, tout pharmacien doit réaliser un premier contrôle de l'ordonnance en présence du patient, directement au comptoir. Il analyse en premier lieu la licéité de l'ordonnance, ainsi que la qualité et la cohérence de la prescription. Il affine son analyse par la recherche de contre-indications ou d'interactions liées à cette prescription puis va chercher les boîtes de médicaments prescrits en arrière-boutique. En prenant l'ordonnance avec lui au moment de sélectionner le conditionnement à délivrer, le pharmacien peut réaliser un contrôle supplémentaire en vérifiant sur l'ordonnance qu'il

²⁵⁰ N° Cerfa : 14465*01, N° d'homologation ministérielle : S3321b.

²⁵¹ Arrêté du 17 juillet 2012 fixant le modèle du formulaire « ordonnance bizonne » utilisé pour les prescriptions destinées aux assurés reconnus atteints d'une affection exonérante.

²⁵² N° Cerfa : 12708*02 - N° d'homologation ministérielle : S3326b

délivre le bon conditionnement, en quantité nécessaire et suffisante et le plus « économique », conformément aux exigences de l'assurance maladie. Enfin, un ou plusieurs contrôles supplémentaires de l'ensemble de la prescription sont réalisés au moment du processus de facturation et de la délivrance, de nouveau en présence du patient.

En dématérialisant l'ordonnance à la source, les pharmaciens seraient ainsi privés de ce support lui permettant de réaliser ce contrôle « en arrière-boutique » qu'il pourrait être périlleux de réaliser uniquement sur la base d'informations mémorisées par le pharmacien. Nous nous efforcerons donc de proposer une alternative efficace à ce désagrément dans le modèle d'e-prescription proposé ci-après.

L'intégration aux logiciels d'aide à la prescription et à la dispensation de bases de données certifiées relatives aux médicaments conjuguée aux efforts entrepris dans la détection automatisée d'incompatibilités thérapeutiques ne peuvent cependant garantir la fin des erreurs de prescription et de dispensation. Grâce à leurs connaissances et leurs capacités d'analyse, les pharmaciens jouent donc un rôle crucial dans la sécurisation du processus de dispensation.

Lors d'une détection d'incompatibilité d'un médicament avec l'état physiopathologique du patient ou de médicaments entre eux, le pharmacien doit parfois communiquer par téléphone avec des prescripteurs souvent débordés, les interrompant au cours de leurs consultations. En y intégrant la plateforme de messagerie sécurisée MSSanté en cours de développement par l'ASIP Santé, un dispositif d'e-prescription permettrait d'établir entre eux une ligne directe de communication sécurisée et asynchrone, autour de la prescription et sa délivrance.

B.3.1.3.b Pièce justificative de prise en charge par l'assurance maladie

Pour permettre la prise en charge des médicaments par un organisme d'assurance maladie, l'ordonnance prescrivant une spécialité pharmaceutique remboursable aux assurés sociaux²⁵³ doit préciser : la posologie et soit la durée du traitement, soit, lorsque la prescription comporte la dénomination du médicament, le nombre d'unités de conditionnement²⁵⁴.

Le circuit matérialisé de l'ordonnance fut profondément bouleversé ces derniers mois avec la numérisation des ordonnances par les pharmaciens en vue de les transmettre par voie électronique à l'assurance maladie sous forme de pièces justificatives numériques. L'image numérique de l'ordonnance est associée aux données de facturation correspondantes (ticket vitale) sous forme d'un fichier au format PDF télétransmis de manière sécurisée au format SMTP S/MIME vers les frontaux de facturation de l'assurance maladie.

Ce système a récemment permis de franchir un pas décisif dans la dématérialisation des échanges avec l'assurance maladie dont l'élan fut récemment nourri d'une volonté claire de dématérialiser l'ordonnance à sa source par la dernière convention pharmaceutique. Les avantages de la numérisation de l'ordonnance à l'officine ne se limitent cependant pas aux échanges avec l'assurance maladie. L'ordonnance numérisée associée aux données de facturations est sauvegardée dans le système informatique officinal et peut permettre aux pharmaciens de réaliser un contrôle *a posteriori* des produits dispensés et facturés au regard de la prescription originale, à la recherche d'éventuelles erreurs de délivrance.

²⁵³ La liste des spécialités pharmaceutiques remboursables est prévue par l'article L.162-17 du code de la sécurité sociale.

²⁵⁴ Article R.5123-1 du code de la santé publique.

B.3.1.3.c Support d'information pour les patients

L'ordonnance restituée au patient constitue la « notice » lui permettant de suivre la stratégie thérapeutique élaborée par le prescripteur enrichie de ses éventuels conseils et de ceux du pharmacien. Il est intéressant de constater dans ce domaine, que la rédaction et l'impression d'ordonnances par les prescripteurs via les logiciels d'aide à la prescription a largement permis de faciliter la lecture et la compréhension de leur contenu par les patients (et les pharmaciens) qui n'ont plus à réaliser un déchiffrement parfois périlleux, de l'écriture manuscrite du médecin.

Par ailleurs, à la fin de la dispensation de toute ordonnance, le pharmacien appose le cachet de l'officine puis imprime sur l'ordonnance qu'il restitue au patient, les informations lui garantissant une bonne information sur le coût des produits de santé qui lui sont délivrés avec le montant de la somme effectivement payée par l'assuré²⁵⁵, le timbre de l'officine, le ou les numéros de registres, la date d'exécution ainsi que les quantités délivrées²⁵⁶. On parle de « ticket vitale patient »

Pourtant précieux, les conseils pharmaceutiques sont le plus souvent dispensés aux patients de manière orale ne laissant ainsi aucune trace pour le patient. En optimisant les rôles d'un plan thérapeutique délivré lors de chaque dispensation d'une e-prescription, il apparaîtrait possible d'améliorer la qualité et la pertinence des informations que le patient conservera avec lui tout au long de son traitement.

Un système d'e-prescription ne se résume cependant pas à une simple transmission électronique d'ordonnances. La panoplie d'outils intégrée à un tel système pourrait permettre, comme nous le verrons, de faciliter les échanges entre professionnels dans un contexte où la loi HPST tend à promouvoir une meilleure coopération entre eux.



Figure 30 : La pharmacie d'officine au cœur du circuit de l'ordonnance.

²⁵⁵ Article L.162-36 du code de la sécurité sociale.

²⁵⁶ Article R.5125-53 du code de la santé publique.

B.3.2. ETAT DES LIEUX DU DEPLOIEMENT DE L'E-PRESCRIPTION EN EUROPE

Afin de réaliser un véritable état des lieux des différentes stratégies régionales et nationales en matière d'e-santé entreprises en Europe, la Commission européenne a mandaté un groupe d'experts chargé d'évaluer l'évolution de certains indicateurs en rapport avec l'e-santé (*e-health strategies*²⁵⁷). L'équipe de travail a ainsi publié en janvier 2011 les comptes rendus offrant un aperçu du développement de l'e-santé de chacun des 27 pays de l'Union européenne, chapeautés d'un rapport général. Des projets de mise en œuvre d'un système d'e-prescription sont ainsi prévus par 22 des 27 membres dont 4 sont d'ores et déjà fonctionnels à l'échelle nationale au Danemark, en Estonie, en Islande et en Suède (112).

En marge de ces différentes initiatives, le projet **epSOS** (*smart open services for european patients*) lancé en 2008 vise à définir les orientations stratégiques à suivre pour déployer un système d'e-santé comprenant un service d'e-prescription développé dans un cadre d'interopérabilité à l'échelle européenne.

B.3.2.1 PLACE DE LA FRANCE DANS LA COURSE EUROPEENNE A L'E-SANTE

La réussite des politiques d'e-santé de certains pays européens est avant tout liée à leur bonne anticipation des principales contraintes techniques et juridiques que supposent de tels systèmes d'information. En développant le DMP au début des années 2000, l'ASIP Santé avait pourtant bien emboîté le pas de la marche européenne vers la dématérialisation des dossiers médicaux en ligne ou *electronic health record (EHR)* ou encore *patient summary* utilisés au quotidien dans sept pays de l'Union européenne (112). Les contraintes techniques conjuguées au faible engouement et la méconnaissance du DMP par les médecins et les patients ont cependant bloqué l'épanouissement de ce projet pendant de nombreuses années. L'ordre des pharmaciens n'a ainsi pas attendu l'ASIP Santé pour concevoir son propre outil d'e-dispensation : le dossier pharmaceutique, dont le succès grandissant ne peut aujourd'hui être contesté.

L'introduction d'un module d'e-prescription au DMP comme il était initialement prévu pourrait donc constituer une belle opportunité pour l'ASIP Santé d'offrir le succès tant attendu que son outil mérite. Il s'agirait ainsi d'établir une véritable **passerelle électronique** entre professionnels de santé permettant de valoriser par ailleurs l'efficacité et l'adaptabilité du dossier pharmaceutique dont il est difficile de douter tant l'ordre s'est efforcé de développer un outil performant en considérant de larges contraintes d'interopérabilité.

En permettant aux prescripteurs et aux pharmaciens d'utiliser un module d'e-prescription en étroite relation avec le DMP et le dossier pharmaceutique, il serait ainsi possible de franchir le cap décisif et tant attendu de l'unification des dispositifs existants. L'étude des différents modèles d'e-santé opérationnels en Europe permet d'ailleurs de constater que l'efficacité d'un tel système repose sur la cohésion et l'interopérabilité entre les systèmes destinés à l'usage des prescripteurs, des pharmaciens, voire des patients.

Dans la continuité de la numérisation des ordonnances par les pharmaciens, il apparaît donc désormais nécessaire de poursuivre les efforts fournis en dématérialisant l'ordonnance à la source, chez les prescripteurs. La prescription électronique n'est pourtant pas une nouveauté en tant que telle puisque les médecins rédigent leurs ordonnances sur leur ordinateur, via leur logiciel d'aide à la prescription depuis déjà quelques années. Les efforts doivent donc porter sur le mode de transmission de l'ordonnance entre le prescripteur et le pharmacien exécutant.

²⁵⁷ <http://www.ehealth-strategies.eu/>

Si seulement quatre pays de l'Union proposent un système d'e-prescription complet depuis quelques années, neuf des vingt-sept pays concernés par l'étude *e-Health Strategies* en 2010 proposent d'ores et déjà un service de transmission électronique de prescriptions (112).

B.3.2.2 LES CLES DU SUCCES DES POLITIQUES D'E-SANTE ETRANGERES

Les différents systèmes européens d'e-prescription actuellement opérationnels doivent servir d'exemples, sinon d'inspirations pour finaliser notre modèle d'e-santé. L'étude *e-Health Strategies* se base notamment sur l'évaluation de certains critères permettant d'apprécier le développement de l'e-santé dans chaque pays de l'Union européenne et de mettre en avant les principales difficultés rencontrées.

Il apparait ainsi que le succès d'une politique d'e-santé dépend avant tout de **critères démographiques**. En effet, le coût de l'infrastructure matérielle et la complexité de sa gestion sont moins élevés pour les pays de faible population tels que l'Islande (319 000 habitants), l'Estonie (1,34 millions d'habitants), le Danemark (5,57 millions d'habitants) et la Suède (9,45 millions d'habitants), véritables leaders européens en matière d'e-santé.

Les dispositifs d'e-prescription opérationnels à l'échelle régionale en Andalousie ou dans certaines régions des Pays-Bas rencontrent d'ailleurs un véritable succès et servent actuellement de socle pour le développement de ces systèmes à l'échelle nationale.

Mis en œuvre depuis 2000 dans la région d'Andalousie (environ 8 millions d'habitants) en Espagne, le système ***Diraya*** est l'exemple typique de modèle réussi d'e-santé à **l'échelle régionale**. Ce système permet de rendre disponible toutes les informations de santé de chaque usager à l'endroit et au moment nécessaire pour le soigner. Aujourd'hui utilisé par 1 500 centres de santé, 29 centres hospitaliers et 102 000 professionnels de santé, son principe repose sur un **dossier de santé électronique** nommé « *historia de salud* » qui répertorie les données administratives et de santé du patient : situation familiale, séjours en établissements, problèmes de santé, traitements suivis, analyses réalisées, mais aussi antécédents médicaux, allergies... Ces dossiers très complets permettent en outre de récolter des données épidémiologiques, sur le taux de diabétiques ou la propagation d'un virus par exemple, à une échelle impossible à atteindre auparavant. Ces données permettent, par la suite, d'identifier, de répondre plus rapidement et finalement de freiner la propagation des épidémies (113).

Sur cette colonne vertébrale se greffent différentes applications au service des patients et des professionnels de santé parmi lesquelles :

- le service « ***Recetta XXI*** » service d'e-prescription qui permet d'établir des ordonnances informatiques transmises directement du médecin à la pharmacie via une plateforme d'échange également utilisée pour le suivi du traitement ;

- le service « ***Citaci3n*** » permettant aux patients de prendre rendez-vous avec un médecin directement par internet. Ce service peut être par exemple mis en œuvre par des établissements de santé afin de faciliter le relais avec la médecine de ville. Il permet ainsi de fluidifier l'accès aux divers centres de soins en évitant les mauvaises orientations ;

- le service « ***InterS@S*** », est un bureau virtuel du système de santé publique sur internet permettant aux usagers d'intervenir directement dans leur parcours de soins. A travers un accès sur le web, les patients peuvent effectuer des opérations de gestion comme changer de

médecin traitant ou solliciter un second avis médical. Il permet également de planifier des pré-consultations à distance par internet (113).

Dans cette région, 1500 centres utilisaient l'ordonnance électronique, couvrant 93,5% de la population en 2010. Plus de 140 millions d'ordonnances avaient été produites à cette date. De janvier à septembre 2011, 18 millions de rendez-vous ont été pris par un moyen télématique (téléphone, internet, SMS) avec des médecins généralistes (40,5%). En novembre 2011, 1 149 centres de soins utilisent le dossier médical de *Diraya*.

B.3.2.2.a Le statut juridique de la signature électronique

Assurer la confidentialité et l'intégrité des données électroniques transmises entre deux entités authentifiées est un enjeu majeur de tout système d'e-santé. Comme nous l'avons vu, une carte de professionnel de santé telle que la carte CPS française dotée de certificats électroniques d'authentification et de signature, permet de répondre aux exigences de sécurité qu'imposent la transmission électronique de données de santé. Cependant, la valeur juridique de la signature électronique ainsi que les moyens employés pour sa mise en œuvre peuvent différer selon les pays au sein de l'Union.

La directive européenne 1999/93/CE du 13 décembre 1999 relative au statut de la signature électronique visant à en « *faciliter l'utilisation et contribuer à leur reconnaissance juridique* » doit ainsi être transposée en droit national afin de garantir une reconnaissance juridique de la signature et des services de certification. Tous se sont dotés de cadres juridiques pour les signatures électroniques, mais leur disparité rend, de ce fait, les transactions électroniques internationales impossibles. La Commission européenne souhaite d'ailleurs actuellement poursuivre l'harmonisation du statut juridique de la signature électronique dans les différents pays de l'Union afin de développer un cadre d'interopérabilité en faveur d'échanges transfrontaliers²⁵⁸.

En utilisant des cartes à puces électroniques permettant la mise en œuvre d'une signature électronique dite « avancée » reposant sur l'utilisation de certificats électroniques, tout système d'e-santé doit ainsi être doté d'une puissante infrastructure de gestion de clés cryptographiques associées, à l'image de l'ASIP Santé en France. A l'aide d'une telle signature sécurisée, les prescripteurs peuvent assurer leur authentification ainsi que l'intégrité et la confidentialité de données transmises par le biais des systèmes d'information de santé.

B.3.2.2.b Le respect des droits des patients

Le caractère hautement confidentiel des données de santé traitées par les systèmes d'information de santé impose, comme nous l'avons vu, un cadre juridique précis permettant de renforcer les droits des patients au regard du traitement de leurs données personnelles. Tout pays bénéficiant d'un système d'e-santé performant doit donc être capable de répondre aux exigences des patients pour le respect de leurs droits fondamentaux et créer ainsi un climat de confiance en faveur de la généralisation de l'utilisation de ces systèmes.

C'est la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, qui définit les grandes orientations que chaque Etat membre doit suivre et transposer en droit national. Dans ce domaine, la CNIL

²⁵⁸ Communiqué de presse de la Commission Européenne du 4 juin 2012, « Stratégie numérique: un nouveau règlement va donner une dimension transnationale aux signatures électroniques et permettre de tirer un meilleur parti de l'identification électronique dans le marché unique du numérique. »

place la France en très bonne position puisque le cadre juridique du traitement automatisé de données personnelles est parfaitement défini, permettant notamment l'usage du dossier pharmaceutique et du DMP dans le respect des droits des patients énoncés par la loi informatique et libertés et le code de la santé publique.

L'e-prescription n'a de raison d'être que si elle améliore la qualité des soins au bénéfice du patient sans pour autant porter atteinte à ses droits fondamentaux. Ainsi, la **confidentialité des données** de l'ordonnance et la **liberté de choix du médecin et de la pharmacie** en charge de l'exécution de la prescription, doivent être préservées à tout prix.

L'étude *e-Health Strategies* met ainsi en évidence les différentes lois relatives aux droits des patients dans le cadre de l'usage des systèmes informatisés en santé, pour chaque pays de l'Union en précisant certaines spécificités relatives à l'usage des dossiers médicaux en ligne et de l'e-prescription. Les principaux points d'attention retenus portent sur :

- Le consentement du patient ;
- La possibilité de définir différents niveaux d'accès aux données selon la catégorie du professionnel de santé (en particulier pour les pathologies psychiatriques) ;
- Le droit d'interdire l'accès au dossier à certains professionnels de santé ;
- La possibilité pour le patient de prendre connaissance du contenu des données traitées soit en lui remettant une copie papier (comme pour le dossier pharmaceutique) ou en autorisant un accès autonome du patient aux données en ligne. Cet accès peut être sécurisé par l'utilisation de cartes à puce dotées de certificats électroniques ou par un couple identifiant / mot de passe ;
- Le droit de s'opposer à ce que certaines informations figurent dans un tel dossier.

Un système d'e-prescription doit en outre se conformer aux exigences spécifiques qu'impose la dématérialisation de l'ordonnance. Il s'avère ainsi nécessaire de proposer un substitut à l'ordonnance permettant au patient de prendre connaissance du contenu de la prescription mais aussi du montant de la facture tout en considérant certaines obligations spécifiques à certains pays comme la nécessité de procéder à un examen clinique avant toute prescription en France.

B.3.2.2.c Le développement d'une infrastructure adaptée

Tout système d'information fait appel à de nombreux outils informatiques permettant le stockage, la transmission et la protection des données traitées. Comme nous l'avons vu, **les cartes à puce électronique** distribuées aux professionnels de santé utilisent des mécanismes cryptographiques reposant sur l'emploi de certificats électroniques permettant de sécuriser l'utilisation des outils d'e-santé.

Les cartes à puces distribuées aux bénéficiaires de l'assurance maladie sont quant à elles vouées à assumer des fonctions variables selon les pays. En Estonie, plus de 800 000 cartes nationales d'identité électroniques utilisées par les systèmes d'information en santé ont été distribuées depuis 2002 aux citoyens. Cette carte, valide pendant dix ans, est dotée de certificats d'authentification et de signature électroniques permettant à tout citoyen de justifier son identité, de s'authentifier auprès d'un portail web d'administration électronique, mais encore de voyager au travers de l'Union européenne (114).

Comme nous l'avons vu, le critère démographique est un argument de poids dans le choix des orientations stratégiques à mettre en œuvre dans le cadre du développement de toute politique d'e-santé puisque le nombre d'assurés conditionne l'ampleur de l'infrastructure technique à mettre en œuvre. Il est ainsi possible de mieux comprendre pourquoi la mise en œuvre d'une infrastructure de gestion de clés cryptographiques garante de l'attribution de certificats électroniques à chaque assuré fut réalisée sans encombre dans les pays leaders en matière d'e-santé. Le coût de développement d'une éventuelle carte nationale d'identité électronique (CNle) fût d'ailleurs l'argument principal évoqué par Monsieur Manuel Valls, ministre de l'intérieur, lors de l'abandon de ce projet évalué à 85 millions d'euros par an²⁵⁹.

L'Allemagne, peuplée de 82 millions d'habitants, est un exemple frappant de la **difficulté de mettre en place des projets de e-santé à l'échelle nationale dans des pays à forte population** et dotés de systèmes de santé que l'histoire a rendus complexes. Depuis Octobre 2011, les patients de certaines régions pilotes expérimentent une nouvelle carte électronique, *Elektronische Gesundheitskarte*, ou eGK, pour le remboursement de dépenses de santé et leur permettant également d'accéder à leur dossier médical en ligne.

Lancé en 2004, ce projet a connu de nombreux rebondissements et fut mis en suspens suite aux inquiétudes de plusieurs médecins et spécialistes de la sécurité informatique concernant l'accès aux données de santé du patient initialement contenues dans la puce électronique de la carte. Le projet fut donc relancé en allégeant la carte de ses données de santé pour ne laisser que des données d'ordre administratives de sécurité sociale et de mutuelle ainsi que certaines données médicales d'urgence (allergies, intolérances, traitements en cours, information sur le don d'organes et coordonnées du médecin traitant) afin de les rendre disponibles facilement en cas d'accident. Les efforts colossaux fournis (plus d'1,7 milliards d'euros investis) semblent commencer à payer et le déploiement de cette carte électronique à l'échelle nationale est actuellement en bonne voie. Il est intéressant de s'apercevoir que l'Allemagne a opté pour un déploiement régionalisé de ces systèmes en confiant la responsabilité de leur gestion aux caisses d'assurance maladie de chaque *Länder* (115).

L'un des enjeux de doter les patients de certificats électroniques est de leur garantir **un accès autonome à une plateforme en ligne de manière sécurisée**²⁶⁰ afin de pouvoir prendre connaissance du contenu de leurs dossiers mais encore d'effectuer certaines opérations directement en ligne. En véhiculant la quasi-totalité des prescriptions par voie électronique, le système d'e-prescription danois « *Apoteket* », fait actuellement figure de leader européen en la matière. Comme tout système de ce type, il est composé de deux versants : l'un dédié aux prescripteurs (historique des prescriptions), l'autre aux pharmaciens (historique des délivrances), regroupés au travers d'une plateforme unique. Malgré les difficultés techniques initialement rencontrées en raison de la lenteur du réseau, ce système connaissant un véritable succès s'étend désormais vers le secteur hospitalier ainsi qu'au domicile de chaque patient. En effet, chacun peut accéder via internet à une plateforme en ligne lui donnant accès au contenu de son dossier pharmaceutique et lui permettant de commander certains produits à sa pharmacie habituelle.

Cette plateforme accueillant plus de 28.000 visiteurs par semaine permet enfin à tout patient de bénéficier d'informations sur le bon usage des médicaments sous forme de dossiers thématiques rédigés par des pharmaciens et met à leur disposition un module de « consultation en ligne » par messagerie directe (*chat*), e-mail, ou *webcam* (116).

²⁵⁹ Réponse du Ministre de l'intérieur Monsieur Manuel Valls (JORF 1^{er} janvier 2013) de la question au Gouvernement n°4746 du Député Monsieur Philippe Meunier (JORF 18 septembre 2012).

²⁶⁰ Par opposition à une authentification simple à l'aide d'un couple identifiant / mot de passe.

L'élan nécessaire à la généralisation de l'e-santé en Suède fut fourni dès la fin des années 1990, par le déploiement d'une **infrastructure réseau** performante de grande ampleur. Il s'agit d'un vaste réseau privé, sécurisé et performant de fibres optiques distinct du réseau internet, dédié à la transmission électronique des données de santé. Il s'agit d'une différence technique fondamentale en matière d'infrastructure réseau puisqu'un tel type, dit *virtual LAN* (VLAN) est dissocié du réseau internet, beaucoup moins vulnérable que les réseaux de type VPN (*virtual private network*) (117).

Ce système permet aujourd'hui de transmettre 85% des prescriptions par voie électronique en Suède selon deux circuits :

- soit le prescripteur utilise le système de dossier patient médical en ligne (équivalent du DMP) récemment enrichi d'un module d'e-prescription pour transmettre une prescription via le réseau national VLAN ;

- soit le prescripteur utilise un *webservice* d'e-prescription disponible en ligne via le réseau internet.

Cet outil permettait initialement de transmettre une ordonnance par voie électronique directement vers la pharmacie désignée par le patient mais fut enrichi d'un système de dépôt dans une base de données sécurisée (comparable à celle du dossier pharmaceutique) depuis 2004²⁶¹. Ce nouveau système fut accueilli avec enthousiasme par l'ensemble des acteurs et particulièrement les patients en leur offrant une plus grande **flexibilité dans leur choix d'une pharmacie**, la quasi-totalité des officines étant raccordées au dispositif. Les efforts actuellement entrepris pour parfaire la qualité de ce système, visent à optimiser l'intégration et la prise en compte de l'historique des prescriptions et de l'historique des dispensations par les dispositifs destinés aux prescripteurs et aux pharmaciens (112).

Enfin, l'une des contraintes majeures de toute politique d'e-santé consiste en **l'interopérabilité des systèmes** destinés à l'usage des différents acteurs (principalement les patients, les professionnels de santé et les organismes d'assurance maladie). Compte tenu du développement actuel de l'e-santé en Europe, cette contrainte technique majeure d'interopérabilité ne doit pas seulement être envisagée à l'échelle nationale. Les différents standards utilisés par les éditeurs de logiciels d'aide à la prescription et à la dispensation doivent donc garantir une parfaite interopérabilité des différents systèmes et sous-systèmes informatisés à l'échelle internationale. Le rapport de l'organisation *e-Health* datant de janvier 2011 mettait d'ailleurs en évidence une certaine disparité entre les différents pays européens dans le choix des standards utilisés. Si les standards HL7 V2 et HL7 V3 sont les plus couramment employés (15 pays), d'autres sont également rencontrés comme les standards ISO 13606, DICOM (*digital imaging and communication in medicine standards*), LOINC (*logical observation identifiers names and codes*), KMEHR (*kind messages for electronic health record*)... (112).

L'un des modèles d'interopérabilité des systèmes informatisés de santé est représenté par le système « *Digilugu* » en Estonie. Ce pays Balte d'1,5 million d'habitants, leader en matière d'e-administration, est l'un des modèles européens d'e-santé les plus aboutis. La moitié de la population nationale dispose ainsi d'un dossier patient informatisé ou « *Digilugu* » accessible en ligne via un portail internet.

²⁶¹ D'un point de vue technique, ce système utilise la classification *SIL* (*Svensk Informationsdatabas för Läkemedel*) des médicaments déjà reconnue par 21 pays membres de l'Union, en utilisant le standard ENV 13607 et d'autres tels que HL7 v3 (117).

Ce dossier, en lien avec un système d'e-prescription depuis 2010, comprend :

- des comptes rendus d'examens et d'hospitalisation ;
- les résultats d'imageries médicales et leurs comptes rendus ;
- les données administratives de prise en charge par les organismes de sécurité sociale.

Ce succès de la dématérialisation des échanges en Estonie fut longuement et brillamment préparé puisque dès la fin des années 1990. L'Estonie a misé sur le développement d'internet et des services d'e-administration en créant une plateforme d'échange de données à l'échelle nationale permettant de sécuriser les transactions électroniques. Cette plateforme unique intitulée *X-Roads* a également permis de définir les standards informatiques utilisés pour les échanges dématérialisés, dès sa conception, et d'**arriver ainsi très rapidement à un point de convergence des systèmes informatisés**. Plus de 3000 services dématérialisés en lien avec l'e-administration sont aujourd'hui proposés aux citoyens estoniens, de l'e-santé jusqu'au vote aux élections par exemple. Ce succès est tout de même à mettre en étroite relation avec la faible démographie du pays, ainsi que les faibles contraintes d'interopérabilité initiales diminuant le coût de déploiement du dispositif (118).

B.3.2.3 LE PROJET EPSOS : UN TERRAIN FERTILE A L'ECHELLE D'UN CONTINENT

Dans la foulée du déploiement de la carte européenne d'assurance maladie, l'Union européenne a souhaité renforcer l'efficacité et l'interopérabilité des systèmes d'information de santé à l'échelle européenne en lançant le projet **epSOS** (*smart open services for european patients*) en juillet 2008. L'objectif principal de cette initiative consiste en l'évaluation de **l'interopérabilité sémantique** de ces systèmes, c'est-à-dire l'interprétation commune des informations échangées (maladies, traitements...) entre deux systèmes de pays différents. Compte tenu de la mobilité croissante des citoyens au sein de l'Union et de leurs exigences vis-à-vis des systèmes de santé, il devenait urgent de garantir une parfaite interprétation de données de santé partagées par des professionnels exerçant dans des pays différents (119).

Les enjeux de l'interopérabilité des systèmes informatisés de santé entre les pays de l'Union sont multiples (120) :

- faciliter la mobilité des patients et garantir leur sécurité au sein de l'Union ;
- améliorer l'efficacité et la rentabilité des soins transfrontaliers ;
- fournir un service médical sûr et sécurisé dans chaque pays européen.

Actuellement 23 pays participent au projet epSOS (annexes 17 et 18) :

- **12 pays sont présents depuis le 1er juillet 2008** (date de lancement du projet) : Allemagne, Autriche, Danemark, Espagne, France, Grèce, Italie, Pays-Bas, République Tchèque, Royaume-Uni, Slovaquie, Suède ;
- **11 pays supplémentaires depuis le 1er janvier 2011** : Belgique, Estonie, Finlande, Hongrie, Malte, Norvège, Pologne, Portugal, Slovaquie, Suisse et Turquie.

En marge des différentes initiatives régionales et nationales en matière d'e-santé, le projet epSOS propose un outil informatique basé sur deux services transfrontaliers :

- le service « *patient summary* » qui contient un résumé du dossier médical du patient (avec son consentement). Un médecin étranger pourra consulter son *patient summary* traduit dans la langue locale afin de faciliter le diagnostic et le traitement ;

- le service « *e-prescription* » qui n'est pas mis en œuvre en France, permet l'édition de la prescription de médicaments par le prescripteur via un logiciel et sa transmission électronique au pharmacien. L'e-dispensation, second volet de ce service, comprend l'envoi électronique des informations sur les médicaments dispensés par le pharmacien vers le dossier du patient (120).

Pionnière de la mise en place du dispositif d'accès au volet « *patient summary* » avec la République Tchèque, la France n'adhère toujours pas au dispositif d'e-prescription. Seuls la Grèce, l'Espagne, l'Italie, l'Autriche, la Suède et la Finlande ont déployé l'e-prescription, alors que la Norvège est en cours d'intégration au dispositif.

Dans la dynamique de la directive européenne visant à faciliter l'accès aux soins transfrontaliers²⁶², le projet epSOS d'échanges de données de santé est entré dans une phase pilote opérationnelle depuis le 8 mars 2012. Il permet aux professionnels de santé d'accéder, dans leur langue, à des services tels que la synthèse médicale (*patient summary*) ou la prescription électronique (*e-prescription*) d'un patient en séjour à l'étranger. Le budget total du projet est de 36 500 000 euros, dont 50% est financé par l'Union européenne. Les partenaires cofinancent les activités de coordination, ramenant ainsi le financement effectif de l'Union européenne à environ 40% (121).

D'un point de vue technique, chaque pays participant fournit l'infrastructure technique nécessaire au dispositif, soit un hébergeur de données de santé agréé et un responsable du développement des applications informatiques. En France, c'est l'ASIP Santé qui a été désignée par le ministère chargé de la santé comme point de contact national chargé de la mise en œuvre du service epSOS au niveau national et de la prise en compte des exigences juridiques, organisationnelles et techniques du projet. L'hébergement des données de santé a été confié à la société CEGEDIM tandis que la maîtrise d'ouvrage est partagée par l'ASIP Santé avec le Groupement de coopération sanitaire eSanté Alsace qui participait déjà à l'expérimentation du DMP (122).

L'ASIP Santé et le ministère chargé de la santé qui sont en charge du déploiement de ce dispositif travaillent en collaboration avec le programme ERASMUS en permettant aux étudiants des universités de Paris ouest (Nanterre), de Bourgogne (Dijon) et de Strasbourg, d'autoriser l'accès à leur *patient summary* à des médecins étrangers adhérent au projet. Ces universités adhérent au système en France sont qualifiés de « points de santé epSOS ». Réciproquement, les étudiants étrangers reçus dans ces universités françaises bénéficient également de ce système (119).

Concrètement, chaque point de contact national propose un ensemble de service accessible en ligne par les professionnels de santé des pays participants. Par exemple, un patient français voyageant dans un pays de l'Union adhérent au dispositif pourra bénéficier de ce système en

²⁶² Directive 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011 relative à l'application des droits des patients en matière de soins transfrontaliers.

permettant au professionnel de santé sollicité à l'étranger de se connecter au **portail d'accès en ligne**, interface de communication avec le point de contact national.

Après authentification du patient et du professionnel de santé²⁶³ auprès du système, ce dernier peut avoir accès au contenu des informations des dossiers « *patient summary* » et/ou « *e-prescription* » au standard HL7 CDA Release 2.0 dont les données sont traduites et normalisées dans sa langue par mise en correspondance des données avec deux fichiers de données au format Excel :

- epSOS MVC (*master value sets catalogue*) exprimant l'ensemble des standards utilisés par le système (HL7, ATC, LOINC, SNOMED...) ;

- epSOS MTC (*master translation / transcoding catalogue*) permettant de traduire l'ensemble des valeurs du catalogue MVC dans les différentes langues (123).

En soutenant la mobilité des patients au travers de l'Europe, ce système devrait permettre d'améliorer l'efficacité, la sécurité et l'efficience des soins transfrontaliers. Les résultats de l'évaluation de ce projet devraient permettre de définir des recommandations ainsi que des spécifications techniques et fonctionnelles visant à améliorer l'interopérabilité des systèmes à l'échelle européenne (121).

B.3.2.4 LE PROJET EUROPEEN PALANTE

Dans la foulée du projet epSOS, le bureau pour la société de l'information de la Commission Européenne a récemment lancé le projet PALANTE pour « *patient leading and managing their healthcare through ehealth* » qui vise à développer l'information des patients sur leur état de santé et en mesurer l'impact sur la qualité du système de soins dans son ensemble. Comme son nom l'indique, l'un des objectifs de ce projet consiste à centrer les dispositifs d'e-santé sur le patient, en lui autorisant un accès autonome via un portail web comme c'est par exemple le cas au Danemark ou en France avec le DMP.

Mené pendant une durée de trois ans (de février 2012 à fin janvier 2015), ce projet associe au total 21 partenaires répartis dans dix pays différents de l'Union, et concerne une population de près de 70 000 utilisateurs. Il vise à évaluer ce droit de regard et d'action inédit du patient sur son dossier de santé et ainsi connaître son impact réel sur la santé des patients dans ces pays. En France, l'évaluation porte donc sur le système d'« accès web patients » du DMP mis en œuvre par l'ASIP Santé, représentant naturel de la France au sein de ce projet (124).

B.3.3. LES ENJEUX DE L'E-PRESCRIPTION

Comme pour toute démarche de simplification des tâches administratives, la dématérialisation des prescriptions à la source promet de nombreux bénéfices dont certains, spécifiques des systèmes informatisés de santé, doivent contribuer à améliorer la santé publique. Dans son rapport sur l'activité officinale française, l'inspection générale des affaires sociales recommande ainsi de poursuivre les démarches entreprises avec la numérisation des ordonnances par les pharmaciens en promouvant l'e-prescription. Ce rapport envisage de nombreux bénéfices tant sur le plan sanitaire en potentialisant l'intérêt des systèmes existants que sur le plan économique, sans pour autant les énumérer ni estimer le montant des « *importantes* » économies potentielles (110).

²⁶³ Au moyen de leurs données d'identification d'origine.

B.3.3.1 LES ATOUTS ECONOMIQUES ET ECOLOGIQUES D'UNE SIMPLIFICATION ADMINISTRATIVE

Si l'élan de la numérisation des ordonnances par les pharmaciens tend à réduire les dépenses liées à la collecte, au tri, au traitement et à l'archivage des ordonnances papiers par l'assurance maladie²⁶⁴, la dématérialisation totale de l'ordonnance pourrait constituer une source d'économies supplémentaire en poussant l'automatisation des contrôles de lots d'ordonnances toujours plus loin. En normalisant l'expression des données de prescription électronique sur la base de standards connus des différents systèmes informatisés de notre système de santé, il serait possible de développer l'automatisation des contrôles des e-prescriptions et des données de facturation par les organismes d'assurance maladie, devenant ainsi plus nombreux et plus efficaces.

Par ailleurs, une évaluation des bénéfices socio-économiques du système *Diraya* fut réalisée en 2008 par le projet Européen EHR-IMPACT. Cette étude pointe comme bénéfices les plus significatifs une économie de 253,3 millions d'euros grâce à la prescription de médicaments génériques facilitée par le système d'e-prescription ainsi qu'une réduction conséquente des erreurs de prescription (125).

Enfin, les bénéfices écologiques liés à toute démarche de dématérialisation paraissent évidents mais ont parfois du mal à être prouvés. Ils concernent principalement une diminution de la pollution liée à la consommation de papier et d'encre ainsi qu'un mode de transmission moins polluant par voie électronique que par voie postale. L'impact écologique du développement exponentiel des *data centers* paraît cependant non négligeable tant en terme de consommation d'énergie que de rejets de dioxyde de carbone, malgré le développement récent de nouvelles structures permettant notamment d'optimiser leurs rejets calorifiques.

B.3.3.2 LES BENEFICES EN MATIERE DE SANTE PUBLIQUE

L'évaluation du système *Diraya* mené en Andalousie a également permis de mettre en évidence de nombreux bénéfices pour les patients et notamment une **amélioration de la continuité des soins**, une **réduction conséquente des erreurs de prescription** ainsi qu'un **gain de temps significatif accordé au patient**. Par ailleurs, une réduction de plus de 15% des visites chez le médecin généraliste, permet de générer des **réductions de coûts et de temps** de transport pour les patients. Cet outil particulier permet également d'apporter un outil d'étude épidémiologique et statistique performant en ligne (125). Ce gain de temps et d'attention au bénéfice du patient est également mis en avant dans les bénéfices attendus du projet epSOS, mais encore dans les conclusions de plusieurs rapports de l'étude *eHealth Strategies* comme en Estonie où l'e-prescription permet de réduire le temps de rédaction des prescriptions mais surtout le temps de lecture, d'analyse et de traitement des ordonnances (114).

La normalisation de l'expression des données de santé au format électronique est également un élément incontournable pour le développement d'un cadre d'interopérabilité autour des systèmes existant. Le dossier pharmaceutique, outil d'e-dispensation, permet d'ores et déjà de réaliser une recherche d'incompatibilités entre plusieurs dispensations. En permettant aux différentes catégories de prescripteurs de prendre connaissance d'autres traitements prescrits, au moment de la rédaction de l'ordonnance, il est possible d'envisager une diminution de l'incidence des erreurs de prescriptions (allergies, contre-indications, interactions entre

²⁶⁴ Le coût annuel de la collecte des ordonnances papier par l'assurance maladie auprès des pharmacies est estimé à 4 millions d'euros tandis que le coût lié à la photocopie d'ordonnances non dupliquées est évalué à 3 millions d'euros par an (23).

médicaments, dosage incorrect par rapport au poids et à l'âge...), et contribuer à limiter les phénomènes de surconsommation de médicaments. Dans ce domaine, les conclusions des différents rapports d'évaluation des bénéfices tirés de l'e-prescription sont variables. Par exemple, une étude menée dans deux hôpitaux australiens a ainsi mis en évidence une réduction des erreurs de prescription de plus de 50 % dont les plus graves ont été réduites de 44%²⁶⁵.

En revanche, le journal de l'association américaine d'information médicale du groupe BMJ a publié un rapport sur la fréquence, les types et les causes d'erreurs liées aux prescriptions électroniques, dans le cadre des soins ambulatoires, aux Etats-Unis. Cette étude de cohorte rétrospective menée par une équipe du *Massachusetts general hospital* de Boston porte sur 3 850 ordonnances générées informatiquement et télétransmises vers une chaîne de pharmacies de trois Etats des Etats-Unis. L'objectif de cette étude était de déterminer, pour ce système, l'incidence des erreurs de prescription, les effets indésirables des médicaments prescrits, le potentiel de dommages et le taux d'erreurs de prescription par type d'erreur. Sur les 3 850 prescriptions, 452 (11,7%) contenaient 466 erreurs au total, dont 163 (35,0%) pouvaient être considérées comme responsables d'effets indésirables. Cette étude n'a donc pas permis de mettre en avant l'amélioration de la sécurité des prescriptions puisque le taux d'erreurs constaté sur les ordonnances électronique (11,7%), est comparable à celui des ordonnances manuelles.

Enfin, l'e-prescription permet au patient de ne plus craindre de perdre ou oublier ses ordonnances et lui permet même de renouveler une dispensation directement en ligne comme au Danemark (112).

Si ce système facilite ainsi le processus de prescription, il lui reste donc encore à prouver son véritable apport en matière de santé publique, mais tout laisse à penser que son efficacité sera prouvée progressivement au cours des années à venir. En effet, les progrès réalisés dans la conception des logiciels professionnels couplés à l'adhésion grandissante des différents partenaires à ce dispositif devraient permettre d'en généraliser l'utilisation par l'ensemble du corps médical très rapidement.

B.3.3.3 FAVORISER LA COOPERATION ENTRE PROFESSIONNELS DE SANTE

Comme pour toute évolution des systèmes informatisés de santé, l'adhésion des professionnels à un nouvel outil dépend avant tout de sa facilité d'utilisation. En optimisant l'utilisation d'un dispositif d'e-prescription, tout professionnel de santé peut tirer de nombreux bénéfices de cet outil. Indépendamment de son mode de transmission, l'ordonnance élaborée au moyen d'outils informatiques offre avant tout un confort de lecture optimal pour les pharmaciens qui n'ont plus à déchiffrer certaines ordonnances manuscrites.

L'e-prescription, permettant une transmission électronique des ordonnances, constitue un véritable outil de coopération interdisciplinaire dont l'utilisation repose sur l'hébergement de l'historique des prescriptions sur un serveur dont l'accès est sécurisé. Il doit permettre de réaliser un suivi actualisé en ligne du statut de délivrance de la prescription par une mise à jour du statut d'exécution de la prescription (entièrement exécutée, partiellement exécutée, à renouveler...). En intégrant l'outil de messagerie sécurisée de santé (MSSanté) en cours de

²⁶⁵ Plus de 50% d'erreurs de prescriptions en moins avec l'informatisation des prescriptions dans des hôpitaux, .Agence de presse médicale (APM), 2 février 2012.

développement, un système d'e-prescription pourrait valoriser les efforts fournis par l'ASIP Santé et garantir une communication efficace entre professionnels de santé.

Ce système pourrait également promettre un gain de temps considérable pour les pharmaciens qui seraient aidés dans leur choix de renouveler ou non un traitement, ligne par ligne, réduisant certains risques d'erreurs de dispensation. En y intégrant les nouvelles missions du pharmacien correspondant prévues par la loi HPST²⁶⁶, un service d'e-prescription pourrait ainsi permettre au pharmacien de procéder facilement au renouvellement d'une ordonnance ou à une éventuelle adaptation posologique. **Il s'agirait ainsi de doter les pharmaciens de l'outil indispensable à la réalisation de ses nouvelles missions en faveur d'une meilleure coopération entre professionnels de santé.**

Enfin, en « shuntant » le patient comme intermédiaire de transmission des ordonnances, les pharmaciens n'auraient plus à se soucier d'une éventuelle falsification de la prescription.

B.3.4. COMMENT DEPLOYER L'E-PRESCRIPTION EN FRANCE ?

L'e-prescription devrait sans aucun doute constituer un tournant majeur pour notre système de santé au cours de la prochaine décennie en modifiant les habitudes d'exercice des professionnels de santé ainsi que la perception de l'ordonnance par les patients. Introduire un tel système dans notre paysage d'e-santé ne présente cependant un intérêt que s'il améliore les pratiques professionnelles, au bénéfice de la santé publique. Les contraintes techniques et juridiques permettant le développement d'un tel projet restent cependant surmontables pour l'ASIP Santé, la Caisse nationale d'assurance maladie et les ordres de professionnels de santé comme en atteste le développement des téléservices existants.

Face à la méfiance des patients et des professionnels de santé envers ces systèmes, définir les droits et les devoirs de chacun permet de bâtir les fondements d'un environnement de confiance. La convergence des dispositifs existants vers un système unique d'e-santé incluant notamment le DMP, le dossier pharmaceutique, la MSSanté et l'e-prescription serait une occasion de clarifier et uniformiser pour ces différents dispositifs :

- les modalités de déclaration de traitement automatisé de données personnelles auprès de la CNIL par les professionnels de santé ;
- l'expression et le recueil du consentement du patient ;
- l'information des patients sur l'e-santé ;
- les droits des patients au regard du traitement de leurs données.

Sans sous-estimer la complexité de mise en œuvre d'un tel projet et la difficulté de gagner l'adhésion des professionnels de santé, le développement d'un tel outil doit en permettre une intégration parfaite dans leur exercice quotidien. Il doit à la fois préserver leur indépendance et leur liberté de jugement tout en améliorant la qualité, la sécurité et l'efficacité de la prescription et de la dispensation de produits de santé.

²⁶⁶ Loi n° 2009-879 du 21 juillet 2009 portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires.

B.3.4.1 EN ANTICIPANT LES BESOINS D'INTEROPERABILITE

Afin d'intégrer cette nouvelle pièce au puzzle de l'e-santé français, il est également nécessaire d'avoir un aperçu global du développement des systèmes d'information de santé en France et à l'échelle européenne. Le développement d'un système d'e-prescription doit ainsi tenir compte de l'ensemble des dispositifs existants ainsi que des différentes orientations stratégiques en matière d'e-santé afin d'assurer un cadre d'interopérabilité sans faille entre les systèmes. Le développement de l'e-prescription en France est un véritable défi technique dont la contrainte principale d'**interopérabilité** des systèmes doit prendre en compte le développement anarchique de l'informatisation des données des patients. En effet, le DMP qui devait initialement permettre la transmission de prescriptions au format électronique est actuellement largement dépassé par le succès du dossier pharmaceutique développé par l'ordre des pharmaciens.

Pour se conformer aux habitudes et aux règles de prescription actuelles, la conception d'un système d'e-prescription doit donc prendre en compte les différents types d'ordonnances utilisées. Toute prescription électronique transmise via un système d'e-prescription étant sécurisée, il deviendrait donc superflu de distinguer une ordonnance « simple » d'une ordonnance « sécurisée » comme il est d'usage pour leurs versions papiers. Cependant, la possibilité de bénéficier d'autres modèles d'ordonnances doit permettre de considérer les prescriptions dans le cadre d'une affection de longue durée ou d'un médicament d'exception.

B.3.4.1.a L'interopérabilité sémantique

L'e-prescription étant un outil dont l'utilisation est partagée par plusieurs catégories de professionnels de santé, les contraintes d'interopérabilité rencontrées dans son développement sont donc complexes. Il s'agit en effet de répondre aux exigences des différents niveaux d'interopérabilité entre les systèmes destinés aux prescripteurs et aux pharmaciens en intégrant un besoin fort pour les systèmes d'information impliquant le médicament : la normalisation des informations liée à la prescription.

Lors de ses travaux menés sur les procédures de certification des logiciels d'aide à la prescription, la Haute Autorité de santé a mis en évidence la nécessité de faire évoluer et uniformiser les différentes codifications et nomenclatures actuellement utilisées pour identifier les produits de santé, comme c'est par exemple le cas en Grande-Bretagne et aux Pays-Bas. Il apparaît en effet nécessaire que les différents systèmes d'information de santé mentionnant un médicament les identifie de la même manière, qu'il s'agisse des logiciels métiers, mais encore, de dossiers médicaux en lignes. La Haute Autorité de santé a d'ailleurs souligné dans un rapport d'analyse des accidents en rapport avec des systèmes informatiques de prescription que ce défaut de normalisation pouvait être à l'origine d'accidents parfois graves (126).

Le développement d'un outil d'e-prescription n'est donc possible que si les données renseignées par le médecin via son logiciel d'aide à la prescription sont parfaitement interopérables, particulièrement d'un point de vue **sémantique**, avec le système automatisé d'e-prescription, le logiciel d'aide à la dispensation du pharmacien et les services web existants (particulièrement le DMP et le dossier pharmaceutique).

Si le recueil des informations administratives nécessaire à l'établissement ou à la dispensation d'une prescription est facilement automatisable (via les logiciels métiers, la carte Vitale et la carte CPS), l'expression de la stratégie thérapeutique adoptée demeure en revanche variable d'un prescripteur à l'autre.

La normalisation de l'expression des données de prescription doit ainsi en faciliter le traitement automatisé au sein des systèmes d'information de santé.

Cette évolution concerne :

- **La normalisation des données d'identification de la spécialité prescrite.** Sans porter atteinte à leur liberté de prescription, il apparaîtrait judicieux de permettre aux médecins de sélectionner ces informations parmi une liste de données normalisées. Conformément aux exigences du référentiel de certification des logiciels d'aide à la prescription, l'ordonnance établit au format électronique doit générer chaque ligne de prescription en identifiant les médicaments par leur DCI ²⁶⁷ et/ou en traduisant le nom commercial de spécialités pharmaceutiques en DCI. En certifiant les logiciels d'aide à la prescription et d'aide à la dispensation, la Haute Autorité de santé s'inscrit dans une démarche de normalisation des données d'identification des produits de santé dont l'enjeu majeur consiste à associer sans ambiguïté une substance active prescrite sous sa dénomination commune à une boîte précise, effectivement dispensée à l'officine. L'intérêt est majeur puisque les prescripteurs, s'intéressent avant tout à la prescription d'une substance active tandis que les pharmaciens qui sélectionnent la boîte de médicament délivrée se soucient également de la référence spécifique du produit : le code CIP puisqu'il s'agit de l'identifiant actuellement utilisé pour la facturation des médicaments. Les enjeux de l'évolution des données d'identification des produits de santé pourraient donc être colossaux tant sur le plan économique qu'en santé publique. Afin de préserver l'interopérabilité des systèmes informatisés de santé et particulièrement ceux impliqués dans le circuit du médicament, il apparaît donc incontournable d'assurer une continuité dans l'expression des données des produits de santé prescrits et effectivement dispensés.

- **La normalisation des informations relatives aux modalités de suivi du traitement** et particulièrement la durée et la posologie définie par le nombre d'unités de prise, le nombre de prises et leur fréquence (par exemple un comprimé trois fois par jour ou une gélule une fois tous les sept jours...). Il est en revanche possible de s'affranchir de la normalisation de l'expression d'un éventuel événement déclencheur comme « au cours d'un repas », « au coucher », ou encore « si douleur... ». Compte-tenu de l'hétérogénéité de ces informations, il apparaît souhaitable que celles-ci soient saisies et traitées en tant que « texte libre » dont le contenu est inséré dans la ligne de prescription.

- **La normalisation de mentions particulières** relatives à une ligne de prescription comme « Non substituable », « A renouveler X fois », « Hors AMM », « A délivrer en une fois », « A délivrer en X fractions », « A délivrer par la Pharmacie X »...

B.3.4.1.b Interopérabilités syntaxique et technique

Afin de s'intégrer parfaitement dans le panel des systèmes d'information de santé, tout nouveau système de traitement automatisé de données doit savoir interpréter les différentes syntaxes couramment utilisées. Le cadre d'interopérabilité des systèmes d'information de santé (CI-SIS) élaboré par l'ASIP Santé constitue le référentiel permettant de définir les normes, les standards et certaines spécifications utilisés. La version 3 du standard HL7 (HL7 V3), LOINC (*logical observation identifiers names and codes*,) ainsi qu'une implémentation d'HL7 intitulée NCPDP²⁶⁸ (HL7-NCPDP) sont les standards principalement utilisés par les systèmes d'e-prescription actuellement opérationnels et pourraient ainsi être utilisés en vue de

²⁶⁷ Dénomination commune internationale.

²⁶⁸ En référence au *National council for prescription drug program*.

la conception d'un tel système en France, en toute interopérabilité avec le dossier pharmaceutique et le DMP basés sur la même famille de standards. Ce cadre d'interopérabilité doit également intégrer l'ensemble des acteurs des systèmes d'information de santé, et notamment les systèmes informatisés des patients (navigateurs internet) lorsqu'un accès au système de manière autonome leur est autorisé, ainsi que ceux des télé-services et des systèmes informatisés des opérateurs sectoriels (annuaire RPPS, portail IMARS de l'assurance maladie...).

D'un point de vue technique, il pourrait s'agir d'un service web s'appuyant sur une base de données Oracle et des serveurs de type Apache, à l'image du dossier pharmaceutique. Concrètement, une fois la prescription rédigée et mise en page, le médecin établit une connexion sécurisée (HTTPS) avec le serveur au moyen de son certificat d'authentification (associé à sa carte CPS) et du certificat serveur de type SSL. Le patient est identifié auprès du système par le calcul de son INS-C²⁶⁹ à partir des informations lues dans sa carte Vitale. Le médecin autorise la transmission de la prescription vers le serveur et le dossier « e-prescription » relatif à ce patient est ainsi incrémenté d'une nouvelle ordonnance numérique, enregistrée dans la base de données. L'opération inverse permettant aux pharmaciens d'accéder à ce dossier et de mettre à jour le statut de délivrance de la prescription, est réalisé dans les mêmes conditions de sécurité.

B.3.4.2 EN CONCEVANT UN OUTIL ADAPTE AUX BESOINS ET AUX INFRASTRUCTURES

Afin de faciliter l'adhésion des professionnels de santé à un tel dispositif, il est impératif de développer une interface adaptée à leur exercice quotidien. Lors d'une consultation médicale, le médecin procède à l'identification de son patient dans son système informatique afin d'accéder à son dossier électronique et éventuellement à son « web-médecin » ou son dossier médical personnel par l'utilisation simultanée des cartes Vitale et CPS. Après examen du patient, il établit une prescription sur son ordinateur au moyen de son logiciel d'aide à la prescription certifié en renseignant l'ensemble des données suffisantes pour en assurer la licéité, la qualité et le traitement automatisé.

Lorsqu'il rédige une prescription à l'aide de son logiciel, le prescripteur choisit le type d'ordonnance sécurisée qu'il souhaite établir (simple, d'affection de longue durée, d'exception). Comme toute ordonnance, l'e-prescription doit d'abord renseigner l'ensemble des informations relatives au prescripteur (nom, prénom, qualité, n° RPPS, coordonnées), relatives au patient (nom, prénom, INS, sexe, âge, poids et taille) ainsi que la date de prescription. Il vérifie que les informations de l'ordonnance automatiquement remontées par le progiciel sont exactes puis crée une nouvelle ligne de prescription. Il sélectionne la DCI (ou le *princeps* assorti de sa DCI) enrichie du dosage et de la forme pharmaceutique, par exemple PARACETAMOL 1000MG CP.

Selon la forme pharmaceutique, le logiciel suggère la voie d'administration adaptée et le médecin précise ensuite la posologie selon des critères normalisés intégrant le nombre d'unités de chaque prise, le nombre de prises et leur fréquence, un éventuel évènement déclencheur de la prise et la durée totale du traitement. Le prescripteur peut également préciser certaines mentions complémentaires définies dans le cadre d'interopérabilité sémantique pour chaque ligne de prescription, permettant d'en signifier les mentions « A renouveler », « Non substituable » ou « Hors AMM » par exemple.

²⁶⁹ Dans l'attente de la mise à disposition de l'INS-A.

A la fin de la rédaction d'une prescription, l'ensemble des données générées lors de la consultation sont enregistrées dans le dossier patient informatisé du logiciel qui lui propose ensuite d'imprimer l'ordonnance ou bien de la transmettre par voie électronique vers le serveur distant d'un hébergeur agréé de données de santé, dédié aux e-prescriptions. En accédant à la base de données de façon sécurisée au moyen de sa carte CPS, le médecin peut y déposer une nouvelle prescription, consulter l'historique des prescriptions du patient, chercher et consulter une prescription antérieure. Pour cela, il doit pouvoir accéder à tout moment au dossier d'e-prescriptions de son patient par calcul de son identifiant national de santé (INS-A ou INS-C). L'hébergement des prescriptions électroniques sur un serveur distant constitue un élément fondamental de tout système d'e-prescription puisqu'il permet au patient de choisir librement et à tout moment la pharmacie dont il souhaite solliciter les services²⁷⁰.

Chaque nouvelle e-prescription alimentant la base de données serait identifiée au moyen d'un numéro unique qui pourrait par exemple être bâti selon un modèle à 22 chiffres consistant en l'assemblage de la date de prescription (8 chiffres), du numéro RPPS du prescripteur (11 chiffres) suivi d'un numéro à 3 chiffres incrémenté à chaque prescription. Le tableau 23 permet d'illustrer un exemple du contenu d'une prescription électronique de médicaments dans le cadre d'une affection de longue durée.

PRESCRIPTION #0206201318308473648001				
PRESCRIPTEUR				
IDENTIFICATION		DUPONT Jean (18308473648)		
QUALITE		Médecine générale		
COORDONNEES		12 rue des arts, 31000 Toulouse Tel : 05.61.28.19.02 – e-mail : dupont.jean@email.fr		
PATIENT				
IDENTIFICATION		DURAND Nathalie (Valeur de l'INS)		
ANTHROPOLOGIE		Femme, 44 ans, 1,74 m, 60 kg		
PRESCRIPTION				
DATE DE PRESCRIPTION		02/06/2013		
SPECIALITE		POSOLOGIE	DUREE	MENTIONS
AFFECTION EXONERANTE (ALD)				
#1	PREVISCAN 20mg, comprimés (voie orale)	1 comprimé 1 fois par jour le soir	28 jours	NS AR2
MALADIES INTERCURRENTES (HORS ALD)				
#2	PARACETAMOL 1g, comprimés (voie orale)	1 comprimé 3 fois par jour	7 jours	
#3	PHLOROGLUCINOL 80 mg - SPASFON LYOC 80 mg, lyophilisats (voie oral)	2 comprimés par jour	5 jours	

Tableau 23 : Illustration possible de la structure d'une e-prescription :
normalisation des données et interopérabilité sémantique.

Après le dépôt de toute prescription il pourrait être intéressant d'autoriser un contrôle automatisé de certaines données par le serveur afin de permettre, par exemple le contrôle des droits de prescription au regard des produits prescrits (pour les médicaments dont la prescription est réservée à certains spécialistes) ou encore d'informer immédiatement le

²⁷⁰ Par opposition au système *Surescripts* opérationnel aux Etats-Unis où le patient choisi et désigne le pharmacien responsable de la dispensation avant son envoi.

prescripteur d'une alerte sanitaire relative à l'un des médicaments de la prescription... Permettre au système d'e-prescription d'interagir avec le dossier pharmaceutique et le dossier médical personnel pourrait également être source de nombreux bénéfices contribuant à sécuriser la prescription et la dispensation des médicaments.

Le patient se rend ensuite dans la pharmacie de son choix pour la dispensation de la prescription et, comme chez son médecin, il remet sa carte Vitale au pharmacien qui s'authentifie fortement auprès du serveur d'e-prescription à l'aide de sa carte CPS. Le patient est identifié par le calcul de son INS auprès du système ce qui permet au pharmacien d'accéder à son dossier d'e-prescriptions et de sélectionner la prescription à dispenser qui est alors automatiquement intégrée dans son logiciel officinal. Le pharmacien contrôle la qualité de la prescription, procède à la facturation des produits prescrits pendant que son logiciel affine la recherche d'incompatibilités au sein de cette prescription et avec des dispensations précédentes. Il accède au dossier pharmaceutique du patient de manière sécurisée, vérifie d'éventuelles incompatibilités avec des dispensations précédentes enregistrées par ce biais (dispensations des 4 derniers mois avec ou sans ordonnance) et alimente l'historique des dispensations du dossier pharmaceutique.

Le statut de la délivrance de la prescription est ensuite mis à jour dans la base d'e-prescriptions du patient (totalement, partiellement délivrée, à renouveler X fois...) permettant à la fois aux pharmaciens de connaître la validité d'une prescription mais aussi aux prescripteurs de préjuger de l'adhésion de leur patient au traitement. Il pourrait ainsi être pertinent d'associer un code couleurs aux prescriptions listées par le dispositif comme par exemple une ligne verte pour une nouvelle prescription, une ligne jaune pour une prescription partiellement délivrée ou à renouveler, une ligne rouge pour une prescription n'étant plus valide.

Après édition des factures électroniques (FSE/DRE) à la norme B2, le pharmacien imprime le plan thérapeutique qu'il remet au patient pour remplacer l'ordonnance dans son rôle d'information sur les modalités de la stratégie thérapeutique, le statut de dispensation de la prescription et sur le coût du traitement. Même si le plan thérapeutique doit être conservé aussi précieusement qu'une ordonnance papier par le patient, sa perte, son oubli ou sa détérioration restent possible comme pour tout document matérialisé. Permettre à tout patient de prendre connaissance du contenu de ses e-prescriptions et de leur historique via internet semble donc incontournable et constituerait un autre avantage de ce système. Si les patients bénéficient d'un accès autonome à leur DMP, ils n'accèdent en revanche à leur dossier pharmaceutique que par l'intermédiaire d'un pharmacien. Qu'en serait-il de ses e-prescriptions ?

A l'image de l'interface web permettant un accès autonome des patients à leur DMP, il apparaîtrait nécessaire d'élargir ce dispositif aux informations du dossier pharmaceutique utiles au patient ainsi qu'au contenu de ses e-prescriptions. **Permettre aux patients d'accéder à un tel système leur permettrait ainsi d'avoir un réel regard sur leur e-santé et pourrait les rendre acteurs de ce système.** En permettant aux patients de renseigner certaines informations directement depuis chez eux, la qualité et l'efficacité de leur suivi médical et pharmaco-thérapeutique pourraient être améliorées, par exemple en permettant au patient de renseigner l'évolution de ses symptômes ou de ses valeurs biologiques depuis son domicile, alertant le prescripteur si nécessaire. Cet outil deviendrait ainsi un véritable atout pour permettre l'épanouissement du pharmacien correspondant dans ses nouvelles missions en lui permettant de renouveler une prescription ou de modifier une posologie facilement, mais encore, en permettant un suivi régulier et en temps réel de leurs patients.

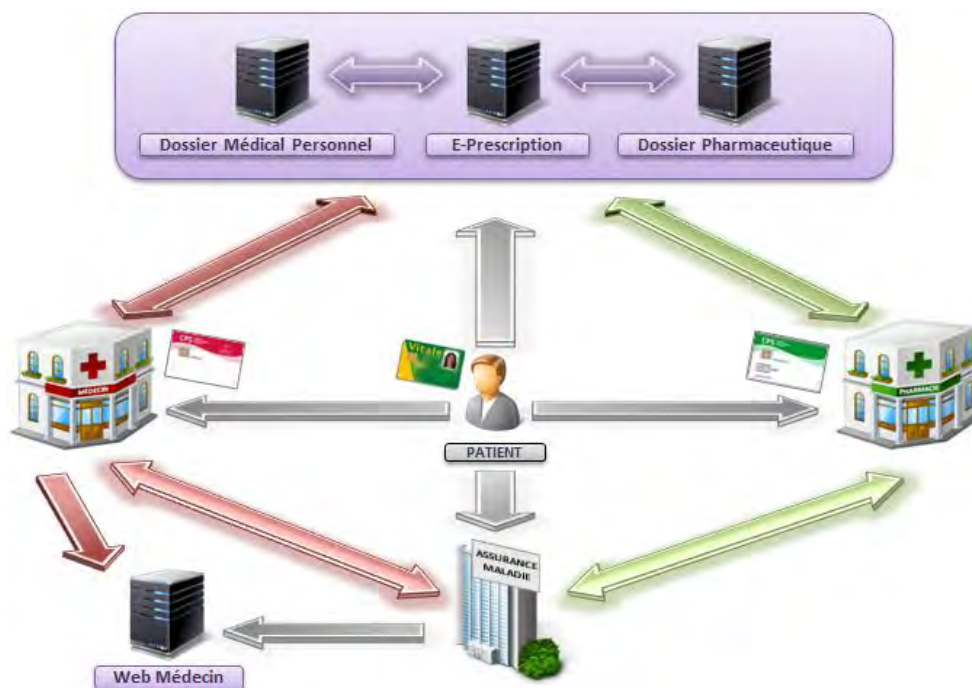


Figure 31 : Le patient au cœur de l'e-santé : une condition incontournable pour l'avenir.

Inclure les patients en tant qu'acteurs de l'e-santé représente toutefois un défi technique, notamment en terme d'interopérabilité, que l'ASIP Santé est capable de relever en coopération avec les ordres de professionnels de santé et la Caisse nationale d'assurance maladie. L'agence et l'ordre des pharmaciens possèdent en effet les compétences et le savoir-faire nécessaire pour développer un tel système. Permettre un accès autonome des patients « en lecture » et « en écriture » à un tel système suppose cependant le respect de règles de sécurité d'accès drastiques. Un accès par la fourniture d'un simple identifiant assorti d'un mot de passe à la création du dossier, comme il est actuellement d'usage pour le DMP, paraît insuffisant.

Le développement d'une e-administration efficace et sûre passe par la création d'un espace de confiance numérique entre les entités impliquées. Une infrastructure de gestion de clés cryptographiques permet, comme nous l'avons vu, d'attester de l'identité numérique d'un individu en lui attribuant des certificats électroniques. Le succès fulgurant de l'e-administration dans certains pays européens comme en Estonie fut permis par une convergence des systèmes d'information au sein desquels les citoyens sont de véritables acteurs reconnus numériquement.

L'ensemble des fonctions de sécurité liées à la création, l'édition ou la modification du DMP et du dossier pharmaceutique étant assumées par la carte CPS et ses certificats électroniques, comment garantir un accès autonome des patients à leurs dossiers médicaux partagés en toute sécurité ?

Malgré les capacités cryptographiques offertes par la carte Vitale 2, celle-ci ne semble actuellement pas utilisée en tant que support de clés cryptographiques pour l'accès aux dossiers médicaux partagés (DMP et dossier pharmaceutique). L'identification des patients au sein de ces systèmes est en effet garantie par le calcul de l'INS ou du NDP relatif au patient à partir d'informations lues dans sa carte Vitale, tandis que l'authentification forte du professionnel de santé, le respect de la confidentialité et de l'intégrité de l'échange sont assurés grâce aux certificats électroniques fournis par l'ASIP Santé (certificats CPS et

certificats de serveurs). Ces fonctions de sécurité offertes par la carte Vitale 2 n'étant pas mises à contribution, certaines communautés en ligne de professionnels de santé spécialistes en la matière s'interrogent, légitimement, quant aux réelles utilisations possibles de la carte, compte tenu des doutes persistant sur l'attribution de certificats électroniques à chaque bénéficiaire de l'assurance maladie.

Enfin, un système d'e-prescription pourrait permettre de valoriser les efforts entrepris par l'ASIP Santé pour généraliser leur messagerie sécurisée de santé en cours de développement (MSSanté). Intégrer ce système de messagerie au dispositif paraît incontournable pour permettre au pharmacien d'interroger le prescripteur au sujet d'un éventuel problème rencontré avec une prescription. Ce type de correspondance permet aux professionnels de santé de communiquer de manière asynchrone sans perturber l'exercice professionnel de l'un ou l'autre, ce qui représente un certain avantage par rapport aux communications téléphoniques qui mobilisent leur attention immédiate et leur oblige d'interrompre leur activité. Dans certains cas, le prescripteur pourra décider de modifier cette prescription, ou éventuellement de l'annuler, l'ensemble des actions étant réalisées directement via le service d'e-prescription et enregistrées dans un historique des traces.

B.3.4.3 EN CONSIDERANT LES LIMITES DE LA DEMATERIALISATION DE L'ORDONNANCE

La concentration des efforts fournis depuis près de vingt ans par le GIE SESAM-Vitale, la Caisse nationale d'assurance maladie, l'ASIP Santé, les ordres et les professionnels de santé permet aujourd'hui de dématérialiser la quasi-totalité des documents jalonnant le parcours de santé de tout patient. En dématérialisant totalement le circuit de l'ordonnance, le patient se voit toutefois privé d'un support d'informations primordial puisqu'elle lui permet de connaître les modalités de suivi de son traitement. Il s'agit précisément de la principale limite de la dématérialisation que tout système d'e-prescription doit considérer en proposant une alternative à l'ordonnance pour l'information du patient sur la stratégie thérapeutique du prescripteur ainsi que sur le coût des dépenses liées à son traitement.

Outre l'impact sur les technologies utilisées par les différents acteurs des systèmes d'information de santé, la dématérialisation totale de l'ordonnance n'est pas dénuée de conséquences sur l'exercice des professionnels de santé et particulièrement les pharmaciens, privés du support matériel de la prescription au moment de la dispensation, source d'erreurs potentielles. Ces limites de la dématérialisation peuvent cependant constituer une opportunité d'améliorer l'information des patients ainsi que la qualité, la sécurité et l'efficacité des dispensations en adaptant le contenu des données matérialisées à la qualité de leur destinataire.

B.3.4.3.a Le support de délivrance du pharmacien

Les prescripteurs utilisant déjà leurs logiciels d'aide à la prescription pour rédiger puis imprimer leurs ordonnances pourraient ne rencontrer que de faibles répercussions sur leur exercice quotidien. Après une éventuelle alimentation ou consultation du DMP, les prescripteurs éditent leurs prescriptions électroniques comme ils le faisaient auparavant avec leur logiciel puis, en lieu et place de l'impression matérialisant l'ordonnance, celle-ci est télétransmise sur le serveur dédié aux e-prescriptions. Les différentes études menées sur l'impact de l'e-prescription sur la qualité de leur exercice mettent d'ailleurs en avant un gain systématique de temps, de productivité ainsi qu'une amélioration de la sécurisation de la prescription.

Le processus d'exécution de l'ordonnance par le pharmacien pourrait en revanche être bouleversé. En effet, lors de chaque dispensation, le pharmacien procède à une analyse totale de l'ordonnance généralement réalisée en plusieurs étapes. Lors de l'accueil d'un patient muni d'une ordonnance au comptoir de la pharmacie, il procède généralement tout d'abord à une analyse de la licéité et de la validité de l'ordonnance. Il réalise ensuite une analyse de la qualité de la prescription visant à rechercher toute incompatibilité liée au traitement en présence du patient puis part chercher les produits prescrits en arrière-boutique²⁷¹. Il emporte avec lui l'ordonnance lui permettant de s'assurer qu'il dispense les produits effectivement prescrits (ou le cas échéant, d'en réaliser la substitution par un médicament générique), en quantités nécessaires et suffisantes tout en choisissant le conditionnement le plus économiquement adapté. Il procède finalement à une dernière analyse globale de la prescription au moment de la facturation et de la délivrance de ses conseils et des médicaments au patient.

Priver le pharmacien du support de prescription original au moment du choix des boîtes à dispenser directement devant le tiroir serait périlleux et il est tout à fait possible d'imaginer que certaines erreurs puissent se produire malgré les contrôles suivants. Il serait donc possible d'envisager que le pharmacien puisse imprimer un ticket récapitulatif des produits à dispenser réservé à son seul usage et lui permettant d'assurer la continuité entre l'analyse de la prescription à l'accueil du patient et l'analyse réalisée lors de la facturation et la délivrance²⁷².

Le modèle de ticket de d'aide à la dispensation réservé à l'usage des pharmaciens pourrait être représenté de la façon suivante :

PRESCRIPTION #0205201318308473648001 Femme de 44 ans, taille : 1,74 m, poids : 78kg Allergie connue à l'amoxicilline #1 PREVISCAN 20 mg : 1 comprimé 1 fois par jour pendant 3 mois. Suggestion : 1 x 34009 334 841 3 2 #2 PARACETAMOL 1 g : 1 comprimé 3 fois jour pendant 7 jours. Suggestion : 3 x 34009 363 815 7 5 #3 PHLOROGLUCINOL 80 mg : 2 comprimés par jour pendant 5 jours. Suggestion : 1 x 34009 369 708 8 5 PLAN DE DISPENSATION RESERVE A L'USAGE DES PHARMACIENS NE DONNANT PAS DROIT A LA DISPENSATION

Tableau 24 : Exemple possible de « ticket d'aide à la dispensation » réservé à l'usage des pharmaciens d'officine.

Comme le suggère ce modèle, il pourrait être intéressant de tirer parti d'un tel « ticket d'aide à la dispensation » en rappelant par exemple les données anthropomorphiques du patient véhiculées par le biais de l'e-prescription ainsi que certaines informations issues du logiciel

²⁷¹ Ce cas de figure ne concerne bien évidemment pas les officines munies d'automates ou robots permettant de sélectionner les conditionnements.

²⁷² L'impression de ce ticket doit pouvoir être facultative par exemple lorsqu'il y a peu de lignes de prescription.

d'aide à la dispensation paramétrées par le pharmacien (signalant par exemple une allergie, une grossesse ou une contre-indication particulière...). Il pourrait être envisagé que le logiciel d'aide à la puiſſe également ſuggérer au pharmacien (tout en préſervant ſon libre choix), le code CIP du conditionnement le plus économique (taille du conditionnement, poſſibilités de ſubſtitutions...) au regard de la ſtratégie thérapeutique adoptée, des produits dont il diſpoſe, de leur diſponibilité auprès des organismes répartiteurs et des alertes ſanitaires actuelles.

B.3.4.3.b Le plan thérapeutique du patient

L'ordonnance préſente, comme nous l'avons vu, un rôle crucial dans l'information du patient. Si un ſystème d'e-prescription peut permettre au patient un accès autonome à ſon historique de prescription et prendre connoiſſance du contenu d'une prescription électronique en utilisant ſon propre ordinateur, une copie du contenu de la prescription doit impérativement lui être remise afin de lui permettre de ſe remémorer les modalités de ſon traitement à chaque inſtant. Une alternative prévue par le CLIO Santé conſiſte ainſi en la remise d'un document papier ne donnant pas droit à la diſpensation, intitulé « **plan thérapeutique** » uniquement voué à l'information du patient. Incontournable, la diſtribution du plan thérapeutique relatif à toute prescription pourrait conſtituer une réelle opportunité d'améliorer l'information des patients en lui délivrant uniquement les données qui lui ſont utiles. Les principaux bénéfices tirés de l'optimiſation de ce plan thérapeutique pourraient être nombreux et notamment :

- **Améliorer la compréhension de la ſtratégie thérapeutique par le patient** en ſupprimant certaines informations portées par l'ordonnance qui étaient juſqu'alors réſervées aux pharmaciens ou aux caiſſes d'assurance maladie. Dans un contexte où certains patients éprouvent parfois des difficultés à établir une corréſpondance entre une ligne de prescription et le conditionnement du médicament associé, il ſerait également intéreſſant de généraliſer l'inscription du numéro de ligne de prescription ſur chaque conditionnement dans un eſpace prévu à cet effet. Les logiciels d'aide à la diſpensation propoſant d'ores et déjà une fonction d'édition d'un ticket de « plan de poſologie » ou « feuille d'adminiſtration », la généraliſation de cette fonction à chaque diſpensation pourrait ainſi permettre de réduire conſidérablement certains riſques d'accidents liés à la méconnoiſſance et au méſuſage des médicaments par les patients. L'objectif d'un tel ſystème doit permettre à chaque patient de prendre le bon médicament, à la bonne doſe, au bon moment, et ſelon la bonne voie d'adminiſtration.

- **améliorer l'information du patient ſur le coût de ſon traitement** en intégrant les données de facturation juſqu'alors imprimées au dos de l'ordonnance, au plan thérapeutique. En notifiant le prix unitaire de chaque conditionnement d'une ligne de prescription ainſi que le prix total et la répartition de la priſe en charge des frais entre les organismes d'assurance maladie obligatoire, complémentaire et le patient. Ces informations pourraient être préſentées dans un tableau facilement compréhensible par miſe en corréſpondance de chaque ligne de facturation avec une ligne de prescription et une ligne de diſpensation par un même numéro.

- **faciliter la compréhension du ſtatut de diſpensation de la prescription** en ſpécifiant pour chaque ligne de prescription le caractère total, partiel ou à renouveler de la diſpensation. Il deviendrait ainſi pertinent dans ce dernier cas, de préciser la date de la prochaine diſpensation afin de réſpecter le délai de 21 jours (ſouvent méconnu des patients) néceſſaire entre deux renouvellements ou dans le cas de délivrance fractionnée.

ſelon l'exemple d'e-prescription élaboré précédemment, le plan thérapeutique remis au patient pourrait être matérialiſé par un document au format d'un ticket de caiſſe de 8 cm de largeur illuſtré par le tableau 25.

PLAN THERAPEUTIQUE

DURAND Nathalie

PRESCRIPTION #0206201318308473648001

Le 2 juin 2013

Dr DUPONT Jean (médecine générale)
12 rue des arts, 31000 Toulouse (05.61.28.19.02)

#1 PREVISCAN 20 mg : 1 comprimé 1 fois par jour
le soir à heure fixe pendant 3 mois.

#2 PARACETAMOL 1 g : 1 comprimés 3 fois jour
si douleur ou fièvre pendant 7 jours.

**#3 PHLOROGLUCINOL 80 mg - SPASFON
LYOC 80 mg** : 2 comprimés par jour pendant 5
jours.

NE PAS DEPASSER LES DOSES PRESCRITES

STATUT DE DISPENSATION

**Pharmacie du moulin de Coty, 3 rue de la rivière,
46000 Cahors (05.65.32.69.48)**

#1 PREVISCAN 20 mg : Délivrance partielle (1
boîte de 30 comprimés le 3 juin 2013). *Prochaine
dispensation à partir du 24 juin 2013.*

#2 PARACETAMOL 1g : Délivrance totale (3
boîtes de 8 comprimés le 3 juin 2013).

**#3 PHLOROGLUCINOL 80 mg - SPASFON
LYOC 80 mg** : Délivrance totale (1 boîte de 10
comprimés le 3 juin 2013).

TICKET VITALE PATIENT

Le 3 juin 2013

	Prix unitaire	Prix total	Total RO	Total RC	Total Patient
#1	3,98	3,98	3,98	0	0
#2	1,95	5,85	3,80	2,05	0
#3	2,32	2,32	0,35	0	1,97
TOTAL		12,15	8,13	2,05	1,97

Les montants du Ticket Vitale sont exprimés en euros.

**PLAN THERAPEUTIQUE POUR INFORMATION DU PATIENT NE
DONNANT PAS DROIT A LA DISPENSATION**

Tableau 25 : Illustration possible du plan thérapeutique remis au patient.

Ce format de ticket de caisse, coutumier des français, pourrait être intéressant car il présente l'avantage de ne pas être limité en longueur puisque ce type d'imprimante utilise un rouleau de papier. Le patient disposerait ainsi de toutes les informations relatives à une dispensation sur un seul et même support, facilement archivable et dont la résistance aux contraintes physiques (déchirement, exposition à l'eau, au feu...) est accrue.

Mais qui du médecin ou du pharmacien pourrait être chargé de la remise du plan thérapeutique au patient ?

Afin d'optimiser totalement les fonctions que le plan thérapeutique pourrait proposer, il apparaît probable que celui-ci soit remis au patient par le pharmacien, au moment de la dispensation. Selon cette hypothèse, le prescripteur devra informer clairement et oralement le patient du contenu de la prescription qui lui sera retranscrit sur le plan thérapeutique remis par le pharmacien.

B.3.4.4 EN FEDERANT LES PROFESSIONNELS DE SANTE AUTOUR D'UN PROJET COMMUN

Afin de parfaire notre modèle d'e-santé, l'e-prescription pourrait constituer une véritable passerelle électronique entre les prescripteurs et les 22000 pharmacies du réseau officinal français, permettant par ailleurs d'insuffler un troisième souffle au dossier médical personnel.

L'adhésion des prescripteurs à l'e-prescription constitue en revanche un véritable défi pour la généralisation d'un tel dispositif comme ce fut le cas pour le dossier médical personnel. Les raisons d'un manque d'adhésion peuvent être multiples mais le vieillissement de la population de médecins moins enclin à utiliser de tels procédés, bouleversant leurs méthodes d'exercices habituelles paraît être un facteur prépondérant. Il est donc nécessaire que cet outil s'intègre parfaitement dans l'exercice professionnel en laissant la liberté à tout prescripteur de matérialiser ses prescriptions à tout instant.

Une première « phase pilote » présentée par le CLIO Santé concernera les pharmacies de deux ou trois bassins de population choisis en fonction de leur dynamisme et de leur degré d'avancement dans la mise en œuvre des projets nationaux en matière d'e-santé. Ces régions pourront tester un système d'e-prescription faisant intervenir dans un premier temps une centaine de pharmacies et de prescripteurs ainsi que certains laboratoires d'analyses médicales.

La mise en œuvre de cette phase pilote et le choix des bassins de population seront définis par un comité de pilotage organisé avec l'ASIP Santé après concertation avec les organisations professionnelles nationales et régionales, dans un cadre défini par la Gouvernance nationale stratégique de déploiement des systèmes d'information en santé à l'intention des Agences régionales de santé, et de l'Union nationale des caisses d'assurance maladie. L'évaluation de cette phase pilote devra permettre une analyse sur un bassin de vie, de l'amélioration des services rendus et constituera également le socle technique et économique nécessaire à la généralisation de ce projet (111).

CONCLUSION

L'avenir de l'e-santé s'annonce exceptionnellement ouvert et de concrètes opportunités d'améliorer les systèmes actuels voient le jour. La mise en œuvre de la loi HPST ainsi que les efforts fournis par les ordres de professionnels de santé, la Caisse nationale d'assurance maladie, les agences régionales de santé et l'ASIP Santé offrent de nouvelles perspectives pour la télé-médecine et la télé-pharmacie. En réaffirmant le statut du pharmacien en tant que professionnel de santé, la loi HPST et l'avenant n°1 à la convention pharmaceutique entré en vigueur le 28 juin 2013, leur offre une chance inespérée de développer leur champ de compétences. Les pharmaciens, et particulièrement les nouvelles générations, ne doivent pas manquer cette opportunité de s'affirmer à l'heure où leur monopole est dangereusement en péril.

L'intégration progressive des TIC dans l'environnement de travail du pharmacien a permis de faciliter la gestion des activités de l'officine et d'améliorer la qualité, la sécurité et l'efficacité de leurs dispensations. Si des solutions d'aide à la dispensation et au suivi thérapeutique sont mises en œuvre localement à l'officine depuis bien longtemps, l'émergence des dossiers médicaux partagés (dossier médical personnel et dossier pharmaceutique) tend à bouleverser les habitudes des professionnels de santé et des patients. Un système d'e-santé abouti promettant de nombreux bénéfices, il apparaît désormais urgent de finaliser le dossier médical personnel et d'en assurer l'interaction avec le dossier pharmaceutique. La création d'une interface en ligne permettant un accès sélectif et sécurisé aux différents systèmes pourrait en favoriser la convergence. Afin d'assurer la cohésion et l'efficacité du parcours de soins de chacun, une telle interface permettrait à tout professionnel de santé, selon ses compétences, d'accéder aux différents outils d'e-santé tels que le dossier médical personnel, le dossier pharmaceutique, l'e-prescription et la MSSanté. Cependant, l'avenir de l'e-santé se tournera certainement vers le patient afin de le rendre acteur de ce système et de lui offrir un regard direct sur ses données de santé, favorisant son implication dans chaque démarche de soins.

Si 70 % des personnes interrogées dans le cadre de l'enquête du Collectif Interassociatif sur la santé portant sur l'information des patients et l'usage des nouvelles technologies en matière de santé, éprouvent de la méfiance à l'égard des services de santé disponibles sur internet, une sur deux en reconnaît l'utilité (13). Puisqu'elles sont sensibles, les données de santé traitées par ces systèmes doivent bénéficier de mesures très strictes permettant d'en préserver la confidentialité. S'agissant de données électroniques, les moyens mis en œuvre afin d'en assurer la sécurité utilisent notamment des techniques cryptographiques basées sur des algorithmes mathématiques complexes dont il est *a priori* impossible de percer le secret. Il pourrait cependant en fait s'agir d'un « secret de polichinelle » puisque les récentes révélations d'Edward Snowden dénonçant l'existence d'un système de surveillance de contenus électroniques transitant par les serveurs des plus grands groupes informatiques mondiaux, seraient fondées. Ces révélations concernent la possibilité de déchiffrement de contenus électroniques sécurisés par certains protocoles tels que TLS et SSL utilisés dans le monde entier pour l'e-Administration, l'e-Commerce, l'e-santé... La *National security agency* ou NSA (l'une des quinze agences de renseignement aux Etats-Unis), puisqu'elle contribue à l'élaboration de ces standards permettant de sécuriser ses propres systèmes, aurait ainsi mis en place un système lui permettant de garder le contrôle de leur conception afin d'y installer des moyens de contournement, véritables failles de ces systèmes, connus uniquement de la NSA²⁷³.

²⁷³The Guardian, September 5th 2013.

De nombreuses inquiétudes naissant chaque jour quant à l'exploitation possible de ces données, l'avenir des techniques de sécurité informatique paraît sombre tant la confiance des utilisateurs de ces systèmes demeure plus que jamais incertaine. Compte tenu des enjeux, et particulièrement en terme de santé publique, poursuivre les efforts entrepris pour développer l'e-santé en France doit cependant rester une priorité pour les orientations stratégiques à venir de notre système de santé.

Alors que Madame Marisol Touraine, ministre des affaires sociales et de la santé, prévoit l'extension de la généralisation du principe du tiers-payant par les médecins, de nombreuses voix s'élèvent face au risque de « surconsommation » en consultations médicales. En permettant aux patients d'interagir en ligne avec leurs professionnels de santé, devenant acteurs de leur e-santé, de nombreuses consultations médicales pourraient certainement être évitées. Comme nous l'avons vu, il s'agit d'ailleurs de l'un des principaux qu'il est possible de tirer d'un système d'e-Santé abouti tel que le système *Diraya* en Andalousie.

L'e-santé pourrait donc constituer une réponse aux nombreuses problématiques futures de notre système de santé et notamment :

- en facilitant l'accès aux soins et leur coordination ;
- en améliorant la qualité, la sécurité et l'efficience des soins et du suivi des patients ;
- en améliorant l'information et l'éducation des patients sur la santé ;
- en favorisant la coopération entre professionnels de santé ;
- en limitant la surconsommation de consultations médicales et de produits de santé.

BIBLIOGRAPHIE

1. **Agence nationale de la sécurité des systèmes d'information, Direction générale de la modernisation de l'État.** *Référentiel général de sécurité version 1.0.* [En ligne] 6 mai 2010. <http://www.ssi.gouv.fr/fr/reglementation-ssi/referentiel-general-de-securite/>
2. **Philippe Moutenet, Mohsen Mechalia, Marie-Agnès Bonnefoy, René Eksl, Dominique Héraud, Philippe Passemard (Union des caisses nationales de sécurité sociale, UCANSS).** Etude des impacts de la dématérialisation des données et des échanges sur les métiers et les compétences au sein des organismes de sécurité sociale. [En ligne] 15 juin 2011. <http://www.ucanss.fr>.
3. **Alain Venot, Anita Burgun, Catherine Quantin.** *Informatique médicale, e-Santé : fondements et applications.* Springer-Verlag, 2013.
4. **European Commission.** *e-Health - making healthcare better for European citizens: an action plan for a European e-Health area.* Bruxelles : 30 avril 2004. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions. /* COM/2004/0356 final */.
5. **Karl A. Stroetmann, Lutz Kubitschke, Simon Robinson, Veli Stroetmann, Kevin Cullen, David McDaid : World health organization.** How can telehealth help in the provision of integrated care ? [En ligne] 2010. <http://www.euro.who.int/>. ISSN 1997-8073.
6. **Conférence nationale de santé.** Avis sur l'informatisation des données de santé. [En ligne] Octobre 2010. <http://www.sante.gouv.fr/>.
7. **D. Thouvenin.** *Le secret médical et l'information du malade.* Presses universitaires de Lyon, 1982. ISBN-13: 978-2729701307.
8. **Collectif interassociatif sur la santé.** Lettre du collectif interassociatif sur la santé n° 6 : Informatisation des données de santé : où allons-nous ? [En ligne] 13 septembre 2012. <http://www.leciss.org>. ISSN : 1969-1386.
9. **JORF n°154 du 5 juillet 2006 page 10085, texte n° 91.** Délibération n° 2006-161 du 8 juin 2006 portant adoption d'une norme simplifiée relative aux traitements automatisés de données à caractère personnel mis en oeuvre par les pharmaciens à des fins de gestion de la pharmacie (norme simplifiée n° 52) . [En ligne] <http://www.legifrance.gouv.fr>. NOR: CNIA0600014X .
10. **Conseil national de l'ordre des pharmaciens.** Guide de recommandations sur le respect de la confidentialité des données de patients dans l'usage de l'informatique. [En ligne] février 2013. <http://www.ordre.pharmacien.fr>.
11. **Agence nationale de la sécurité des systèmes d'information.** Morpho - Carte Vitale 2 - Applications ADELE et VITALE Composant SB23ZL48 masqué par le logiciel SESAM VITALE v1.0.1 avec correctif version 1. *Produits qualifiés - ANSSI.* [En ligne] <http://www.ssi.gouv.fr>.
12. **Agence des systèmes d'information partagés de santé.** La carte CPS3 : présentation générale. [En ligne] 2011. <http://integrateurs-cps.asipsante.fr>.
13. **GALLAY Anne-Laure, TARDIEU Blandine : Collectif interassociatif sur la santé.** Enquête : "Le baromètre des droits des malades". [En ligne] mars 2013. <http://www.leciss.org/>.
14. **Ministère de la santé, TNS SOFRES.** La perception des droits des patients par les professionnels de santé, enquête qualitative (note de synthèse). [En ligne] 4 mars 2011. <http://www.sante.gouv.fr>.
15. **Commission nationale de l'informatique et des libertés.** Guide pour les professionnels de santé. [En ligne] 2011. www.cnil.fr.
16. **Tristan Klein (Centre d'analyse stratégique), Daniel Ratier (Direction générale du travail).** L'impact des TIC sur les conditions de travail. [En ligne] février 2012. <http://www.strategie.gouv.fr>. ISBN : 978-2-11-009049-2.

17. **CARNUS Cécile.** Le pharmacien et l'informatique officinale à travers une enquête menée dans le Lot en 2001. Thèse : Pharmacie : Toulouse 3 : 2002 ; 2002TOU32065.
18. Les techniques de numérisation. *Le fonctionnement du scanner*. [En ligne] <http://www.culture.gouv.fr>.
19. **Club Inter Pharmaceutique.** DATA MATRIX : Support de la traçabilité du médicament, caractéristiques techniques. *Les cahiers CIP-ACL*. [En ligne] Novembre 2007. <http://www.ucdcip.org>.
20. **MAQUART Bruno : Inspection générale des affaires sociales.** *La suppression de la vignette pharmaceutique, évaluation des modalités de mise en oeuvre*. Juillet 2012. RM2012-095P.
21. **RAIMBAULT Guy.** *Mille mots pour aborder l'informatique*. s.l. : Editions L'Harmattan, 2006. ISBN : 229600198X.
22. **Haute Autorité de santé.** Charte de qualité des bases de données sur les médicaments destinées à l'usage des LAP candidats à la certification de la HAS. [En ligne] 15 juin 2009. <http://www.has-sante.fr>.
23. **MARTIN Françoise.** Cours de communication, 6ème année officine, Faculté des sciences pharmaceutiques de Toulouse. 2011.
24. **Centre d'études et de recherchesur sur les partenariats avec les entreprises et les professions.** Gestion des stocks, la gestion sur seuil. [En ligne] 18 Janvier 2005. <http://www.cerpet.education.gouv.fr>.
25. **GIE SESAM-Vitale.** Cahier des charges Sesam Vitale, spécifications externes des modules SESAM-Vitale, ordonnance du 24/04/1996, version 1.40 intégrant l'addendum N°6 de juillet 2010 avec erratum mars 2012. [En ligne] avril 2003. <http://www.sesam-vitale.fr>. PDT-CDC-001.
26. **Agence des systèmes d'information partagés de santé.** Qu'est-ce que la carte CPS ? [En ligne] 4 octobre 2013. <http://esante.gouv.fr>.
27. **GIE SESAM-Vitale.** Rapport d'activité 2011. [En ligne] <http://www.sesam-vitale.fr>.
28. **WILLIAMS Bob.** *Intelligent transport systems standards*. s.l. : Artech House, 2008. ISBN 1596932910, 9781596932913.
29. **Secrétariat général de la défense nationale, Direction centrale de la sécurité des systèmes d'information.** Référentiel général de sécurité version 1.0. Processus de qualification d'un produit de sécurité - niveau renforcé -. [En ligne] <http://www.ssi.gouv.fr/N°/SGDN/DCSSI/SDR>.
30. **GIE SESAM-Vitale.** Les différents CDC, référentiels et paliers - Fonctionnalités. [En ligne] 26 juillet 2012. <http://www.sesam-vitale.fr>.
31. —. Journées nationales SESAM Vitale, atelier carte Vitale 2 et chaînes d'administration des cartes. [En ligne] 11 octobre 2006. <http://www.unrs.fr>.
32. **Agence des systèmes d'information partagés de santé.** Les cartes de la famille CPS. [En ligne] 12 juin 2012. <http://esante.gouv.fr/services/espace-cps/les-cartes-de-la-famille-cps>.
33. **GIE SESAM-Vitale.** 80% des pharmaciens télétransmettent en version SESAM-Vitale 1.40. [En ligne] 1er février 2013. <http://www.sesam-vitale.fr>.
34. **Centre national de dépôt et d'agrément.** Notre mission. [En ligne] <http://www.cnda-vitale.fr/php/CNDA.php?libelle=nos+missions>.
35. **GIE SESAM-Vitale.** Le référentiel d'homologation accès cartes (RAC) : présentation. [En ligne] 28 août 2012. <http://www.sesam-vitale.fr>.
36. **Agence des systèmes d'information partagés de santé.** Comment fonctionne une carte CPS ? [En ligne] 12 juin 2012. <http://esante.gouv.fr/services/espace-cps/comment-fonctionne-une-carte-cps>.
37. **GIE SESAM-Vitale.** Migration en v3.x des lecteurs SESAM-Vitale. [En ligne] <http://www.sesam-vitale.fr/divers/lecteurs-migration.asp>.

38. **Agence des systèmes d'information partagés de santé.** Obtention, actualisation, renouvellement de votre carte CPS. [En ligne] 20 novembre 2012. <http://esante.gouv.fr/services/espace-cps/pour-les-professionnels-de-sante#A>.
39. **GIE SESAM-Vitale.** *Rapport d'activité 2012*. 28 octobre 2013.
40. **JORF n°0107 du 6 mai 2012 page 8112 , texte n° 34 .** Arrêté du 4 mai 2012 portant approbation de la convention nationale organisant les rapports entre les pharmaciens titulaires d'officine et l'assurance maladie . NOR: ETSS1220861A .
41. **GIE SESAM-Vitale.** *Cahier des charges numérisation et télétransmission des pièces justificatives "Tout PS prescrits" version 2.00*. Novembre 2011. PDT-CDC-002.
42. **Conseil national de l'ordre des pharmaciens.** Formulaire de demande d'inscription ou de modification d'inscription au tableau de la section A de l'ordre des pharmaciens. [En ligne] 9 août 2010. <http://www.ordre.pharmacien.fr>.
43. **Agence des systèmes d'information partagés de santé.** FAQ des demandes d'accès RPPS. [En ligne] 22 octobre 2012. <http://esante.gouv.fr/services/referentiels/identification/faq-des-demandes-d-acces-rpps>.
44. **Commission nationale de l'informatique et des libertés.** Conclusions de la Commission nationale de l'informatique et des libertés sur l'utilisation du NIR comme identifiant de santé. [En ligne] 20 février 2007. <http://www.cnil.fr>.
45. **Agence des systèmes d'information partagés de santé.** Programme identifiant national de santé, dossier de conception de l'INS-C. [En ligne] 28 octobre 2009. <http://esante.gouv.fr>. [SPEC INSC CONCEPT].
46. —. INS et dossier médical personnel. [En ligne] octobre 2012. <http://www.dmp.gouv.fr/documentation/ins>.
47. —. Programme identifiant national de santé, algorithme de calcul de l'INS-C. [En ligne] 30 octobre 2009. <http://esante.gouv.fr>. [SPEC INS-C].
48. —. Programme identifiant national de santé, exemples de code. [En ligne] 30 Octobre 2009. <http://esante.gouv.fr>. [SPEC INSC CODE].
49. **GS1 France.** Découvrir GS1. [En ligne] <http://www.institutionnel.gs1.fr/Qui-sommes-nous/Decouvrir-GS1>.
50. —. Guide des bonnes pratiques de lecture du code à barres 2D, GS1 Datamatrix. [En ligne] 16 Mai 2012. <http://www.publications.gs1.fr>.
51. **Club Inter Pharmaceutique.** Evolution de la codification et du marquage des produits de santé. *Les cahiers CIP/ACL*. [En ligne] Juillet 2009. <http://www.dilec.fr>.
52. **Conseil national de l'ordre des pharmaciens.** *Guide de stage de pratique professionnelle en officine, 6ème année*. 2012.
53. **JORF n°0024 du 29 janvier 2013 page 1784, texte n° 113.** Avis aux fabricants et aux distributeurs de spécialités pharmaceutiques. [En ligne] <http://www.legifrance.gouv.fr>. NOR: AFSS1242364V .
54. **GS1 France.** Les standards GS1. [En ligne] <http://www.institutionnel.gs1.fr/Qui-sommes-nous/Les-standards-GS1>.
55. **Club Inter Pharmaceutique.** Mise en oeuvre de la traçabilité du médicament. *Les cahiers CIP/ACL*. [En ligne] décembre 2008. <http://www.ucdcip.org>.
56. —. Caractéristiques techniques du Data Matrix pour la traçabilité version 1.0. [En ligne] 29 novembre 2007. <http://www.coserm.fr>.
57. **APSYDOC.** Code 128. [En ligne] 2006. <http://www.apsydoc.fr/>.
58. **BICLET Philippe, président du Comité d'agrément des hébergeurs de données de santé.** Hébergement et échange de données de santé. *Médecine et droit*. Novembre- Décembre 2010, n°105, pp. 159-160.
59. **Mémoires du DUEC "Qualité à l'officine", faculté des sciences pharmaceutiques de Lille.** Procédure d'archivage en officine. [En ligne] 16 juillet 2007. <http://qualiteofficine.univ-lille2.fr>.

60. **Agence des systèmes d'information partagés de santé.** Hébergement : FAQ, Q13 – Les données de santé doivent-elles nécessairement être hébergées sur le territoire français ? [En ligne] 26 septembre 2011. <http://esante.gouv.fr/services/referentiels/securite/hebergement-faq#13>.
61. —. Cadre d'interopérabilité des SIS, document chapeau. [En ligne] 13 Novembre 2012. <http://esante.gouv.fr/v1.3.1>.
62. **Direction générale de la modernisation de l'Etat.** Référentiel général d'interopérabilité version 1.0. [En ligne] 12 mai 2009. <http://esante.gouv.fr/>.
63. **Commission nationale de l'informatique et des libertés.** Guide, la sécurité des données personnelles. [En ligne] 2010. <http://www.cnil.fr>.
64. **Agence nationale de la sécurité des systèmes d'information.** Référentiel général de sécurité version 1.0, annexe B1, mécanismes cryptographiques. Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques. [En ligne] 26 janvier 2010. <http://www.ssi.gouv.fr>.
65. **SHAMIR Adi and TROMER Eran.** Factoring large numbers with the TWIRL device. [En ligne] 2003. <http://www.iacr.org>.
66. **Agence nationale de la sécurité des systèmes d'information.** Référentiel général de sécurité version 1.0, annexe B3, règles et recommandations concernant les mécanismes d'authentification. [En ligne] 13 janvier 2010. <http://www.ssi.gouv.fr>.
67. —. Référentiel général de sécurité version 1.0, annexe A3, Fonction de sécurité "signature". [En ligne] 11 février 2010. <http://www.ssi.gouv.fr>.
68. —. Référentiel général de sécurité version 1.0, annexe B2, règles et recommandations concernant la gestion des clés utilisées dans les mécanismes cryptographiques. [En ligne] 24 octobre 2008. <http://www.ssi.gouv.fr>.
69. **Agence des systèmes d'information partagés de santé.** IGC-CPS2ter-2020 – Gabarits des certificats et des CRL applicables aux cartes CPS2ter et CPS3. [En ligne] 20 mars 2012. <http://integrateurs-cps.asipsante.fr>.
70. **Agence nationale de la sécurité des systèmes d'information.** Qualification des prestataires de services de certification électronique (PSCE). [En ligne] <http://www.ssi.gouv.fr>.
71. **Agence des systèmes d'information partagés de santé.** Politiques de certification de l'IGC "CPS", autorité de certification "PROFESSIONNEL - Classe 1", certificats de signature et d'authentification. [En ligne] 13 décembre 2004. <http://esante.gouv.fr>.
72. —. Les certificats CPS. [En ligne] 12 juin 2012. <http://esante.gouv.fr/services/espace-cps/les-certificats-cps>.
73. —. Politique de certification de l'infrastructure de gestion de clés "carte de professionnel de santé". Certificats de confidentialité. [En ligne] 19 mars 2002. http://esante.gouv.fr/sites/default/files/PC_conf_V1.3.pdf.
74. —. Conditions générales d'utilisation des produits de certification de l'ASIP Santé. [En ligne] 11 septembre 2012. http://esante.gouv.fr/sites/default/files/ASIP_CGU-Produits-Certification_v1-6_20120911.pdf.
75. —. Politique de certification de l'infrastructure de gestion de clés "carte de professionnel de santé". Certificats de serveurs applicatifs. [En ligne] 19 mars 2002. <http://esante.gouv.fr>.
76. **BERTRAND Mathieu.** Le dossier pharmaceutique au service du pharmacien : un outil informatique construit pour une utilisation professionnelle optimale [En ligne] sous la direction de Francine Paulus.- Nancy : SCD de l'Université de Lorraine, 2012. Thèse : Pharmacie : Nancy1 : 2012 : univ-lorraine-ori-17657. Format pdf. Disponible sur : http://docnum.univ-lorraine.fr/public/BUPHA_T_2012_BERTRAND_MATHIEU.pdf
77. **Agence des systèmes d'information partagés de santé.** Certificats SSL/SMIME de l'ASIP Santé. [En ligne] <http://integrateurs-cps.asipsante.fr>.
78. **Centre national de la recherche scientifique d'Aquitaine.** L'accès sécurisé aux données, les applications du chiffrement. [En ligne] <http://www.cnrs.fr>.

79. **Agence des systèmes d'informaion partagés de santé.** Prorogation IGC-CPS2ter, impacts sur les applications CPS. [En ligne] 29 juin 2012. <http://integrateurs-cps.asipsante.fr>.
80. **Caisse nationale d'assurance maladie des travailleurs salariés.** La carte vitale. [En ligne] 10 octobre 2012. <http://www.ameli.fr>.
81. **Agence nationale de la sécurité des systèmes d'information.** Rapport de certification, carte Vitale 2 - application VITALE : composant SB23ZL48 masqué par le logiciel SESAM VITALE v1.0.1 avec correctif version 1. [En ligne] 7 juin 2012. <http://www.ssi.gouv.fr>. ANSSI-CC-2011/67.
82. —. Rapport de certification, carte Vitale 2 - application ADELE : Composant SB23ZL48 masqué par le logiciel SESAM VITALE v1.0.1 avec correctif version 1. [En ligne] 7 juin 2012. <http://www.ssi.gouv.fr>. ANSSI-CC-2011/68.
83. —. Référentiel général de sécurité version 1.0, annexe A2, Fonction de sécurité : authentification. [En ligne] 11 février 2010.
84. **Décision n° 2012-652 du Conseil constitutionnel du 22 mars 2012 sur la loi relative à la protection de l'identité.** [En ligne] 22 mars 2012. <http://www.conseil-constitutionnel.fr>.
85. **LESAULNIER Frédérique.** Internet, santé et données personnelles. *Médecine & droit*. Elsevier Masson, janvier 2013, Vol.2013, N° 118.
86. **Caisse national d'assurance maladie des travailleurs salariés.** Modernisation et efficience du système de soins : la dématérialisation des ordonnances par les pharmaciens est engagée. [En ligne] 1er dDécembre 2011. <http://www.ameli.fr>.
87. **GIE SESAM-Vitale.** Cahier des charges organismes concentrateurs techniques basé sur la version 1.40 addendum n°4 avec erratum du CDC Sesam-Vitale. Cahier des règles et spécifications fonctionnelles et techniques. [En ligne] 3 mars 2009. <http://www.sesam-vitale.fr>.
88. **Caisse nationale d'assurance maladie des travailleurs salariés.** Cahier des charges de la norme B2 inter-régimes. Télétransmission de factures entre professionnels de santé et organismes d'assurance maladie. [En ligne] Juin 2007. <http://www.ameli.fr>.
89. **Caisse nationale d'assurance maladie des travailleurs salariés.** ENTSCANORDO, Message d'entête pour l'échange d'ordonnances Scannées version 02.06. [En ligne] 20 octobre 2011. <http://www.ameli.fr/>.
90. **DEGOULET P. , FIESHI M. - Informatique médicale 3ème édition.** Paris : Masson, 1998. ISBN: 9782225832826.
91. **ROGER FRANCE F.** *Le résumé du dossier médical, indicateur informatisé d eperformance et de qualité de soins.* Bruxelles : 1982.
92. **Faculté des sciences pharmaceutiques de Lille.** Le dossier de suivi pharmacothérapeutique au sein d'un groupe de pharmacies. [En ligne] <http://qualiteofficine.univ-lille2.fr>.
93. **Conseil national de l'ordre des pharmaciens.** *Kit de démarrage du DP. Introduction à votre nouvel outil professionnel.*
94. **Collectif interassociatif sur la santé.** Fiche thématique n°29 du CISS : Le dossier pharmaceutique. [En ligne] 2012. <http://www.leciss.org>.
95. **Agence des systèmes d'informaion partagés de santé.** La conférence du 9 avril 2009. [En ligne] 9 avril 2010. <http://esante.gouv.fr/actus/politique-publique/la-conference-du-9-avril-2009>.
96. **Conseil national de l'ordre des pharmaciens.** Le dossier pharmaceutique. [En ligne] 1 avril 2013. <http://www.ordre.pharmacien.fr/Le-Dossier-Pharmaceutique/Qu-est-ce-que-le-DP>.
97. **Collectif interassociatif sur la santé.** Fiche thématique du CISS n°15. Informatisation des données de santé : le web-médecin. [En ligne] 2012. <http://www.leciss.org>.
98. *Des alertes sanitaires sur le dossier pharmaceutique.* **Anne-Laure Mercier, le moniteur des pharmacies.** n°2799 p.12, octobre 2009.
99. **Conseil national de l'ordre des pharmaciens.** Le dossier pharmaceutique cahier 1. *Chiffres, mode d'emploi, perspectives et acteurs majeurs : l'essentiel pour mieux comprendre*

- cet outil professionnel incontournable.* [En ligne] septembre 2011. <http://www.ordre.pharmacien.fr>.
100. **Agence nationale de sécurité du médicament.** Retraits de lots des médicaments : un nouveau système d'information plus performant. *Communiqué de l'ANSM.* [En ligne] 25 octobre 2011. <http://ansm.sante.fr/>.
101. **GS1.** Guide d'utilisation des standards GS1 pour les produits de santé. [En ligne] 2008. www.gs1.fr.
102. **Conseil national de l'ordre des pharmaciens.** Le journal de l'ordre des pharmaciens. Retraits et rappels de lots : un nouveau système d'alerte. [En ligne] 8 novembre 2011. <http://www.ordre.pharmacien.fr/>.
103. **Commission nationale de l'informatique et des libertés.** Délibération n°2008-487 du 2 décembre 2008 portant autorisation des traitements de données personnelles permettant la mise en œuvre généralisée du dossier pharmaceutique. [En ligne] 2 décembre 2008. <http://www.legifrance.gouv.fr>.
104. **Agence des systèmes d'information partagés de santé.** Avis du conseil d'éthique et de déontologie de l'ASIP Santé sur les messageries contenant des données personnelles de santé. [En ligne] 25 octobre 2012. <http://esante.gouv.fr>.
105. —. Messagerie sécurisée de santé : présentation du service. Journée nationale des industriels. [En ligne] 15 novembre 2012. <http://esante.gouv.fr>.
106. Réunion de concertation sur les messageries sécurisées de santé. **Agence des systèmes d'information partagés de santé.** Paris : Maison de la chimie, 15 mai 2013. <http://esante.gouv.fr>.
107. **RIALLE Vincent.** *Technologies nouvelles susceptibles d'améliorer les pratiques gériatriques et la vie quotidienne des malades âgés et de leur famille.* [En ligne] mai 2007. <http://www.social-sante.gouv.fr>.
108. *Pharmagest fait bouger l'officine.* **Pharmacien Manager.** 104, février 2011.
109. *Les applications iphone de Plus Pharmacie illégales.* **Clausener, M.** 2012, Le moniteur des pharmacies 2917:10.
110. **BRAS Pierre-Louis, KIOU Abdelkrim - Inspection générale des affaires sociales.** Pharmacies d'officine : rémunération, missions, réseau. [En ligne] juin 2011. <http://www.ladocumentationfrancaise.fr>. Rapport n° RM2011-090P.
111. **Comité de liaison inter-ordres de santé.** Comment déployer la prescription électronique ? *Note d'orientation.* [En ligne] Janvier 2012. www.ordre.pharmacien.fr.
112. **STROETMANN Karl, ARTMANN Jörg, STROETMANN Veli, PROTTI Denos, DUMORTIER Jos, GIEST Sarah, WALOSSEK Uta, WHITEHOUSE Diane.** - eHealth Strategies Report. *European countries on their journey towards national ehealth infrastructures.* [En ligne] Janvier 2011. <http://www.ehealth-strategies.eu/report/>.
113. **Agence des systèmes d'information partagés de santé.** Focus sur le projet « Diraya », le système de santé électronique de l'Andalousie. [En ligne] 19 juin 2012. <http://esante.gouv.fr/le-mag-numero-3/focus-sur-le-projet-diraya-le-systeme-de-sante-electronique-de-l-andalousie>.
114. **DOUPI P., RENKO E., GIEST S., HEYWOOD J., DUMORTIER J.** - e-Health Strategies. *Country brief: Estonia.* [En ligne] Octobre 2010. <http://www.ehealth-strategies.eu>.
115. **Agence des systèmes d'information partagés de santé.** L'Allemagne ou le difficile déploiement de la e-santé à grande échelle. [En ligne] 12 avril 2013. <http://esante.gouv.fr/the-mag-issue-7/l-allemande-ou-le-difficile-deploiement-de-la-e-sante-a-grande-echelle>.
116. **DOUPI P., RENKO E., GIEST S., DUMORTIER J.** - eHealth Strategies. *Country brief: Denmark.* [En ligne] Octobre 2010. <http://www.ehealth-strategies.eu>.
117. —. eHealth Strategies. *Country brief: Sweden.* [En ligne] Octobre 2010. <http://www.ehealth-strategies.eu>.
118. **Agence des systèmes d'information partagés de santé.** En Estonie, la moitié de la population possède un dossier médical électronique. [En ligne] 15 novembre 2012.

- <http://esante.gouv.fr/the-mag-issue-5/en-estonie-la-moitie-de-la-population-possede-un-dossier-medical-electronique>.
119. —. Le projet européen epSOS. [En ligne] 19 juin 2012. <http://esante.gouv.fr/le-mag-numero-3/le-projet-europeen-epsos>.
120. **epSOS - European patients smart open services**. Le projet européen epSOS. [En ligne] www.epsos.eu/france/le-projet-epsos.html.
121. **epSOS - European patients smart open services**. Foire Aux Questions (FAQ). [En ligne] <http://www.epsos.eu/france/faq.html#c6502>.
122. **Commission nationale de l'informatique et des libertés**. Délibération n°2011-173 du 9 juin 2011 autorisant l'ASIP Santé à mettre en œuvre les traitements de données à caractère personnel nécessaires à la première phase d'expérimentation du projet pilote de e-santé, EPSOS. [En ligne] 2011. <http://www.legifrance.gouv.fr/>.
123. **epSOS - European patients smart open services**. Technical background. [En ligne] <http://www.epsos.eu/technical-background/systems-standards.html>.
124. **Agence des systèmes d'informaion partagés de santé**. Lancement du projet européen PALANTE. [En ligne] Avril 2012. <http://esante.gouv.fr/actus/politique-publique/lancement-du-projet-europeen-palante>.
125. **DOBREV Alexander, JONES Tom, VATTER Yvonne, PENG Kai, STROETMANN Karl, STROETMANN Veli** - EHR Impact, Socio-économique impact of interoperable electronic health record and ePrescription systems in Europe. [En ligne] 9 juillet 2009. <http://www.ehr-impact.eu>.
126. **Haute Autorité de santé** - Assises du médicament, groupe de travail N°4 : « Développer la formation et l'information sur les produits de santé ». Séance 5 : information à destination des professionnels de santé. [En ligne] 8 avril 2011. <http://www.sante.gouv.fr>.

Annexe 1 : Modèle de lettre de demande d'accès à son dossier médical informatisé :

Modèle de demande de droit d'accès à son dossier médical

Expéditeur :

Monsieur le Directeur
Service du droit d'accès
ADRESSE

Recommandée avec accusé de réception

Objet : Demande de droit d'accès à mon dossier médical

Madame, Monsieur,
Docteur (ou Monsieur le Directeur),

En application des dispositions de l'article 43 de la loi n° 78-17 du 6 janvier 1978 modifiée en août 2004, je vous prie de bien vouloir m'adresser l'ensemble des données dont vous disposez concernant ma santé, qu'elles soient sous forme papier ou sur support informatique (dans cette dernière hypothèse, avec indication de la signification des codes, sigles ou abréviations éventuellement utilisés).

Pour faciliter le traitement de ma demande, je vous précise que [à compléter]...

Je vous prie d'agréer, Docteur (Monsieur le Directeur), l'expression de mes salutations distinguées.

Signature :

MODÈLE DE DEMANDE DE DROIT D'ACCÈS À SON DOSSIER MÉDICAL

Annexe 2 : Modèle de note d'information des usagers relative au consentement à l'hébergement de données de santé à caractère personnel et au DMP.

A INSERER DANS UNE NOTE D'INFORMATION / LIVRET D'ACCUEIL

Vous êtes pris en charge par l'établissement _____. Dans ce cadre, des données de santé à caractère personnel vous concernant peuvent être hébergées à l'extérieur de l'établissement, par un hébergeur. Cet hébergeur dispose de l'agrément délivré par le ministre en charge de la Santé, en application des dispositions de l'article L.1111-8 du code de la Santé Publique et du décret n°2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé à caractère personnel.

Cet hébergement ne peut avoir lieu qu'avec votre consentement exprès ou celui de votre représentant légal (titulaire de l'autorité parentale pour un mineur, tuteur (rice) légal pour un majeur sous tutelle).

Ce consentement est dématérialisé (il est conservé dans le système informatique et non sous la forme d'un document papier) et son recueil est tracé (la date de votre consentement et l'identité de la personne qui le recueille sont également conservés).

La finalité de cet hébergement consiste à :

- Garantir la conservation, l'archivage et la sécurité des données de santé à caractère personnel,
- Assurer le respect des exigences de confidentialité, de sécurité et de pérennité de ces données.

Vous pouvez, conformément à la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés :

- accéder à vos données de santé à caractère personnel hébergées et en demander la rectification ;
- demander copie de l'historique des accès aux données de santé hébergées, des consultations ainsi que du contenu des informations consultées et des traitements éventuellement opérés.

Seuls les établissements et les professionnels de santé participant à votre prise en charge peuvent accéder aux données de santé hébergées, ainsi que le médecin présent chez l'hébergeur qui, comme le prévoit le code de la santé publique, est le garant de la confidentialité des données de santé à caractère personnel hébergées et veille au conditions d'accès à ces données dans le respect de la loi du 6 janvier 1978 modifiée et du code de la santé publique. Ses missions s'exercent dans le cadre de l'organisation prévue dans le contrat qui lie l'hébergeur au responsable du traitement et dans le cadre de l'exécution de son contrat de travail.

Pour exercer vos droits, vous pouvez vous adresser, par courrier ou par courriel, ou vous rendre directement:

- auprès du service « _____ » de l'établissement ou du professionnel de santé qui participe à votre prise en charge ;
- ou auprès du Médecin de l'Hébergeur ;
- ou _____ (A compléter le cas échéant).

A l'occasion de votre prise en charge, vous pouvez demander la création de votre DMP - ou elle vous sera proposée, afin de faciliter la coordination, la qualité et la continuité des soins entre les professionnels de santé qui vous soignent. Seuls les professionnels de santé que vous autorisez peuvent alimenter et/ou consulter votre DMP.

Votre consentement à la création de votre DMP est recueilli de façon dématérialisée et son recueil est tracé. Pour garantir leur confidentialité, les données de votre DMP sont stockées chez un hébergeur national, agréé pour l'hébergement de données de santé à caractère personnel. *(Pour plus d'informations, vous pouvez vous adresser aux professionnels de santé qui participent à la prise en charge ou consulter la brochure d'information du DMP le site dmp.gouv.fr.)*

Annexe 3 : Exemple d’affichette informative sur le traitement automatisé de données personnelles destinée aux pharmaciens d’officine (15):

Cette pharmacie est équipée d’un système informatique **destiné à** assurer sa gestion et la délivrance des médicaments (facturation, tiers-payant, suivi des remboursements, tenue de l’ordonnancier), ceci dans le **strict respect du secret professionnel** auquel sont astreints les pharmaciens.

Sauf opposition justifiée de votre part, certains renseignements vous concernant, recueillis sur la base de l’ordonnance qui vous a été délivrée, de votre carte d’assuré social ainsi que, le cas échéant, de votre carte d’assurance maladie complémentaire (mutuelle ou assurance), feront donc l’objet d’un enregistrement informatique.

L’usage en est exclusivement réservé, dans la limite de leurs attributions, à votre pharmacien, votre caisse de sécurité sociale, votre organisme d’assurance complémentaire.

Ces données pourront être traitées, de façon totalement anonyme, à des fins statistiques professionnelles.

Conformément aux dispositions de la loi informatique et libertés*, **vous pouvez obtenir communication** auprès de cette pharmacie **des informations vous concernant et, le cas échéant, en demander la modification.**

* Loi n°78-17 du 6 janvier 1978 modifiée en 2004 relative à l’informatique, aux fichiers et aux libertés

Annexe 4 : Organisation et modalités d'accès aux données contenues dans les volets de la carte Vitale (25):

DONNEES DE LA CARTE VITER	LECTURE	ECRITURE
Volet mapping		
Version mapping : cette zone contient des informations techniques concernant la version du mapping.	Libre	Protégée (réservée pour les AMO)
Volet Administration carte		
Zone optionnelle contenant la date de fin de validité de la carte.	Libre	Protégée (réservée pour les AMO)
Volet famille		
Unique pour tous les bénéficiaires, elle contient les éléments de droits AMO pour l'ensemble de la famille, notamment le matricule de l'assuré	Libre	Protégée (réservée pour les AMO)
Nom de famille Zone adresse	Libre	Protégée (réservée pour les AMO)
Zone services AMO : zone optionnelle de niveau famille (dont les données sont valables pour l'ensemble des bénéficiaires portés sur la carte)	Libre	Protégée (réservée pour les AMO)
Volet ETM famille		
Zone optionnelle, elle contient les informations de couverture AMO particulière (Exonération du Ticket Modérateur ETM) dont bénéficie l'ensemble des membres de la famille	Réservée aux professionnels de santé, établissements de santé et aux agents des organismes d'AMO	Protégée (réservée pour les AMO)
Volet bénéficiaire		
Propre à chaque bénéficiaire, elle contient son identification, ainsi que des informations de couverture AMO particulière dont il bénéficie.	Libre	Protégée (réservée pour les AMO)
Exonération du Ticket Modérateur (ETM)	Réservée aux professionnels de santé, établissements de santé et aux agents des organismes d'AMO	Protégée (réservée pour les AMO)
NIR du bénéficiaire	Libre	Protégée (réservée pour les AMO)
Complément ETM : zone optionnelle, contient des précisions sur les ETM bénéficiaires. Cette zone complète la zone d'information ETM contenues dans la zone bénéficiaire	Réservée aux professionnels de santé, établissements de santé et aux agents des organismes d'AMO	Protégée (réservée pour les AMO)
Zone services AMO : zone optionnelle de niveau bénéficiaire (propre à un ayant-droit donné porté sur la carte)	Libre	Protégée (réservée pour les AMO)
Volet mutuelle (par complémentaire gérée par AMO)		
Zone optionnelle, propre à chaque bénéficiaire, elle contient ses informations de couverture AMC dans le cas d'une gestion unique.	Libre	Protégée
Volet AMC (par complémentaire gérée par un organisme d'AMC)		
Zone optionnelle propre à chaque bénéficiaire, contient les informations spécifiques au contrat d'AMC	Libre	Protégée
Volet complémentaire (en complément du Volet mutuelle ou volet AMC)		
Zone commune complémentaire	Libre	Protégée (réservée pour les AMO ou les AMC selon le cas)

Volet Transcard (par famille)		
Zone optionnelle, zone spécifique pour expérimentation	Libre	Protégée (réservée pour les AMO)
Volet Netlink		
Zone optionnelle, zone spécifique propre à chaque bénéficiaire pour expérimentation	Libre	Protégée (réservée pour les AMO)
Volet AT		
Zone optionnelle portant les informations nécessaires pour gérer un accident du travail	Libre	Peut être utilisée par un organisme gestionnaire des AT qui n'est pas forcément le gestionnaire maladie.
Volet E111		
Zone optionnelle portant les informations nécessaires à l'édition d'un formulaire européen E 111.	Libre	Protégée (réservée pour les AMO)
Volet E112		
Zone optionnelle portant les informations nécessaires à l'édition d'un formulaire européen E 112.	Libre	Protégée (réservée pour les AMO)
Volet E128		
Zone optionnelle portant les informations nécessaires à l'édition d'un formulaire européen E 128.	Libre	Protégée (réservée pour les AMO)

Annexe 5 : Contenu des certificats X509 de classe 1, d'authentification et de signature électronique des cartes CPS (69)

Objet	Format	Certificat clé de signature d'une CPS et CPF	Certificat clé d'authentification d'une CPS et CPF
Certificate	Sequence		
TbsCertificate	Sequence		
version	Integer	2 (version 3)	
serialNumber	Integer	n° de certificat	
signature	OID	Sha-1WithRSAEncryption	
Issuer	PrintString	C=FR,O=GIP-CPS, OU=GIP-CPS PROFESSIONNEL, CN=GIP-CPS CLASSE-1	
validity	UTC-Time	NotBefore : date début de validité carte NotAfter : date fin de validité carte + 1 mois	NotBefore : date début de validité carte NotAfter : date fin de validité carte
subject	PrintString T61String PrintString T61String T61String	C=FR,O=GIP-CPS, OU= « nom de la (future) profession », CN= « PS_IdNat », SN= « nom d'exercice », GN= « prénom usuel »	
subjectPublicKeyInfo	Sequence		
algorithmIdentifier	OID	RSAEncryption (Parameter = NULL)	RSAEncryption (Parameter = NULL)
subjectPublicKey	BitString	clé publique de 2.048 bits + exp. pub. (=2E16+1)	clé publique de 1.024 bits + exp. pub. (=2E16+1)
extensions	Sequence		
authorityKeyId	OctString	« SHA1 KP "ACI CLASSE-1" (certSign) »	
subjectKeyId	OctString	« SHA1 subjectPublicKey »	
keyUsage	Sequence		
critical	Boolean	true	true
value	BitString	'C0' : digitalSignature & nonRepudiation	'80' : digitalSignature (clé d'authentification)
extKeyUsage value(s)	Sequence OID	id-kp-emailProtection	id-kp-clientauth si CPS3 : + szoid_kp_smartcard_logon
privateKeyUsagePeriod	GenTime	NotBefore : date début de validité carte NotAfter : date fin de validité carte	objet absent
certificatePolicies	Sequence		
certPolicyId	OID	{ id-gip-icp-doc-pc2004-exploit 1 1 2 1 }	{ id-gip-icp-doc-pc2004-exploit 1 1 1 1 }
basicConstraints	Sequence	Séquence vide – non-critique	
crlDistributionPoint	Sequence	« http://annuaire.gip-cps.fr/crl/gip-cps-professionnel/classe-1.crl » « ldap://annuaire.gip-cps.fr/cn=gip-cps classe-1,ou=gip-cps professionnel,o=gip-cps,c=fr ?certificaterevocationlist,binary »	
freshestCrl	Sequence	« ldap://annuaire.gip-cps.fr/cn=gip-cps classe-1,ou=gip-cps professionnel,o=gip-cps,c=fr ?deltarevocationlist,binary »	
subjectAltName	Sequence	objet absent	LogonNT (UPN - UserPrincipalName)
netscapeCertType	BitString	'20' : client S/MIME	'80' : client SSL
gipCardID	PrintString	issuerID "/" cardserialnumber	
gipCardCategory	OctString	'00' (Carte PS)	
gipCardType	Integer	'00' si CPS '01' si CPF	
gipProfessionCode	Integer	« code de la profession »	- que pour les CPS
gipFutureProfessionCode	Integer	« code de la future profession »	- que pour les CPF
gipOldIDNatPS	PrintString	Ancien « PS_IdNat »	- optionnel - que pour les CPS
gipSpecialiteRPPS	Sequence	Liste des spécialités RPPS	- optionnelle - que pour les CPS Médecins et Chirurgiens dentistes
gipTableauPharmacien	Sequence	Liste des tableaux pharmacien	- optionnelle - que pour les CPS Pharmaciens
signatureAlgorithm	OID	Sha-1WithRSAEncryption	
signatureValue	BitString	Signature du certificat, calculée avec la clé privée "ACI CLASSE-1" (certSign)	

Annexe 6 : Groupes de la zone d'échange d'une FSE couramment utilisés par les pharmaciens (25) :

TYPE DE GROUPE	CONTENU
Groupe <i>identification facture</i> (1110)	Numéro de facture, date de facturation, nature de l'opération
Groupe <i>identification du professionnel de santé</i> (1120)	N° d'identification de facturation et sa clé N° RPPS et sa clé Nom, prénom du PS Code spécialité, code conventionnel
Groupe <i>identification du bénéficiaire</i> (1130)	N° national d'immatriculation NIR assuré et sa clé Date de naissance, rang de naissance Qualité, code couverture
Groupe <i>identification structure</i> (1140) Facultatif	Nom, type et numéro d'identification de la structure
Groupe <i>identification remplaçant</i> (1150)	Ce groupe identifie le professionnel de santé qui exécute les prestations et signe la feuille de soins électronique dans le cas d'un remplacement, il est obligatoire en cas de remplacement. N° d'identification de facturation et sa clé Nom, prénom du PS Indicateur de signature (indique que la facture est élaborée par un remplaçant)
Groupe <i>liste d'opposition carte Vitale</i> (1170)	Cette information est à prendre dans l'en-tête du fichier de la liste d'opposition.
Groupe <i>Organismes AMO</i> (1310)	- code régime Cf. fonction « Lire Droits Vitale » du module SSV - Caisse gestionnaire et centre gestionnaire Cf. fonction « Lire Droits Vitale » du module SSV - code organisme destinataire et code centre informatique
Groupe <i>Organismes AMC</i>(1321) optionnel	-Type de contrat, numéro de l'organisme complémentaire, le numéro d'adhérent, données de la complémentaire...
Groupe <i>Données complémentaires additionnelles</i> (1330)	N° AMC ou n° de l'opérateur de règlement et contexte conventionnel
Groupe <i>cadre de remboursement</i> (1410)	Informations sur l'application du tiers-payant sur les parts AMO et AMC
Groupe <i>identification de pièce justificative pour l'AMO</i> (1420)	Nature de la pièce justificative (aucune, attestation papier, carte Vitale, autre...) Date de validité Origine de la pièce justificative (code l'organisme l'ayant délivrée)
Groupe <i>nature d'assurance</i> (151X)	Ensemble d'informations permettant d'indiquer à l'assurance maladie si les prestations indiquées sur la feuille de soins relèvent du risque maladie, maternité, accident du travail, prévention ou du contexte Soins Médicaux Gratuits

Groupe <i>prestation</i> (1610)	Les informations télétransmises reflètent exactement la facturation des actes retranscrite sur le support papier. Il est donc nécessaire de créer autant de groupes 1610 que d'actes répertoriés sur la feuille de soins. Une prestation concernant la famille pharmaciens (groupe 1610) ne peut inclure à la fois des codes médicaments (groupes 1740 et 1741) et des codes LPP (1730). Pour les médicaments : On établit un groupe <i>1610 Prestation</i> par code prestation de groupe fonctionnel « Médicament » (cf. annexe2-Table1). Pour les prestations admettant le codage (top codage affiné = oui, cf. annexe2-Table1), ce groupe 1610 est suivi d'un groupe 1740 « <i>Prestation détaillée code CIP</i> », lui-même éventuellement suivi de 1 à 30 groupes 1741 « <i>Prestation détaillée lot d'un code CIP</i> » pour identifier les numéros de lot et de série des conditionnements de médicaments délivrés. Le prix unitaire du groupe 1610 correspond au montant de la prestation, à savoir : • le prix unitaire de la boîte de médicament délivré multiplié par le nombre de boîtes délivrées (multiplication du champ 1740-4 par le champ 1740-5) • ou bien, en cas de déconditionnement, le prix de l'unité multiplié par le nombre d'unités délivrées. (multiplication du champ 1740-10 multiplié par le champ 1740-9) La valeur du dénombrement du groupe 1610 demeure 1. Spécificité : LPP Pour les Dispositifs médicaux (DM) de la LPP (anciennement TIPS) : Pour chaque code prestation de type de nomenclature LPP (cf. annexe2-Table1), on établit un groupe <i>1610 Prestation</i>. Ce groupe 1610 est suivi de 1 à 10 groupes <i>1730 Prestation détaillée</i>. Cas particulier : En nature d'assurance SMG, ce groupe 1610 est nécessairement suivi d'un et un seul groupe 1730 <i>Prestation détaillée</i>. Le prix unitaire du groupe 1610 est renseigné par la somme des « montants de la LPP » identifiés dans les groupes 1730 qui s'y rattachent. La base de remboursement du groupe 1610 est renseignée par la somme des « montants totaux de la LPP » identifiés dans les groupes 1730 qui s'y rattachent. La valeur du dénombrement du groupe 1610 correspond au nombre de groupe 1730 qui s'y rattache. Dans le cas d'une location, la date d'exécution de la prestation
---	--

	(1610) = Date de début de location (1730) Numéro d'ordre de la prestation Date d'exécution de la prestation Code prestation Montant des honoraires et qualificatif de la dépense Quantité, dénombrement, prix unitaire Base de remboursement, taux applicable et montant remboursable par l'AMO et l'AMC.
Groupe prestation détaillée LPP (1730)	Numéro d'ordre de la prestation Code LPP associé à la prestation Type de prestation (achat, location, entretien...) Date de début de location ou date d'achat ou de délivrance Date de fin de location ou de service Tarif de référence, prix unitaire, nombre d'unités, montant total facturé
Groupe prestation détaillée code CIP (1740)	Numéro d'ordre de la prestation Type de code CIP (CIP7 ou CIP13) Code CIP Prix unitaire (base de remboursement d'un conditionnement), quantité délivrée (nombre de conditionnements) Indicateur du médicament délivré (médicament n'appartenant pas à un groupe générique, générique soumis ou non au TFR, référent du groupe générique soumis ou non au TFR). Indicateur de substitution (substitution pour urgence ou accord du prescripteur, ou refus de substitution) Informations sur un éventuel déconditionnement (prix unitaire, quantité...) Mode de prescription : Mention non substituable
Groupe prestation détaillée lot d'un code CIP (1741)	Permet d'identifier les numéros de lot et éventuellement les numéros de série des conditionnements délivrés ou utilisés (cas du déconditionnement).
Groupe complément de prestation, Exonération TM (1820)	Informations sur certains modes de prise en charge, régimes spéciaux (SNCF, Mines...) l'ALD, soins particulier (traitement de la stérilité, soins aux prématurés...)
Groupe complément de prestation renouvellement (1850)	Indique le numéro d'ordre de renouvellement
Groupe Total facture (1910)	Nombre de prestations (groupes 16XX) Total des montants facturés Total remboursable par l'AMO Total remboursable par l'AMC Total participation de l'assuré

Annexe 7 : Codification des fichiers de télétransmission des factures électroniques à la Norme B2/PH

Codification du fichier		
Type 000	DEBUT DE FICHIER	- Type d'émetteur : - Valeur TP si transmission par partenaire de santé autre qu'établissement - Valeur OT si transmission entre un OCT et l'organisme d'AM - N° d'émetteur : - N° national d'identification et clé si l'émetteur est un partenaire de santé (TP) - n° SIRET en SESAM ou SESAM dégradé, n° attribué par l'organisme d'AM ou n° SIREN en B2 si l'émetteur est de type OT - Type de destinataire : Codification du cahier des charges norme B2 (ex CP pour CPAM, MA pour MSA...) - N° de destinataire : Code grand régime du cahier des charges norme B2 - Date de réception du flux sur le frontal : AAMMJJ - Application : Valeur TO pour les flux transitant par un OCT. Sinon valeur TR - Identification du fichier : Nom du fichier transmis, attribué par l'émetteur. Alphabétique ou numérique, sans caractère spécial, unique pour chaque fichier - Date de création du fichier : AAMMJJ - Norme utilisée : Valeur PH pour la pharmacie - Version de la norme : Valeur B2
		- Volume du Fichier : Totalisation de l'envoi. Nombre total d'enregistrements à transmettre. - Nombre total de lots contenus dans le fichier.
Type 999	FIN DE	

Codification du lot de factures		
Type 1	DEBUT DE LOT	- Identification du partenaire de santé : N° ADELI + clé et vérification de la clé, Nom - N° d'organisme Destinataire auquel est adressé le lot de factures. - N° de lot : Attribué par le partenaire de santé. Il caractérise l'ensemble des factures transmises à une caisse. Pour une même caisse, ce N° doit être différent d'un lot à l'autre. - Identification de la norme : Code type = B2, Code norme = PH, Code version = 062007 - Date de création du lot : AAMMJJ - Certification du lot : Blanc = B2 non sécurisée, non chiffrée. S = SESAM avec Vitale, sécurisé, chiffré. F = SESAM sans Vitale, sécurisé, chiffré. D = SESAM dégradé, chiffré avec CPS, sans Vitale. - Unité monétaire de facturation : U pour monnaie Unique : tous les montants sont exprimés en euros.

Type 6	FIN DE LOT	- Nombres de factures :	Nombre d'enregistrements de type 2, 2A, et 5 transmis sous le même numéro de lot. (même partenaire de santé – même organisme).
		- Nombre de lignes actes :	Nombre d'enregistrements de type 3, 4, 4A, pour l'ensemble des factures transmises sous un même numéro de lot.
		- Montant total général du lot prestations facturées	pour toutes les factures du lot
		- Montant total général du lot prestations remboursables par l'organisme d'AM	pour toutes les factures du lot
		- Montant total général du lot prestations remboursables par les organismes complémentaires	pour toutes les factures du lot
		- Type de facture :	Hors SESAM : à blanc SESAM et SESAM dégradé : valeur F
		- N° d'agrément du progiciel de facturation :	Fourni par le CNDA
		- N° d'identification du PS signataire	
Codification de la facture			
Types 2 et 2A	DEBUT DE FACTURE	- N° immatriculation assuré et sa clé, date et rang de naissance du bénéficiaire	
		- N° de facture, date de facturation, la nature de l'opération	
		- Type de facture :	SESAM sécurisée, SESAM dégradée ou hors SESAM
		- Modalités d'éclatement des flux	de FSE et de DRE par le PS
		- Code du grand régime et numéros de caisse et de centre gestionnaires	
		- Nature des pièces justificatives	des droits AMO et AMC
		- Numéro de prescripteur et sa clé	
		- La date de prescription :	AAMMJJ
		- La nature de l'assurance :	Maladie, maternité, AT...
		- Justification d'exonération ou de modulation du ticket modérateur	
		- Destinataire du règlement :	- Hors Tiers Payant = règlement à l'assuré, - Tiers Payant sur la part obligatoire seule (y compris le cas d'exonération du Ticket Modérateur) : règlement au partenaire de santé. - Tiers Payant Intégral (part RO+RC) : règlement au partenaire de santé. - Tiers Payant sur la part complémentaire seule : règlement au partenaire de santé
		- N° d'organisme complémentaire	
		- N° d'adhérent à un organisme complémentaire et type de contrat souscrit	

TYPE 2n	SUIVE DU DEBUT DE	- Si n= S, Type 2S : permet de véhiculer des informations supplémentaires de niveau début de facture comme les informations liées au choix d'un médecin traitant (non utile pour le pharmacien), la date de référence de la liste d'opposition Vitale utilisée lors de l'élaboration de la facture. Si n=M ou n= P, Types 2M et 2P: permettent de véhiculer des données relatives à la gestion de la part complémentaire (Identifiants, codes...) Si n=E, Type 2E : permet de véhiculer des informations supplémentaires de niveau facture, relatives à l'identification des PS et des structures telles que l'identifiant RPPS du prescripteur, le n° de la structure dans laquelle le PS a prescrit (n° SIRET ou FINESS)
TYPES 4 ET 4A	LIGNE DE FACTURE	- Séquence de Renouvellement : N° d'ordre du renouvellement (00, 01, 02...) - Date de dispensation du produit (ou de début de location) : AAMMJJ - Quantités d'actes : Une valeur > 1 peut être acceptée si au cours d'une même journée, un acte identique (même coefficient, même lettre clé, même code complément d'acte) prescrit par un même prescripteur a été réalisé par un même exécutant - Dénombrement LPP : Nombres de type 4F - Prix unitaire : Montant, en centimes, de l'unité tarifaire (lettre clé) au tarif conventionnel. Pharmaciens : indiquer le résultat de l'opération : Quantité x PU du type 4P ou en cas de déconditionnement : quantité d'unités x PU de l'unité du type 4P - Base de remboursement - Montants remboursables par l'organisme d'assurance maladie et complémentaire - Qualificatif de la dépense
TYPES 4S ET 4E	SUIVE LIGNE DE	Type 4S : permet de véhiculer des informations supplémentaires de niveau ligne hors codage, quelle que soit la norme utilisée comme les conditions d'exercice de l'exécutant. Type 4E : permet de véhiculer des informations supplémentaires de niveau ligne, notamment les nouvelles identifications des PS et des structures.

Type 4P

Obligatoire pour la délivrance de la pharmacie codée avec code CIP à 7 ou 13 caractères

- **Mode de Prescription :** mention du Médecin sur la prescription « non substituable »
- **Indicateur de substitution :** Substitution pour Urgence ou Accord du médecin (de Générique à Générique, de Générique à Réfèrent ou de Réfèrent à Générique)
- **Types du code CIP du médicament prescrit et du médicament délivré :** 7 ou 13 caractères
- **Codes CIP du médicament prescrit et du médicament délivré**
- **Indicateur du médicament délivré :** Générique soumis ou non au TFR, référent du groupe générique soumis ou non au TFR ou bien médicament n'appartenant pas à un groupe générique
- **Quantité de conditionnements délivrés :** Quantité de conditionnements délivrés pour ce code CIP.
- **Prix unitaire du conditionnement Délivré**
- **Modalités et tarification des médicaments dispensés après déconditionnement :** si le médicament est déconditionné. Dans ce cas, la facturation de ce médicament est entièrement effectuée en unités.

Type 4R

Permet de véhiculer des informations supplémentaires de niveau affiné

- **N° de lot du conditionnement**
- **Quantité de conditionnement appartenant au même lot**
- **Numéro de série du conditionnement délivré**

Type 4F

Obligatoire dans la norme fournisseurs pour identifier les produits de la LPP avec le codage.

- **Code de la LPP associé à 7 caractères**
- **Type de prestation fournie A (achat, location...)**
- **N° SIRET du fabricant**
- **Date début de location ou date d'achat ou de délivrance :** En cas de facturation partielle d'une location, la date de début de location correspond à la date de début de facturation de la période concernée.
- **Date de fin de location ou de service :** En cas de facturation partielle d'une location, la date de fin de location correspond à la date de fin de facturation de la période concernée. En cas de changement de tarif en cours de période, indiquer une fin de période à la date de fin de l'ancien tarif et finir la période avec le nouveau tarif
- **Nombre d'unités :** Indique le nombre de fois où l'article est facturé. Correspond pour les locations au nombre de jours, semaines ou mois facturés.
- **Tarif de référence et prix unitaire de vente ou de location**
- **Base de remboursement :** Tarif de référence LPP x nombre d'unité
- **Montant total facturé :** Prix unitaire de vente x nombre d'unités

TYPE 5	FIN DE FACTURE	- Nombre d'enregistrement de Type 4 - Total des montants Facturés dépassement compris - Total remboursable par la Caisse d'AM - Total participation assuré avant participation de l'organisme complémentaire : Résultat de l'opération Total montants facturés - Total remboursable par la caisse - Total remboursable par l'organisme complémentaire - Top éclatement des flux par l'OCT : Valeur « A » : il y a eu éclatement des flux par un OCT, Valeur blanc : il n'y a pas eu d'éclatement, ni de demande de remboursement AMC. Autres valeurs : remboursement de la part AMO et AMC par l'AMO : indiquer la nature de la pièce justificative des droits AMC.
--------	----------------	--

Annexe 8 : Mandat de télé-déclaration de mise en œuvre du dossier pharmaceutique par une officine.

CONSEIL NATIONAL DE L'ORDRE DES PHARMACIENS MANDAT DE TELE-DECLARATION										
Je soussigné (e) : Nom : Prénom : Pharmacien titulaire de l'officine : Etablie à l'adresse : CP : Ville : Code APE : Téléphone : Fax :	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 80%; height: 15px;"></td> <td rowspan="8" style="width: 20%; text-align: center; vertical-align: middle; font-weight: bold;">A VERIFIER</td> </tr> <tr><td style="height: 15px;"></td></tr> <tr><td style="height: 15px;"></td></tr> <tr><td style="height: 15px;"></td></tr> <tr><td style="height: 15px;"></td></tr> <tr><td style="height: 15px;"></td></tr> <tr><td style="height: 15px;"></td></tr> <tr><td style="height: 15px;"></td></tr> </table>		A VERIFIER							
	A VERIFIER									
Le Contact Dossier Pharmaceutique au sein de l'officine est : Nom : Prénom : Téléphone : Fax : N° SIRET pharmacie : Adresse électronique du contact : Adresse électronique de l'officine : Au sein de mon officine, les données traitées concernent environ Le logiciel de gestion d'officine utilisé est	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 80%; height: 15px;"></td> <td rowspan="8" style="width: 20%; text-align: center; vertical-align: middle; font-weight: bold;">A COMPLETER</td> </tr> <tr><td style="height: 15px;"></td></tr> <tr><td style="height: 15px;"></td></tr> <tr><td style="height: 15px;"></td></tr> <tr><td style="height: 15px;"></td></tr> <tr><td style="height: 15px;"></td></tr> <tr><td style="height: 15px;"></td></tr> <tr><td style="height: 15px;"></td></tr> </table>		A COMPLETER							
	A COMPLETER									
☒ En cochant cette case j'accepte que l'adresse électronique communiquée à CELTIPHARM dans le cadre du présent mandat soit communiquée au CNOP afin que celui-ci puisse m'adresser tout document lié au Dossier Pharmaceutique. Autorise la société CELTIPHARM, ayant son siège social 3, Allée Nicolas Le Blanc, 56000 VANNES, immatriculée au Registre du commerce et des sociétés de Vannes sous le numéro B 327 350 321, à réaliser pour mon compte, auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL), les formalités préalables imposées par la loi n° 78-17 relative à l'informatique, aux fichiers et libertés, à savoir, en l'espèce, une télé-déclaration conforme à la norme simplifiée n° 52. Je déclare avoir pris connaissance de la délibération de la CNIL n°2006-161 du 8 juin 2006 portant adoption d'une norme simplifiée relative aux traitements automatisés de données à caractère personnel mis en œuvre par les pharmaciens à des fins de gestion de la pharmacie. Je certifie que les traitements de données à caractère personnel réalisés dans mon officine sont en tous points conformes aux dispositions de la norme simplifiée n° 52 précitée. A la suite de cette télé-déclaration, je recevrais de la CNIL à l'adresse électronique susmentionnée, le récépissé de déclaration de conformité à une norme simplifiée, que je m'engage à conserver. Par ce document, vous autorisez Marie-Pierre DANIEL, correspondant CNIL, à effectuer pour vous votre télé-déclaration. A ce titre, son nom apparaîtra sur le récépissé que vous recevrez de la CNIL.										
Pour faire valoir ce que de droit. Fait à _____, le ____/____/____ A RENVoyer AU PLUS VITE PAR FAX AU 0800 71 80 71 DOC-CNOP D90402-CNO Mandat Télédéclaration_LK.doc	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 80%; height: 15px;"></td> <td rowspan="2" style="width: 20%; text-align: center; vertical-align: middle; font-weight: bold;">A SIGNER</td> </tr> <tr> <td style="height: 15px;"></td> </tr> </table>		A SIGNER							
	A SIGNER									

ATTESTATION DE CREATION D'UN DOSSIER PHARMACEUTIQUE

Pour :

Nom et prénoms du (de la) patient(e) :

Né(e) le :

Adresse :

.....

Je, soussigné(e) :

Pharmacien :

.....

déclare que :

1) J'ai remis à la personne désignée ci-dessus⁽¹⁾ la brochure d'information relative au Dossier pharmaceutique.

2) Elle reconnaît avoir pris connaissance de cette brochure et être informée de l'ensemble de ses droits.

3) J'ai recueilli son consentement pour qu'un Dossier pharmaceutique soit créé à son nom. Elle accepte que ce dossier soit hébergé par Santeos, désigné par le Conseil national de l'Ordre des pharmaciens, conformément à l'article L. 1111-8 du code de la santé publique.

4) J'ai créé pour elle ce Dossier et je lui ai remis un exemplaire de la présente attestation.

En cochant la case ci-après, je certifie l'exactitude de cette déclaration ☒

Fait à :

Le (date) :

⁽¹⁾ ou, pour un mineur âgé de moins de 16 ans ou majeur sous tutelle, à son représentant légal, qui a justifié de son identité :

Nom et prénoms du représentant légal :

Qualité (père, mère, tuteur) :

Adresse, si elle est différente de celle du (de la) patient(e) :

.....

DP-ACRE-060620

**ATTESTATION
DE REFUS D'ALIMENTATION
D'UN DOSSIER PHARMACEUTIQUE**

Pour :

Nom et prénoms du (de la) patient(e) :

Adresse :

.....

Je, soussigné(e) :

Pharmacien :

.....

déclare que :

1) La personne désignée ci-dessus⁽¹⁾ m'a fait connaître son opposition à ce que j'inscrive dans le Dossier pharmaceutique établi à son nom certains médicaments que je lui ai délivrés ce jour.

2) Je l'ai informée que cette décision ne me permettra pas d'assurer une analyse pharmaceutique complète de ses traitements.

3) Je lui ai indiqué que son Dossier pharmaceutique portera pendant quatre mois la mention « dossier incomplet ».

4) Je lui ai remis un exemplaire de la présente attestation.

En cochant la case ci-après, je certifie l'exactitude de cette déclaration ☒

Fait à :

Le (date) :

⁽¹⁾ ou, pour un mineur âgé de moins de 16 ans ou majeur sous tutelle, à son représentant légal, qui a justifié de son identité :

Nom et prénoms du représentant légal :

Qualité (père, mère, tuteur) :

Adresse, si elle est différente de celle du (de la) patient(e) :

.....

DP-A-RAL-080731

**ATTESTATION
DE REFUS DE CONSULTATION
D'UN DOSSIER PHARMACEUTIQUE**

Pour :

Nom et prénom du (de la) patient(e) :

Adresse :

.....

Je, soussigné(e) :

Pharmacien :

.....

déclare que :

1) La personne désignée ci-dessus⁽¹⁾ m'a fait connaître ce jour son opposition à ce que je consulte le Dossier pharmaceutique établi à son nom.

2) Je l'ai informée que cette décision ne me permettra pas d'effectuer une analyse pharmaceutique complète de ses traitements.

3) Je lui ai indiqué que son Dossier pharmaceutique mentionnera qu'elle a exercé son droit de refus de consultation.

4) Je lui ai remis un exemplaire de la présente attestation.

En cochant la case ci-après, je certifie l'exactitude de cette déclaration ☒

Fait à :

Le (date) :

⁽¹⁾ ou, pour un mineur âgé de moins de 16 ans ou majeur sous tutelle, à son représentant légal, qui a justifié de son identité :

Nom et prénom du représentant légal :

Qualité (père, mère, tuteur) :

Adresse, si elle est différente de celle du (de la) patient(e) :

.....

DP-A RCD-060519

DOSSIER PHARMACEUTIQUE DEMANDE DE DROIT D'ACCÈS

Seul le titulaire du Dossier pharmaceutique dûment identifié peut demander un droit d'accès.

L'identification du patient est obligatoirement réalisée au moyen de la présentation d'un titre d'identité comportant la photographie du patient (carte d'identité, passeport, permis de conduire).

Je, soussigné(e) :

Nom :

Prénom :

Adresse :

.....

né(e) le à

Je souhaite faire valoir mon droit d'accès sur les éléments contenus du Dossier pharmaceutique me concernant.

J'ai bien pris note de ce que :

- ce droit d'accès est strictement personnel et s'inscrit dans le strict respect du droit d'accès prévu par l'article 39 de la loi n° 78-17 relative à l'informatique aux fichiers et aux libertés ;
- l'accès sera formalisé par la remise, dans l'officine, de la version papier des quatre derniers mois d'historique du Dossier pharmaceutique qui me concerne ;
- les données qui font l'objet d'accès sont les informations relatives à l'identité du patient, les noms des médicaments délivrés, ainsi que les quantités et dates de dispensation à l'exclusion de toute autre information ;
- l'officine est en droit de me demander de payer une somme qui ne peut excéder le coût de la reproduction ;
- à compter de la remise du Dossier pharmaceutique qui me concerne, je demeure seul responsable de son utilisation et de sa conservation.

Fait à, le

Si le patient souhaite que l'historique soit remis à un tiers, il devra aussi remplir le mandat type prévu à cet effet, et le remettre à la personne concernée avec le présent document. La copie du Dossier pharmaceutique sera remise à ce tiers sous pli fermé.

Annexe 13 : Attestation de clôture d'un dossier pharmaceutique remise au patient.

**ATTESTATION DE CLÔTURE
D'UN DOSSIER PHARMACEUTIQUE**

Pour :

Nom et prénoms du (de la) patient(e) :

Né(e) le :

Adresse :

.....

Je, soussigné(e) :

Pharmacie :

.....

déclare que :

1) A la demande de la personne désignée ci-dessus⁽¹⁾, j'ai clos ce jour le Dossier pharmaceutique établi à son nom.

2) Cette opération a été effectuée immédiatement par l'hébergeur de ce Dossier, Santeos SA. Elle entraîne l'effacement total et définitif de toutes les données contenues dans le Dossier.

3) La personne conserve le droit, si elle le souhaite, de demander la création d'un nouveau Dossier pharmaceutique.

4) Je lui ai remis un exemplaire de la présente attestation.

En cochant la case ci-après, je certifie l'exactitude de cette déclaration ☒

Fait à :

Le (date) :

⁽¹⁾ ou, pour un mineur âgé de moins de 18 ans ou majeur sous tutelle, à son représentant légal, qui a justifié de son identité :

Nom et prénoms du représentant légal :

Qualité (père, mère, tuteur) :

Adresse, si elle est différente de celle du (de la) patient(e) :

.....

DP-A.CLO-080820

Annexe 14 : Modèle d'ordonnance sécurisée.

1 Docteur DUPONT François
 5 rue des cerises
 75000 Paris
 Cabinet : 01 42 42 42 42
 Médecine générale
 49 1 5555 22

2 04 janvier 2010

3 Madame DURAND Elise Marie
 50 ans

4 Spécialité stupéfiant X
 Une gélule de soixante milligrammes matin et soir pendant 28 jours

5 Dupont

6 9B12345

7 1

- 1 Informations prescripteur**
 Nom - prénom - Qualité
 Qualification, titre ou spécialité
 Adresse
 Si ordonnance hospitalière, le nom de l'établissement ou du service de santé
 Numéro RPPS ou par défaut numéro Adeli
- 2 Date de rédaction de l'ordonnance**
- 3 Informations patient**
 Nom - Prénoms - Sexe - Age
 Taille et poids si nécessaire
- 4 Informations prescription**
 - Dénomination du médicament
 - En toutes lettres :
 - nombre d'unités thérapeutiques de prise,
 - nombre de prises,
 - dosage
 - Durée du traitement ou nombre d'unité de conditionnement.
- 5 Signature du prescripteur**
 immédiatement sous la dernière ligne de la prescription
- 6 Numéro d'identification du lot d'ordonnances**
- 7 Nombre de spécialités prescrites**

Source : Meddispar (<http://www.meddispar.fr>)

Identification du prescripteur N° 14465*01	Identification de la structure LEDRQWPLDONGNPLEJCHVHC-NEDCNMP LQBNQ \$0), 1(66 EX 65(T
Identification du patient (nom de famille (de naissance) suivi du nom d'usage facultatif et celui à l'échelle de la commune pour les étrangers) Q GIP PIMDEXIARQ ; FRPS@MUSIDU MTS H	
Prescriptions relatives au traitement de l'affection de longue durée reconnue (liste ou liste réduite) (AFFECTION ENONERANTE)	
Prescriptions SANSRAPPORT avec l'affection de longue durée (MALADIES INTERCURRENTES)	

Quiconque se rend coupable de fraude ou de fausse déclaration est passible de pénalités financières, d'amende et/ou d'emprisonnement (articles 313-1, 441-1 et 441-6 du Code pénal, articles L. 114-13 et L. 162-1-14 du Code de la sécurité sociale).

Annexe 16 : Modèle d'ordonnance de médicament d'exception.

cerfa
n° 12708*02

ordonnance de médicaments, de produits ou de prestations d'exception

article R. 163-2, 3ème alinéa et R. 165-1 dernier alinéa du Code de la sécurité sociale
article L. 115 du Code des pensions militaires d'invalidité et des victimes de guerre

VOLET 1
à conserver
par l'assuré(e)

personne recevant les soins et assuré(e) (voir notice au verso du volet 1)

personne recevant les soins (la ligne "nom et prénom" est obligatoirement remplie par le médecin)

nom et prénom _____
(nom de famille (de naissance) suivi du nom d'usage (facultatif et s'il y a lieu))

numéro d'immatriculation _____

date de naissance _____

assuré(e) (à remplir si la personne recevant les soins n'est pas l'assuré(e))

nom et prénom _____
(nom de famille (de naissance) suivi du nom d'usage (facultatif et s'il y a lieu))

numéro d'immatriculation _____

adresse de l'assuré(e) _____

identification du prescripteur et de la structure dans laquelle il exerce

nom et prénom _____

raison sociale _____

adresse _____

identifiant _____

n° structure _____
(cf. Annexe 10)

à compléter par le prescripteur

☐ médicament, indiquer son nom (marque ou générique) : _____

☐ produit ou prestation, indiquer sa désignation précise : _____

s'il s'agit d'un médicament, préciser la forme, le dosage, la posologie, la voie d'administration : _____

s'il s'agit d'un produit ou d'une prestation, préciser la quantité de produits nécessaires ou la posologie : _____

durée du traitement, le cas échéant : _____

conditions de prise en charge

maladie ☐ soins en rapport avec une ALD : oui ☐ non ☐ soins dispensés au titre de l'art. L. 115 ☐

accident du travail ou maladie professionnelle ☐ date : _____

Je soussigné(e), Docteur _____, atteste que la prescription concernant le patient susvisé est conforme aux indications et aux conditions des prescriptions et d'utilisation prévues par la fiche d'information thérapeutique établie par la Haute Autorité de Santé. S'il existe, le volet patient de ladite fiche a été remis par mes soins à ce patient.

si prescription initiale par un établissement, date limite de la prochaine consultation dans l'établissement : _____

date : _____ signature du prescripteur : _____

identification du pharmacien ou du fournisseur et de la structure dans laquelle il exerce

nom et prénom _____

raison sociale _____

adresse _____

identifiant _____

n° structure _____
(cf. Annexe 10)

à compléter par le pharmacien ou le fournisseur qui délivre le médicament, le produit ou la prestation

mentions obligatoires à reporter sur l'ordonnance : _____

date de délivrance : _____

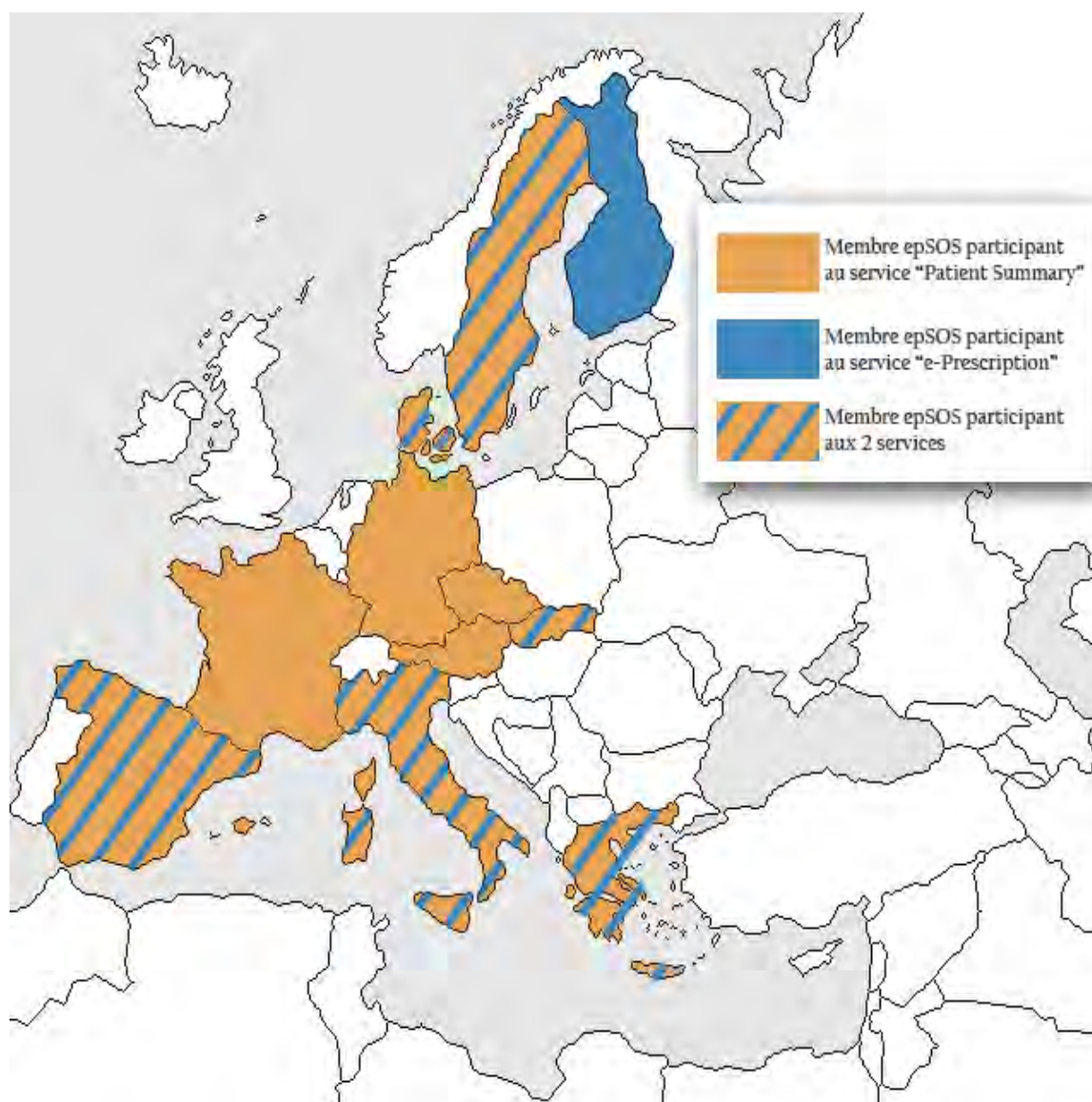
Quiconque se rend coupable de fraude ou de fausse déclaration est passible de peines pécuniaires, d'amende et/ou d'emprisonnement (articles 313-1, 440-1 et 441-6 du Code pénal et articles L. 146-13 et L. 162-1-14 du Code de la sécurité sociale).

Annexe 17 : Répartition géographique des différents pays européens adhérant au dispositif epSOS²⁷⁴



²⁷⁴ Source : <http://www.epsos.eu/france/le-projet-epsos/les-partenaires.html>

Annexe 18 : Répartition géographique des états membres epSOS proposant le service « Patient Summary » et/ou le service « e-prescription »²⁷⁵.



²⁷⁵ Source : <http://www.epsos.eu/epsos-services.html>

LA PHARMACIE D'OFFICINE A L'ERE DE LA DEMATERIALISATION

RESUME :

Dans une époque où tout devient donnée numérique, les pharmaciens d'officine ont su intégrer et tirer profit des technologies de l'information et de la communication dans l'accomplissement de leurs missions. Ils disposent ainsi d'outils informatiques facilitant leurs relations avec l'assurance maladie et permettant d'améliorer la qualité, la sécurité et l'efficacité de leurs dispensations et du suivi de leurs patients. En perpétuelle évolution, le panel des services offerts par notre système d'e-santé, déjà doté d'un outil d'e-dispensation performant (le dossier pharmaceutique), pourrait s'élargir avec l'apport d'un système d'e-prescription, véritable passerelle électronique entre le prescripteur et le pharmacien correspondant, né de la loi HPST. Parce qu'elles sont sensibles, les données de santé traitées par ces systèmes doivent bénéficier de mesures de sécurité adaptées à ces nouveaux usages afin d'en garantir la confidentialité et préserver le principe intangible du secret médical.

TITLE : Pharmacy in the dematerialization age

While everything becomes numeric, pharmacists had known how to integrate and to benefit from information and communication technologies to accomplish their missions. They make thus use of information technology tools to make their relations with health insurance easy and to improve the quality, the security and the efficiency of their dispensations and of patients monitoring. In perpetual evolution, the panel of services offered by our e-health system, already endowed with a performing e-dispensation tool (the pharmaceutical file), could be extended with the introduction of an e-prescription system, real electronic bridge between the prescriber and the corresponding pharmacist, born with the HPST law. Because they are sensitive, health data treated by these systems must benefit of security measures adapted to these new habits in order to guarantee their confidentiality and to preserve the sacred principle of medical secret.

DISCIPLINE administrative : Droit pharmaceutique et Economie de la santé

MOTS-CLES : Pharmacie, officine, dématérialisation, informatique, logiciel de gestion d'officine, aide à la dispensation, internet, dossier pharmaceutique, e-prescription, e-santé

INTITULE ET ADRESSE DE L'UFR OU DU LABORATOIRE :

Faculté des Sciences Pharmaceutiques. 35, chemin des maraîchers, 31062 Toulouse Cedex 09

Directeur de thèse : Madame le professeur TABOULET Florence