

**UNIVERSITÉ TOULOUSE III PAUL SABATIER  
FACULTÉ DES SCIENCES PHARMACEUTIQUES**

**ANNÉE : 2024**

**THÈSE : 2024/TOU3/2005**

**THÈSE**

**POUR LE DIPLÔME D'ÉTAT DE DOCTEUR EN PHARMACIE**

Présentée et soutenue publiquement  
par

GIL Sarah

**L'INTÉGRITÉ DES DONNÉES DANS LES INDUSTRIES PHARMACEUTIQUES :  
ÉVOLUTION AU COURS DU TEMPS ET DANS LE MONDE**

Date de soutenance : le Vendredi 02 Février 2024

Directrice de thèse : Madame ARELLANO Cécile

**JURY**

Président : SUDOR Jan, Maître de Conférences des Universités en Chimie Analytique  
1er assesseur : CAZALBOU Sophie, Maître de Conférences des Universités en Pharmacie  
Galénique  
2ème assesseur : BASSINO Pascale, Docteur en Pharmacie Responsable Assurance  
Qualité à Sanofi Compiègne  
3ème assesseur : ARELLANO Cécile, Maître de Conférences des Universités en Chimie  
Thérapeutique

**PERSONNEL ENSEIGNANT**  
**du Département des Sciences Pharmaceutiques**  
**de la Faculté de santé**  
**au 08 mars 2023**

**Professeurs Emérites**

Mme BARRE A.	Biologie Cellulaire
M. BENOIST H.	Immunologie
Mme NEPVEU F.	Chimie analytique
Mme ROQUES C.	Bactériologie - Virologie
M. ROUGE P.	Biologie Cellulaire
M. SALLES B.	Toxicologie

**Professeurs des Universités**

**Hospitalo-Universitaires**

Mme AYYOUB M.	Immunologie
M. CESTAC P.	Pharmacie Clinique
M. CHATELUT E.	Pharmacologie
Mme DE MAS MANSAT V.	Hématologie
M. FAVRE G.	Biochimie
Mme GANDIA P.	Pharmacologie
M. PARINI A.	Physiologie
M. PASQUIER C.	Bactériologie - Virologie
Mme ROUSSIN A.	Pharmacologie
Mme SALLERIN B. (Directrice-adjointe)	Pharmacie Clinique
M. VALENTIN A.	Parasitologie

**Universitaires**

Mme BERNARDES-GENISSON V.	Chimie thérapeutique
Mme BOUTET E.	Toxicologie - Sémiologie
Mme COSTE A.	Parasitologie
Mme COUDERC B.	Biochimie
M. CUSSAC D. (Doyen-directeur)	Physiologie
Mme DERA EVE C.	Chimie Thérapeutique
M. FABRE N.	Pharmacognosie
Mme GIROD-FULLANA S.	Pharmacie Galénique
M. GUIARD B.	Pharmacologie
M. LETISSE F.	Chimie pharmaceutique
Mme MULLER-STAU MONT C.	Toxicologie - Sémiologie
Mme REYBIER-VUATT OUX K.	Chimie analytique
M. SEGUI B.	Biologie Cellulaire
Mme SIXOU S.	Biochimie
M. SOUCHAR D J-P.	Chimie analytique
Mme TABOULET F.	Droit Pharmaceutique
Mme WHITE-KONING M.	Mathématiques

## Maîtres de Conférences des Universités

### Hospitalo-Universitaires

M. DELCOURT N.	Biochimie
Mme JUILLARD-CONDAT B.	Droit Pharmaceutique
Mme KELLER L.	Biochimie
M. PUISSET F.	Pharmacie Clinique
Mme ROUCH L.	Pharmacie Clinique
Mme ROUZAUD-LABORDE C	Pharmacie Clinique
Mme SALABERT A.S.	Biophysique
Mme SERONIE-VIVIEN S (*)	Biochimie
Mme THOMAS F. (*)	Pharmacologie

### Universitaires

Mme ARELLANO C. (*)	Chimie Thérapeutique
Mme AUTHIER H.	Parasitologie
M. BERGE M. (*)	Bactériologie - Virologie
Mme BON C. (*)	Biophysique
M. BOUJILA J. (*)	Chimie Analytique
M. BROUILLET F.	Pharmacie Galénique
Mme CABOU C.	Physiologie
Mme CAZALBOU S. (*)	Pharmacie Galénique
Mme CHAPUY-REGAUD S. (*)	Bactériologie - Virologie
Mme COLACIOS C. (*)	Immunologie
Mme ECHINARD-DOUIN V. (*)	Physiologie
Mme EL GARAH F.	Chimie Pharmaceutique
Mme EL HAGE S.	Chimie Pharmaceutique
Mme FALLONE F.	Toxicologie
Mme FERNANDEZ-VIDAL A.	Toxicologie
Mme GADEA A.	Pharmacognosie
Mme HALOVA-LAJOIE B.	Chimie Pharmaceutique
Mme JOUANJUS E.	Pharmacologie
Mme LAJOIE-MAZENC I.	Biochimie
Mme LEFEVRE L.	Physiologie
Mme LE LAMER A-C. (*)	Pharmacognosie
M. LE NAOUR A.	Toxicologie
M. LEMARIE A.	Biochimie
M. MARTI G.	Pharmacognosie
Mme MONFERRAN S	Biochimie
M. PILLOUX L.	Microbiologie
M. SAINTE-MARIE Y.	Physiologie
M. STIGLIANI J-L.	Chimie Pharmaceutique
M. SUDOR J. (*)	Chimie Analytique
Mme TERRISSE A-D.	Hématologie
Mme TOURRETTE-DIALLO A. (*)	Pharmacie Galénique
Mme VANSTEELANDT M.	Pharmacognosie

(\*) Titulaire de l'habilitation à diriger des recherches (HDR)

## Enseignants non titulaires

### Assistants Hospitalo-Universitaires

M. AL SAATI A	Biochimie
Mme BAKLOUTI S.	Pharmacologie
Mme CLARAZ P.	Pharmacie Clinique
Mme CHAGNEAU C.	Microbiologie
Mme DINTILHAC A.	Droit Pharmaceutique
M. LE LOUEDEC F.	Pharmacologie
Mme RIGOLOT L.	Biologie Cellulaire, Immunologie
Mme STRUMIA M.	Pharmacie Clinique

### Attaché Temporaire d'Enseignement et de Recherche (ATER)

Mme HAMZA Eya	Biochimie
Mme MALLI Sophia	Pharmacie Galénique
M. TABTI Redouane	Chimie Thérapeutique

## AVANT-PROPOS ET REMERCIEMENTS

À ma Directrice de Thèse :

Je tiens tout d'abord à honorer Madame Cécile ARELLANO pour avoir accepté de m'accompagner avec une immense bienveillance dans la rédaction de cette thèse et pour m'avoir prodigué autant de précieux conseils et de sympathie.

Aux membres du Jury :

À Monsieur Jan SUDOR, Président de mon Jury, un chaleureux merci d'avoir endossé cette responsabilité aussi vite et pour tout ce que j'ai pu apprendre en tant qu'étudiante et m'étant indispensable dans ma vie professionnelle.

À Madame Sophie CAZALBOU, je transmets toute ma gratitude de bien vouloir faire partie de mon Jury et pour nous avoir enseigné à mes camarades et moi-même des cours et des travaux pratiques aussi intéressants chaque année.

À Madame Pascale BASSINO, j'envoie une attention particulière pour m'avoir ouvert la voie à l'Intégrité des Données et au monde professionnel de l'industrie en général avec autant de gentillesse et de patience.

À mes parents, mes grands-parents et ma sœur Tacha, je vous adresse mon entière reconnaissance pour votre soutien inconditionnel, vos encouragements et votre présence.

À Greg, je te transmets mes tendres remerciements d'être au quotidien mon ange gardien et mon inspiration pour me motiver à donner le meilleur de moi-même et m'améliorer, que ce soit pour cette thèse ou dans tous les aspects de notre vie.

À Franck et Philippe, pour leur confiance alors que j'étais encore étudiante, leur accueil clément au sein de leur équipe et sans qui ce sujet ou ce plan de thèse n'existeraient pas.

À Ludo, Max, Laurent et tous mes autres collègues de Compiègne et Paris, je vous remercie pour les connaissances que vous m'avez apporté sur tellement de sujets, de même que pour les bons moments passés ensemble.

À ma binôme Léa, je chérirai toujours nos expériences, nos joies et nos discussions, que ce soit en TP, à la BU ou en soirées, et qui m'ont permis d'en arriver à cette étape.

À Benjamin, Estelle, Loïc et mes chers camarades de la Faculté de Pharmacie, merci pour votre support et votre écoute, pour votre bonne humeur et vos rires durant nos années d'études.

À Éliisa et sa famille, que je considère comme la mienne, et Fabien, mes amis les plus proches depuis plus de dix ans, sans qui je ne serai pas celle que je suis aujourd'hui.

## TABLE DES MATIÈRES

TABLE DES ACRONYMES .....	8
TABLE DES FIGURES .....	11
INTRODUCTION .....	12
I. L'INTÉGRITÉ DES DONNÉES DE NOS JOURS .....	13
1. Définition et fondements de l'Intégrité des Données.....	13
A. Contexte et challenge.....	13
B. Visée et implication de l'Intégrité des Données .....	15
C. Principes et notions clés.....	17
2. Composantes de l'Intégrité des Données .....	20
A. Cycle de vie des données .....	20
B. Sécurité des données.....	23
C. Management des risques et des systèmes .....	26
3. Niveaux de l'Intégrité des Données .....	28
A. Niveau 1 de l'Intégrité des Données.....	28
B. Niveau 2 de l'Intégrité des Données.....	30
C. Niveau 3 de l'Intégrité des Données.....	34
II. L'INTÉGRITÉ DES DONNÉES DANS DIFFÉRENTES INDUSTRIES PHARMACEUTIQUES .....	37
1. L'Intégrité des Données dans les industries pourvues d'anciens équipements 37	
A. Informatique .....	37
B. Équipements .....	39
C. Management .....	41
2. L'Intégrité des Données dans les industries disposant d'équipements modernes .....	42
A. Informatique .....	42

B. Équipements .....	44
C. Management .....	47
3. L'Intégrité des Données dans les industries 4.0 .....	48
A. Informatique .....	48
B. Équipements .....	53
C. Management .....	56
III. L'INTÉGRITÉ DES DONNÉES RÉGLEMENTÉE DANS DIVERSES RÉGIONS DU GLOBE .....	59
1. L'Intégrité des Données en Chine.....	59
A. Les ressemblances avec l'Europe et les États-Unis .....	59
B. Les différences avec l'Europe et les États-Unis .....	60
C. Exemples d'infractions.....	62
2. L'Intégrité des Données au Japon .....	64
A. Les similitudes avec l'Europe et les États-Unis .....	64
B. Les distinctions avec l'Europe et les États-Unis .....	66
C. Exemples d'écarts .....	67
3. L'Intégrité des Données dans d'autres contrées.....	68
A. L'Intégrité des Données en Inde.....	68
B. L'Intégrité des Données en Russie.....	70
C. L'Intégrité des Données au Canada .....	71
D. L'Intégrité des Données au Mexique .....	72
E. Synthèse de l'Intégrité des Données entre les nations.....	73
CONCLUSION.....	74
BIBLIOGRAPHIE.....	75
TITRE ET RÉSUMÉ EN ANGLAIS .....	82

## TABLE DES ACRONYMES

AI : Artificial Intelligence, Intelligence Artificielle

ATR : Audit Trail Review, Revue de Piste d'Audit

CDSCO : Central Drugs Standard Control Organization, Organisation Centrale de Contrôle des Normes Pharmaceutiques

CFDA : Chinese Food and Drug Administration, Administration Chinoise des Aliments et des Médicaments

COFEPRIS : Comisión Federal para la Protección contra Riesgos Sanitarios, Commission Fédérale pour la Protection contre les Risques Sanitaires

CQA : Critical Quality Attributes, Attributs Qualité Critiques

DIMM : Data Integrity Maturity Model, Modèle de Maturité de l'Intégrité des Données

DIRA : Data Integrity Risk Assessment, Évaluation des Risques liés à l'Intégrité des Données

DL : Deep Learning, Apprentissage Profond

DRP : Disaster Recovery Plan, Plan de Retour après Sinistre

ELN : Electronic Lab Network, Réseau de Laboratoire Électronique

eQMS : electronic Quality Management System, Système de Management de la Qualité électronique

ERES : Electronic Records and Electronic Signatures, Enregistrements Électroniques et Signatures Électroniques

ERP : Enterprise Resource Planning, Progiciel de Gestion Intégré

EU : European Union, Union Européenne

FDA : Food and Drug Administration, Agence Fédérale Américaine des Produits Alimentaires et Médicamenteux



FSID & GP : Federal State Institute of Drugs and Good Practices, Institut Fédéral des Médicaments et des Bonnes Pratiques

GAMP 5 : Good Automated Manufacturing Practices issue 5, Bonnes Pratiques de Fabrication Automatisée

GMP : Good Manufacturing Practices, Bonnes Pratiques de Fabrication

HPLC : High Performance Liquid Chromatography, Chromatographie en Phase Liquide à Haute Performance

IaaS : Infrastructure as a Service, Infrastructure en tant que Service

ICH : International Council for Harmonization of Technical Requirements for Pharmaceuticals for Human Use, Conseil International d'Harmonisation des Exigences Techniques pour l'Enregistrement des Médicaments à Usage Humain

IIOT : Industrial Internet Of Things, Internet Industriel Des Objets

IMCRA : International Coalition of Medicines Regulatory Authorities, Coalition Internationale des Autorités de Réglementation des Médicaments

ISPE : International Society for Pharmaceutical Engineering, Société Internationale de l'Ingénierie Pharmaceutique

IT : Information Technology, Technologie de l'Information

JPMA : Japan Pharmaceutical Manufacturers Association, Association Japonaise de l'Industrie Pharmaceutique

MAM : Multi-Attribute Method, Méthode Multi-Attributs

ML : Machine Learning, Apprentissage Automatique

NMPA : National Medical Products Administration, Administration Nationale des Produits Médicaux

PaaS : Platform as a Service, Plate-forme en tant que Service

PAT : Process Analytical Technology, Technologie Analytique des Procédés

PIC/S : Pharmaceutical Inspection Convention and Pharmaceutical Inspection Co-Operation Scheme, Convention sur l'Inspection Pharmaceutique et Schéma de Coopération dans le domaine de l'Inspection Pharmaceutique

PMDA : Pharmaceuticals and Medical Devices Agency, Agence des Médicaments et des Dispositifs Médicaux

RUTH : Recipe management, User management, Time & date synchronization, Historian data storage & management

SaaS : Software as a Service, Logiciel en tant que Service

WHO : World Health Organization, Organisation Mondiale de la Santé

## TABLE DES FIGURES

Figure 1 : Les principes ALCOA +

Figure 2 : Quelques étapes principales du cycle de vie des données

Figure 3 : Les différents types de sécurités

Figure 4 : Data Flow Mapping sur l'étape de compression d'un processus de fabrication

Figure 5 : Les piliers de la Data Governance

Figure 6 : L'évolution de l'industrie dans le temps

Figure 7 : Le Cloud

Figure 8 : Le fonctionnement parcellisé d'un système autonome

Figure 9 : Les paramètres du système vertical RUTH

Figure 10 : La maturité numérique de l'Intégrité des Données By Design dans la cadre de la Pharma 4.0

Figure 11 : Les principes ALCOA en Chine

Figure 12 : Les trois exigences de la réglementation japonaise

Figure 13 : Tableau comparatif de l'Intégrité des Données parmi les pays abordés

## INTRODUCTION

De prime abord, l'Intégrité des Données semble assimilée à une notion informatique. Il est vrai qu'elle s'apparente effectivement plus aux domaines des télécommunications et de la cryptographie. Cependant, elle revêt une importance grandissante dans le secteur pharmaceutique, comme en témoigne les premières et rares citations éparses et minimales dans plusieurs guidelines avant les années 2000 et l'apparition du terme dans des lettres d'avertissement dès 2007. (1)

Depuis quelques années, même si un médicament a l'air prometteur ou est réputé comme sûr, n'importe quel site de fabrication de produit est susceptible d'être arrêté sur le champ si l'Intégrité des Données n'est pas respectée. Il est alors possible de se risquer à supputer que les données sont devenues certains des actifs les plus inestimables d'une entreprise.

Dans l'optique de jauger ce postulat, nous débuterons par exposer ce qu'est l'Intégrité des Données à l'aide de sa définition dans son contexte, des éléments la composant, tels que le cycle de vie des données et le management des risques et des systèmes, et les niveaux d'exécution la constituant.

Puis, nous nous pencherons sur l'adoption de l'Intégrité des Données dans différentes catégories d'industries pharmaceutiques, qu'elles soient équipées de machines anciennes, actuelles ou ultra modernes. Cela sera fait en se basant sur les trois mêmes points de vue, qui sont ceux de l'informatique, des équipements et du management.

Enfin, nous observerons les éventuelles nuances d'Intégrité des Données dans une poignée de pays en Asie et en Amérique du Nord en tâchant de synthétiser les points communs et opposés avant de citer des exemples de lettres d'avertissement.

# I. L'INTÉGRITÉ DES DONNÉES DE NOS JOURS

## 1. Définition et fondements de l'Intégrité des Données

### A. Contexte et challenge

Afin de garantir la sûreté et la qualité des produits pharmaceutiques et de leurs processus de fabrication, différents ouvrages de référence ont été rédigés tels que les GMP (les Good Manufacturing Practices ou Bonnes Pratiques de Fabrication) et les lignes directrices issues des travaux de l'ICH (International Council for Harmonization) relatifs aux Exigences Techniques pour l'Enregistrement des Médicaments à Usage Humain. L'évolution des exigences réglementaires et des pratiques (incluant l'utilisation de nouvelles technologies) engendre ainsi de plus en plus de paramètres à contrôler et à enregistrer et *in fine* une multitude de données recensées. La qualité d'un médicament est alors étroitement liée à la qualité de ses données et une mauvaise gestion de ces dernières peut de surcroît mener à une perte de temps et d'argent, une atteinte de l'image de marque, des sanctions légales... (2)

Il est primordial d'assurer l'Intégrité des Données pour qu'une décision pharmaceutique stratégique soit robuste, c'est ce que l'on nomme le « Reliable Decision-Making ». (3) En effet, nous ne pouvons décemment pas avoir confiance en un produit renseigné par une base de données erronée, c'est pourquoi les risques d'altérations de ces données doivent être aussi maîtrisés que ceux portant sur les produits. L'Intégrité des Données fait par conséquent partie intégrante du Système Qualité, pour certifier la qualité du médicament, la sécurité du patient et la Santé Publique. (4)

Les données dont nous parlons peuvent être générées par un opérateur ou par un équipement et pendant une étape de production ou de contrôle quel que soit leur support, ce qui les rend mobiles au travers de plusieurs applicatifs. (5) Nous faisons de plus face à une évolution de l'informatique et de la façon de conserver les données, suite à la mondialisation des activités, la digitalisation croissante des processus et la multiplication des Systèmes Informatisés par lesquels circulent les données. Il faut dans ce cas démontrer que les transports et changements successifs d'une donnée n'en altèrent pas sa qualité ni son accessibilité.

L'autre raison justifiant la nécessité d'apporter la preuve de données intègres résulte des progrès informatiques et du fait que les informations récoltées peuvent être désormais plus faciles à corrompre, que ce soit par le biais de détériorations volontaires ou non. Cela comprend par exemple des données supprimées ou non prises en compte à cause de résultats non satisfaisants au cours d'essais cliniques, des retests jusqu'à la conformité dans le cadre de la libération de lots, des pertes ou manques de traçabilité donnant lieu à des réclamations qualité ou même des falsifications de données avec des modifications de dates de péremption. Ainsi, il s'agit de protéger les données numériques fragiles des tentatives de fraudes internes, des nuisances externes (c'est-à-dire le cybercrime, entre autres...), des virus informatiques, des défaillances techniques du Système d'Information (comme un bug dans une application qui supprimerait la mauvaise donnée), des erreurs lors des transferts d'informations ou des répliques, des erreurs humaines de saisie, d'exploitation ou de manipulation, des risques matériels (incendies, pannes, etc.). (2)

La maîtrise de l'Intégrité des Données s'est organisée en trois temps. Initialement, elle reposait sur la validation des Systèmes Informatisés. Les fonctions étaient définies, développées et testées et le rapport de validation portait la conformité du système.

L'approche a ensuite évolué vers une maîtrise des risques en incluant l'environnement du système et son cycle de vie. Cette méthode de « Risk-Based Approach » intégrait de ce fait la vérification de la mise en place de divers aspects organisationnels pour l'exploitation (formations, procédures, pour ne citer qu'eux) mais se contentait de rester concentrée au niveau du système.

Aujourd'hui, cette approche est rendue obsolète par la profusion des Systèmes Informatisés, bien souvent interconnectés entre eux et affichant un degré de configuration élevé corrélé à une complexité des flux. La validation des Systèmes Informatisés, si elle est toujours demandée, n'est plus suffisante pour garantir une gestion des risques convenable sur l'Intégrité des Données. Il devient indispensable de passer d'un modèle centré sur les systèmes à un modèle focalisé sur les données grâce à l'instauration d'un « Quality Data Management », structuré et piloté par le risque et attestant d'une cohérence de traitement au sein d'une organisation. Ce

modèle présente une sensibilisation continue à l'Intégrité des Données sur l'ensemble des processus (en particulier critiques) et non plus seulement sur les systèmes critiques, en considérant les données électroniques, les données papier et les interfaces entre les deux au cours du cycle de vie. (3)

Au final, si l'on respecte bien tous ces paramètres, l'Intégrité des Données peut également servir à encourager l'innovation et l'avancement technologique. (6)

## **B. Visée et implication de l'Intégrité des Données**

En premier lieu, d'après les différents supports du WHO (World Health Organization ou Organisation Mondiale de la Santé), de la FDA (Food and Drug Administration ou Agence Fédérale Américaine des Produits Alimentaires et Médicamenteux) et du PIC/S (Pharmaceutical Inspection Convention and Pharmaceutical Inspection Co-Operation Scheme ou Convention sur l'Inspection Pharmaceutique et Schéma de Coopération dans le domaine de l'Inspection Pharmaceutique), l'Intégrité des Données est : « la mesure dans laquelle les données critiques restent complètes, cohérentes et exactes tout au long de leur cycle de vie ». Elle implique que ces données complètes, cohérentes et exactes soient attribuables, lisibles, contemporaines, originales et fiables, notions que nous développerons dans une partie ultérieure. Une bonne maîtrise des systèmes et des contrôles de l'Intégrité des Données est censée faciliter la détection des erreurs, des omissions et des résultats aberrants au cours de la vie de la donnée. (7)

Ce n'est pas seulement une problématique informatique, cela touche aussi l'automatisation des processus et la limitation des erreurs liées aux interventions humaines. Un paramètre essentiel du Système Qualité d'une organisation est le fait de permettre l'identification et la mise sous contrôle des points de vulnérabilité des données critiques, que les supports de ces données soient électroniques ou papier. (3)

Ce n'est pas non plus que la sécurité physique des données : cela correspond à l'ensemble des mesures prises pour empêcher la corruption des données. L'Intégrité des Données met effectivement en œuvre l'utilisation de systèmes, processus et

procédures qui bloquent l'accès des données aux personnes qui pourraient en faire un usage néfaste ou détourné par exemple. Les conséquences seront des failles de sécurité des données pouvant être mineures et faciles à contenir ou pouvant se révéler majeures et entraîner de sérieux dommages.

L'objectif global de l'Intégrité des Données est donc de conserver des données intactes et exactes tout au long de leur cycle de vie tandis que la sécurité des données vise quant à elle à protéger les informations d'attaques extérieures. La sécurité matérielle des données n'est qu'un aspect parmi d'autres de l'Intégrité des Données, il convient alors de distinguer ces deux termes. La simple sécurité physique des données n'est pas assez étendue pour intégrer les nombreux processus fondamentaux servant à garder les données inchangées dans le temps. (8)

Nous pouvons noter que, pour l'instant, l'application de l'Intégrité des Données n'est pas obligatoire selon la FDA. (9)

Dans un second temps, pour correctement prendre en compte la donnée dans sa totalité, il est nécessaire de préciser la définition d'une métadonnée. Les métadonnées sont les informations attachées à une donnée qui amènent un élément de contexte et permettent de mieux en comprendre le sens. (10)

Nous pouvons ajouter qu'une donnée ne veut rien dire sans les renseignements additionnels que sont les métadonnées. En effet, pour reprendre l'exemple des guidelines « Data Integrity and Compliance With Drug CGMP, Questions and Answers, Guidance for Industry » de la FDA à propos d'une pesée, la mention du nombre « 23 » est inutile sans métadonnées, telles que l'indication de l'unité « mg ». Elles comprennent subséquemment le lien entre une donnée et son horodatage (qui doit lui-même respecter les attendus), l'identification de l'instrument et de l'opérateur ayant conduit le test ou l'analyse générant la donnée, l'historique d'évolution de cette donnée ainsi que ses différents états successifs et les informations structurées qui décrivent, expliquent ou facilitent la récupération, l'utilisation ou la gestion des données. (7)



À chaque fois qu'une modification est apportée aux métadonnées, un utilisateur doit justifier la raison de son changement pour que les données restent à jour. Un système eQMS (electronic Quality Management System ou Système de Management de la Qualité électronique) peut assister à maîtriser le risque récurrent de la désynchronisation des métadonnées à l'occasion d'un processus de révision puisque le lien entre une donnée et ses métadonnées doit être préservé à l'aide d'un moyen traçable et sécurisé pour suivre les activités GMP. (9)

### C. Principes et notions clés

Comme abordé précédemment, un outil précieux regroupant les concepts à appliquer en Intégrité des Données a été déployé dans le but de faciliter l'apport de preuve de la conformité et de l'intégrité opérationnelle des données : l'ALCOA. C'est un acronyme stipulant que les données et leurs enregistrements doivent être Attribuables (Attributable), Lisibles (Legible), Contemporains (Contemporaneous), Originaux (Original) et Exacts (Accurate) tout au long du cycle de vie de cet enregistrement de données.

Le principe « **Attribuable** » signifie que chaque donnée devrait être reliée à l'individu ou au système qui l'a collectée ou a traité l'activité, c'est-à-dire que l'auteur et la source sont à identifier. De plus, le lieu d'origine, la date et l'heure du recensement de la donnée doivent être notés. En cas d'altération de la donnée, l'opérateur ayant effectué la correction est lui aussi signalé. (11) Dans les faits, cela pourrait se traduire par l'implémentation d'un identifiant personnel unique, d'une signature pour chacun des enregistrements pour les associer à l'instrument ou à la personne qui a réalisé la mesure et d'une référence au système analysé et à la date et l'heure. Le contrôle de ce format de signature peut être spécifique d'un type d'équipement ou d'un procédé et doit également être tracé. (12)

La notion « **Lisible** » veut dire que les données sont censées être lues et interprétées sans difficulté à court et long terme. Par conséquent, les matériels et supports de données utilisés pour recueillir et sauvegarder les informations sont tenus d'être durables. (11) Dans les industries, cela peut être accompli par l'interdiction de documents manuscrits, l'emploi d'un stockage sous format ouvert

pour les enregistrements électroniques afin qu'ils puissent être lus sur de nombreux formats informatiques et, de ce fait, être accessibles et lisibles pendant des années. (12) La norme 21 CFR Partie 11 recommande pour sa part de mettre en place des Bonnes Pratiques Documentaires, des Logbooks et des Audit Trails (dispositifs que nous définirons plus loin).

La précision « **Contemporaine** » indique que les données doivent être documentées en même temps que l'activité est développée, autrement dit qu'elles sont à enregistrer au moment où elles sont collectées. Ces enregistrements devant être créés immédiatement quand l'échantillon est mesuré, la transcription manuelle des documents papier ou la compilation de documents papier puis leur transcription manuelle en format électronique à une date ultérieure ne sont *de facto* pas des Bonnes Pratiques. (12) Les options pourront plutôt être l'enregistrement des données sur le support définitif, l'installation d'un horodatage et d'une synchronisation horaire sur les appareils et la limitation des mémoires temporaires. (3)

Une donnée **Originale** est une donnée dont l'enregistrement de base a été conservé et dont les copies, dans le cas de duplicatas, ont été authentifiées et certifiées conformes par le créateur de l'enregistrement élémentaire, dans l'objectif de préserver le sens et l'Intégrité des Données. (11) La FDA propose que le dossier électronique soit l'enregistrement original et qu'il soit créé dès la fin du test, au lieu de risquer une duplication ou un scan manqué lors de la numérisation de plusieurs documents papier au format électronique. Effectivement, il y a un danger à chaque transcription de résultats de tests d'une forme à une autre (les enregistrements transcrits manuellement étant évidemment les plus sensibles à cause de la plus grande opportunité d'erreurs humaines), il est donc conseillé de garder les données et métadonnées dans leur statut initial. (12)

Le concept « **Exact** » peut être assimilé à fiable et se réfère à l'absence d'erreur pour que les données soient viables et que leur qualité soit maintenue. Il ne peut ainsi pas y avoir de rectification sans documents pour accompagner et justifier les changements. (11) Concrètement, le processus de saisie des enregistrements électroniques doit être robuste pour assurer leur fiabilité, ce qui implique que les calculs et la saisie manuelle de données lorsqu'il existe des possibilités d'erreurs humaines devraient être évités et que les enregistrements électroniques générés par

des instruments en ligne devraient contenir des informations raccordant les données à l'instrument utilisé pour effectuer la mesure. (12)

L'outil ALCOA s'est affiné vers la méthode ALCOA + en y adjoignant les qualificatifs Complete (Complet), Consistent (Cohérent), Enduring (Durable), Available and Accessible (Disponible et Accessible) et parfois Credible (Crédible) et Corroborated (Corroboré). Ces notions ainsi que les précédentes sont schématisées dans la Figure 1.

Des données **Complètes** sont tenues de ne manquer d'aucun élément critique permettant de reconstituer un évènement et nul paramètre n'est censé être supprimé d'un enregistrement depuis sa date de documentation. (13)

L'attribut « **Cohérent** » préconise de créer, traiter et stocker les données dans un ordre logique, par exemple en les classant chronologiquement avec un horodatage compris pour tout ajout aux données originales et en suivant leur régularité par l'application de divers audits durant leur durée de vie. (11)

Le matériel et la manière privilégiés pour garantir la **Durabilité** sont choisis pour leur capacité à favoriser l'enregistrement des données sur une période aussi longue que nécessaire sans perdre en lisibilité.

Les adjectifs « **Disponible** et **Accessible** » annoncent que les données et enregistrements sont susceptibles d'être passés en revue à n'importe quel moment en cas de besoin pour des décisions de libération de routine, des investigations ou des inspections pendant tout leur intervalle de rétention. (13)

Pour finir, des données **Crédibles** s'appuient sur des faits réels et fiables et elles sont **Corroborées** si elles sont supportées par des informations ou des preuves. (14)



*Figure 1 : Les principes ALCOA +*

## 2. Composantes de l'Intégrité des Données

### A. Cycle de vie des données

Tout d'abord, le cycle de vie des données représente toutes les phases de la vie de la donnée, y compris la donnée brute, à partir de la génération initiale et de l'enregistrement jusqu'au retrait et à la destruction d'une façon contrôlée à la fin de leur vie. (13) Ces étapes englobent la création ou l'acquisition, le traitement, la revue et la vérification de l'exhaustivité et de l'exactitude des données déclarées et des informations traitées, l'approbation, la transformation en renseignements utilisables, la récupération pour utilisation, l'emploi des données ou des résultats pour prendre une décision, la modification, la conservation et l'extraction des données en vue de les protéger contre la perte ou la modification non autorisée, le report, la transmission, la mise à disposition, la distribution, le stockage, l'archivage... (15)

Certains stades sont particuliers comme la régénération, intervenant lorsque la structure de stockage devient obsolète ou ne peut pas être conservée. (16) Le transfert occure quant à lui au moment du passage d'une solution informatique à une autre ou papier ou bien entre différentes organisations internes (le Contrôle

Qualité, l'Assurance Qualité, le service Informatique, la Production, etc.) et externes d'une société (prestataires, sous-traitants). (14) La mutation équivaut à réimplanter les données dans un nouveau Système Informatique par le biais de ce qui est appelé une « reprise de données ». (16)

La FDA et le PIC/S, respectivement au travers des directives « Data Integrity and Compliance With Drug CGMP, Questions and Answers, Guidance for Industry » et du guide « Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments », rendent compte d'une nuance entre la sauvegarde et l'archivage. La sauvegarde (« backup ») fait référence à une copie conforme de l'enregistrement original, maintenue en sécurité au cours de la période de conservation des dossiers et comportant les données, les métadonnées et les paramètres de configuration dans leur format primaire ou un format compatible. (7) Ce duplicata est gardé dans l'optique d'une restauration en cas de perte ou d'endommagement des données principales car la simple création d'une double sauvegarde temporaire sera jugée insuffisante par les autorités. (3)

L'archivage de son côté, est la rétention permanente, sur le long terme et dans leur forme finale, des données complètes, des métadonnées pertinentes et des signatures électroniques. Il servira à consulter les données le temps de leur durée de rétention et à reconstruire une activité ou un processus. (13)

Quel que soit le mode de préservation des données, leur intégrité doit être respectée, une description des différentes étapes de procédé et de contrôle doit être rédigée et la documentation doit faire partie du Système Qualité. Certaines des phases les plus importantes du cycle de vie des données sont représentées dans la Figure 2.

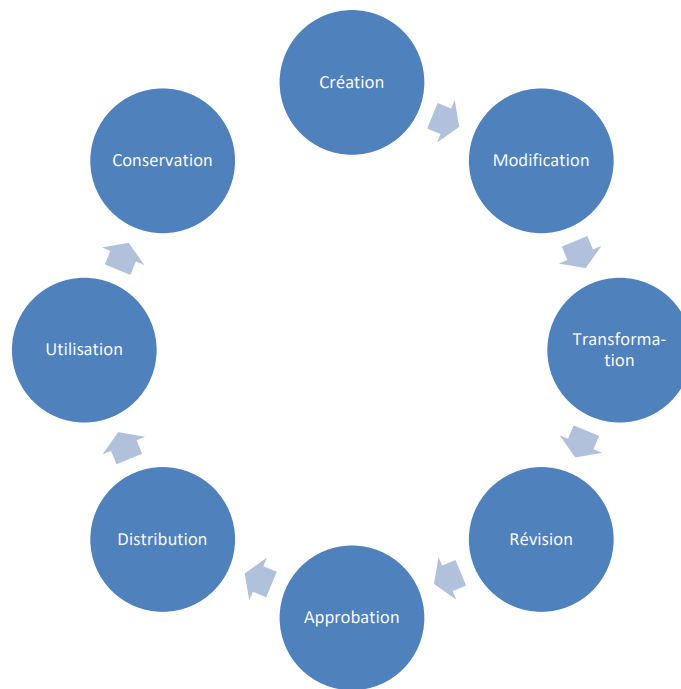


Figure 2 : Quelques étapes principales du cycle de vie des données

Dans cette continuité, la FDA précise également la dichotomie entre des enregistrements statiques et dynamiques. Un enregistrement statique est un document où les données sont immuables et non modifiables comme sur un papier ou une image électronique alors qu'un enregistrement dynamique est un format acceptant les interactions entre son contenu et un utilisateur dans le but d'en extraire des renseignements essentiels à l'exploitation. (17) Ces interactions peuvent par exemple aller de l'ajustement des paramètres d'intégration d'un graphique au changement d'une formule d'un tableur pour calculer des résultats de tests. Comme précédemment, il est demandé que les copies entretiennent le fond et la signification des données élémentaires (ce qui comprend les métadonnées associées) et que le caractère dynamique d'un enregistrement soit immortalisé. (18) De surcroît, les dossiers papier et électroniques seront soumis à l'inspection de la FDA.

Les phases de chaque donnée ou enregistrement listées ci-dessus sont identifiées et comprises de sorte que tout risque de modification ou d'altération puisse être en mesure d'être détecté. C'est la condition *sine qua non* pour constituer une démarche appropriée validant et documentant la conservation de la qualité des données dans

le cadre de leur cycle de vie et affirmant que leurs transformations successives n'en altèrent pas la valeur. En effet, le concept de cycle de vie de la donnée en soi aide à comprendre qu'il est primordial d'assurer que la portée sémantique de la donnée ne trahisse pas la valeur première qui a été créée par l'équipement source. (16) Il commence à être admis que le cycle de vie des données n'est pas seulement l'e-data et le Système Informatisé. (3)

Une nouvelle idée du cycle de vie de la donnée se dessine en opposition à une représentation relativement ancienne du cycle de vie applicatif.

Actuellement, la donnée surtout informatique dispose d'une identité propre et existe par elle-même et non plus exclusivement au travers de l'applicatif ou des applicatifs qui l'ont générée et la manipulent. C'est pourquoi il devient plus aisé de concevoir que la donnée qui était autrefois étudiée et envisagée uniquement par l'intermédiaire de l'applicatif (lequel devait être validé comme mentionné antérieurement) prend son « indépendance » des systèmes pour devenir pleinement information. L'accroissement de l'informatique dans les entreprises favorise justement ces transferts de données. (16)

## **B. Sécurité des données**

Dans la première partie, il a été signalé qu'il n'y a pas que la sécurité physique des données à prendre en compte. Effectivement, l'Intégrité des Données dans son entièreté repose sur trois principes à suivre au long du cycle de vie de ces dernières, à savoir la sécurité physique, la sécurité logique et la sécurité de continuité. (16)

L'intégrité physique regroupe l'ensemble des mesures qui permettent de protéger l'unité et l'exactitude des données des détériorations provoquées par des moyens physiques. Ces problématiques incluent les coupures de courant, les risques d'incendie et ceux dus aux animaux mais aussi les erreurs humaines et les piratages des fonctions des bases de données. (8) Les dégradations et les dangers sont

susceptibles de provenir de solutions isolées physiquement (comme une solution « stand alone » contrôlant un équipement), de périphériques aux réseaux (des armoires techniques par exemple) ou d'éléments physiques de stockage. (16)

La sécurité logique vise à conserver les données intactes dans une base de données relationnelle durant leurs différentes utilisations. Les soucis liés aux opérateurs et aux pirates informatiques sont toujours présents dans ce spectre d'action mais pas de la même manière que pour la sécurité physique. (8) En pratique, cela revient à ce que l'accès aux systèmes soit possible uniquement pour les personnes autorisées, formées et non anonymes (c'est-à-dire nommées et dont le profil manipulateur, administrateur ou autre a été statué) et sous contrôle d'un enregistrement strict et d'une traçabilité complète des accès. (16) Quatre types d'intégrités logiques ont été recensés : l'intégrité de domaine, l'intégrité d'entité, l'intégrité référentielle ou de relation et l'intégrité définie par l'utilisateur (catégorie régissant des règles spécifiques que les trois autres genres d'intégrités ne couvrent pas). (2)

L'intégrité de domaine fait référence aux processus attestant de l'exactitude de chaque donnée dans une base de données et aux plages de valeurs acceptables et stockables qu'une colonne particulière de cette base est autorisée à contenir. Les variétés de données concernées peuvent être des entiers, des textes, des dates, etc. et toutes les entrées de ces valeurs dans une colonne doivent être uniformes (les types de données ne doivent pas se mélanger dans le même domaine). (19)

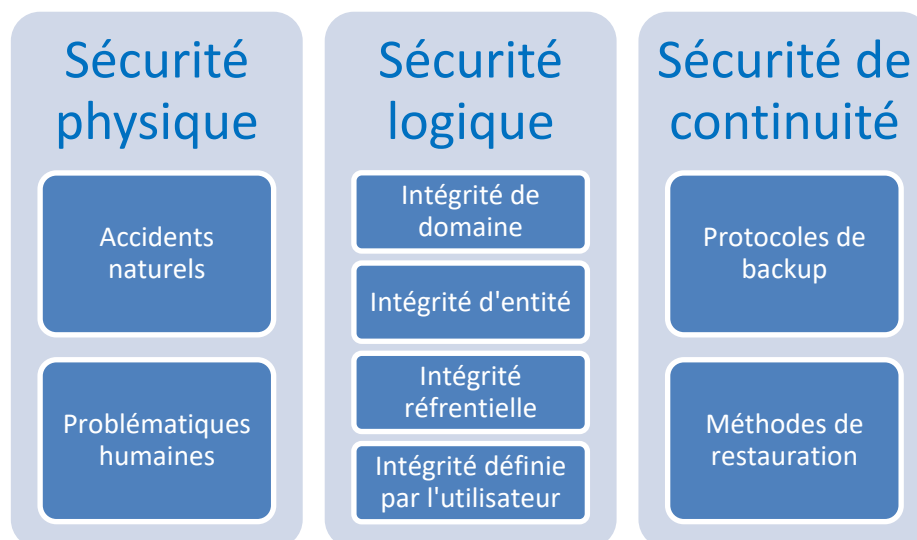
L'intégrité d'entité consiste à désigner chaque donnée ou enregistrement d'une entité de façon unique grâce à la création de clés primaires, dans l'objectif de certifier que les données ne sont pas répertoriées plus d'une fois dans une table et qu'aucune zone de celle-ci n'est nulle. (8)

La sécurité référentielle sert à garder la cohérence et l'homogénéité dans le stockage et l'utilisation des données entre deux tables en s'appuyant sur des règles établies dans la structure de la base de données en rapport avec des clés étrangères. Ces outils sont censés être employés pour garantir que les modifications, les ajouts et les suppressions dans la base de données ne portent pas atteinte à l'Intégrité des Données et que seuls les changements appropriés soient effectués. (19)



Lorsque ces trois intégrités ne suffisent pas à maintenir l'Intégrité des Données ou qu'un opérateur souhaite implanter des règles et des contraintes pour satisfaire des besoins particuliers, l'intégrité définie par l'utilisateur entre en jeu. (8) Il faudra souvent se renseigner et incorporer la politique spécifique de l'entreprise au nouveau fonctionnement, ce qui est généralement accompli par le biais de procédures stockées et de déclencheurs (des blocs d'instructions s'exécutant automatiquement si des évènements prédéfinis se produisent). (19)

La sécurité de continuité se résume à l'éventail de mesures qui permettent de conjecturer les opérations préventives ou correctives à activer en cas de sinistres ou d'accidents. Quel que soit l'évènement, il ne doit pas y avoir de perte ou d'endommagement de données donc pour ce faire, il est envisageable d'avoir recours à des protocoles de backup ou des méthodes de restauration. Le choix et la description de ces démarches seront détaillés dans des plans de continuité d'activité et notamment le DRP (Disaster Recovery Plan ou Plan de Retour après Sinistre) après une consultation des analyses de risques. (16) Cette sécurité et celles définies ci-dessus sont résumées dans la Figure 3.



*Figure 3 : Les différents types de sécurités*

### C. Management des risques et des systèmes

Pour commencer, d'après le GAMP 5 de l'ISPE (Good Automated Manufacturing Practices issue 5 de l'International Society for Pharmaceutical Engineering ou Bonnes Pratiques de Fabrication Automatisée de la Société Internationale de l'Ingénierie Pharmaceutique) et comme les dernières sous-parties le laissent entrevoir, les risques pour l'Intégrité des Données et l'intégrité des enregistrements sont supposés être identifiés et managés au même titre que les risques Qualité et Sécurité. Cela est concevable par l'adoption d'une approche par management des risques reposant sur la compréhension des processus, des technologies, des « business models » et du cycle de vie des données et entrant dans les applications de la Data Governance (une thématique qui sera explicitée ultérieurement). (20)

Cette méthode centrée sur le risque considère deux paramètres pour déterminer l'importance de chaque donnée et étape de traitement et ainsi adapter les efforts de contrôle : la Data Criticality et le Data Risk. (13) Le niveau d'effort à apporter pour maîtriser l'Intégrité des Données et donc attester de la qualité du produit et de la sécurité du patient combine ces critères et sera ensuite fixé selon l'impact des données sur les CQA (Critical Quality Attributes ou Attributs Qualité Critiques). (3)

La Data Criticality se traduit par le fait que les décisions sur lesquelles les données agissent peuvent être plus ou moins importantes et que les données en tant que telles ont une influence variable sur ces décisions. Cette notion s'articule alors autour de deux questions qui sont « Quelle décision la donnée influence-t-elle ? » et « Quel est l'impact des données sur la qualité ou la sécurité du produit ? ». (13)

Le Data Risk recense les risques d'altérations associés aux données critiques de l'étape préalable et estime leur degré de vulnérabilité vis-à-vis de la probabilité de détection d'altérations involontaires ou de falsifications intentionnelles, de suppressions, de pertes... Cette analyse de risques évalue les flux de données et les méthodes de génération et de traitement de celles-ci (et pas seulement les technologies informatiques) et dépend de la complexité du processus analysé, de son degré d'automatisation ou d'interaction avec les opérateurs et de la subjectivité de l'interprétation des résultats, entre autres. (3)

Les efforts déployés pour le contrôle se concentreront sur les données les plus critiques et vulnérables. (21)

Dans les situations d'automatisation et de risque d'exposition de la vulnérabilité des données qui deviennent fréquentes, les Systèmes Informatisés requièrent d'être validés et contrôlés pour préserver ces données. (21) Cette validation est vaste et concerne autant le matériel et les logiciels que les périphériques, les réseaux et les éléments du Cloud. L'Organisation Mondiale de la Santé demande aussi qu'elle englobe la conception, la mise en œuvre et la maintenance des contrôles pour assurer l'Intégrité des Données. (15)

Le système dans sa totalité doit répondre aux spécifications et à des exigences pertinentes et être validé pour l'utilisation prévue, ce qui est faisable en fondant les critères de validation sur l'utilisation du Système Informatisé et son incidence sur la qualité du produit. (13)

De plus, l'étendue de la validation devrait être proportionnelle au risque représenté par le système et, si ce système est employé pour réaliser des actions GMP et non GMP, la possibilité que les fonctions non GMP affectent les opérations GMP est censée être examinée et atténuée de façon appropriée. (7) Pareillement, les incidents en lien avec les Systèmes Informatisés et qui pourraient avoir un impact sur la qualité des intermédiaires ou des principes actifs ou sur la fiabilité des résultats ou des dossiers sont attendus d'être consignés et étudiés. (17) Dans un registre semblable, les manipulations non autorisées et préjudiciables pour les données pendant leur cycle de vie ont pour recommandation d'être atténuées et, si possible, éliminées. Pour les systèmes électroniques sans logiciels configurables ou ne conservant pas de données électroniquement (par exemple des pH-mètres ou des balances, y compris celles couplées avec une imprimante), des contrôles sont mis en place dans le but d'éviter la manipulation délétère des données et la répétition d'essais visant à obtenir le résultat souhaité. (15)

Le procédé des tests de qualification devra être adapté au Système Informatisé en cours de validation. Comme pour les autres qualifications, cette dernière pourra

inclure une Qualification de Conception, une Qualification d'Installation, une Qualification Opérationnelle et une Qualification de Performance. (13)

Outre ces aspects techniques, les opérateurs du système, les manuels d'utilisation et les procédures opérationnelles sont également considérés comme intégrés au sein du Système Informatisé et sont tenus d'être contrôlés.

### **3. Niveaux de l'Intégrité des Données**

#### **A. Niveau 1 de l'Intégrité des Données**

Dans les trois sous-parties suivantes, nous allons nous appuyer sur deux outils : le Data Integrity Maturity Model ou DIMM (se traduisant par le Modèle de Maturité de l'Intégrité des Données) et le DIRA. Ce dernier correspond au Data Integrity Risk Assessment (c'est-à-dire l'Évaluation des Risques liés à l'Intégrité des Données) que nous avons abordé dans les pages précédentes et qui analyse les risques de chaque processus de données et la criticité de celles-ci avant d'en identifier les contrôles et d'en documenter les résultats. (22)

Le dispositif du DIMM, quant à lui, sera véritablement notre fil directeur dans les prochains paragraphes. Il va se baser sur les conclusions du DIRA et déterminer les zones de processus les plus vulnérables à évaluer, définir des facteurs de maturité pour chacune et caractériser le niveau de maturité. (6) Les zones de processus peuvent correspondre à la gestion des données, des propriétaires des données, des systèmes de données, du management des données, etc. et les niveaux de maturité seront divisés en trois dans la suite de ce texte, à savoir « à améliorer » (Niveau 1), « acceptable » (Niveau 2) et « maîtrisé » (Niveau 3).

Les facteurs de maturité pour valider le Niveau 1 de l'Intégrité des Données peuvent comprendre l'instauration d'une sensibilisation annuelle de tout le personnel, la programmation de formations auprès des salariés concernés tels que ceux manipulant des données GMP ou faisant partie du service Qualité, la garantie que chaque donnée puisse être trouvée et utilisée et la documentation des modalités de

sauvegarde et de restauration des informations. La mise à jour et le passage en revue de tous les accès autorisés aux données GMP et l'attribution des rôles de propriétaires et de supports des données pour perpétuer la ségrégation des droits sont tout autant considérés, sans oublier et la vérification que les systèmes de données électriques et papier soient adéquats pour l'usage prévu...

Plus concrètement, tous les sujets ayant trait au contrôle des permissions et des droits d'accès et des modifications sont capitaux pour l'obtention du Niveau 1 de l'Intégrité des Données. D'après la norme 21 CFR Partie 11 de la FDA sur les enregistrements et les signatures électroniques (autrement nommée ERES pour Electronic Records and Electronic Signatures), le maniement des multiples Systèmes Informatisés nécessite tout d'abord d'être effectué exclusivement par les personnes autorisées. En effet, tous les employés ne devraient pas être capables de modifier ou supprimer certaines données, c'est pour cette raison que les droits d'accès aux Systèmes Informatisés leur sont octroyés par rapport à leur travail et qu'une liste des individus habilités est régulièrement actualisée. (23)

Les différents utilisateurs seront amenés à être des administrateurs ou bien opérateurs des données et leurs statuts seront certifiés grâce à l'emploi d'identifiants de connexion propres à changements périodiques pour assurer la conformité et qui serviront aussi à des fins de signatures électroniques. Ces signatures électroniques ont une importance similaire aux signatures manuelles, les salariés aptes à les utiliser doivent par conséquent être informés, identifiés et convenablement documentés. (24)

D'autres facteurs de maturité à intégrer dans le Niveau 1 de l'Intégrité des Données sont le fait d'inspecter si les instruments d'analyse et de production sont adaptés à l'usage souhaité et de contrôler les formulaires vierges, Logbooks et protocoles usités pour remplir les données de fabrication et surveiller la qualité. (20) Cette supervision des cycles de ces supports est autant valable pour le format papier que pour le format électronique (par exemple dans le cadre de la gestion de formulaires

de saisie), tout comme pour les matrices Excel types (matrices de calcul « Templates »). (16)

Finalement, essayer de répondre aux attentes du Niveau 1 sera l'occasion de convenir d'une « Policy », ou procédure de politique générale, reconnaissant la prise en compte de la problématique de l'Intégrité des Données au plus haut niveau de l'organisation. La direction de l'entreprise est ainsi censée l'approuver après un large consensus et contribuer à sa diffusion et formation globale tracée auprès de l'effectif. Cette « Policy » (procédure de politique générale) inclut la compréhension de la définition de l'Intégrité des Données et de son périmètre par la société, la distinction des données qui ne font pas l'objet d'un stockage, d'une gestion électronique ou d'un stockage hybride ou encore la création d'un Data Management ou la nomination d'un responsable général des données. (16)

## **B. Niveau 2 de l'Intégrité des Données**

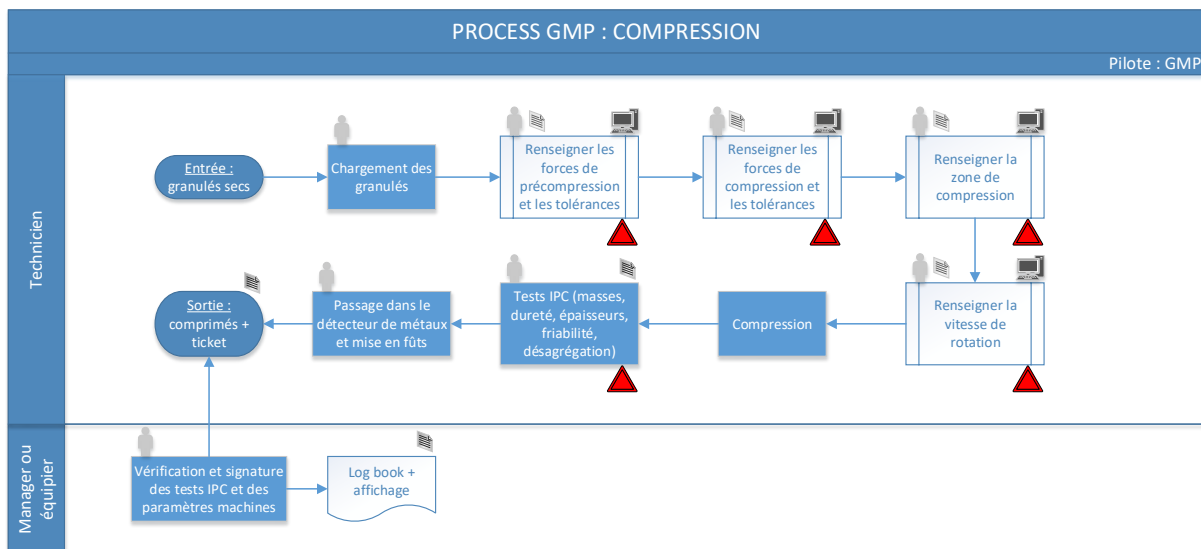
En premier lieu, les facteurs de maturité à déployer pour franchir le Niveau 2 de l'Intégrité des Données sont, pour ce qui est de l'aspect gestion des données, le fait que les sujets d'Intégrité des Données et les risques d'acquisition et de stockage soient intégrés dans la routine de formation des personnes régissant les données GMP, et que la manière de jauger les demandes de partages de données et les réponses à apporter soit réexaminée proactivement et couramment. D'un point de vue procédés GMP, il est conseillé de décrire les flux de données (pour les procédés GMP comportant des données de haute criticité) et de renseigner des revues de données d'Audit Trail (pour les procédés GMP pertinents) afin de comprendre comment les données sont traitées et de déceler les points faibles.

Une certaine idée de la « Governance », que nous expliquerons dans la section suivante, commence à faire son apparition puisqu'il est requis de disposer de processus pour détecter les infractions d'Intégrité des Données (des audits ou diverses auto-inspections pour ne citer qu'eux) et d'une ébauche de plan d'implémentation de l'Intégrité des Données. Vis-à-vis des systèmes de données, il faut que les contrôles de l'Intégrité des Données soient pris en considération de routine lors de leur développement et de leur maintenance et que l'exploitation de

systemes conformes pour atténuer les fragilités de l'Intégrité des Données fasse partie des plans d'investissements.

Le premier genre de documents à établir est la cartographie des processus qui est une solution de maîtrise au même titre que les conditions générales d'évaluation du risque (auxquelles elle est affiliée) et d'autres moyens appropriés pour garantir le maintien de l'Intégrité des Données. Cela consiste à cerner les formalités selon lesquelles les données sont utilisées dans l'organisation, comment elles sont récoltées et tracées, comment une analyse de risques est réalisée dans leur cycle de vie et quelles mesures sont prises pour certifier leur pérennité. À cette fin, au cours de l'étude du risque et de la vulnérabilité des données et pour correctement identifier et maîtriser les Systèmes Informatisés et leurs données, il est essentiel que ces différents systèmes ne soient pas négligés dans le contexte de leur pratique au sein des processus.

Effectivement, l'intégrité des résultats générés par une méthode analytique ou une production ayant recours à une interface informatique intégrée est impactée par la préparation des échantillons et des matières, la saisie des poids ou d'étalons variés dans le système et le mode d'utilisation de ce dernier pour extraire les données et traiter puis enregistrer le résultat final avec leur aide. La synthèse de Data Flow Mappings (ou Process Flowcharts, Cartographies de Flux de Données ou de Processus) est alors la façon la plus claire et complète de compiler ces paramètres et de décider de l'intervalle des revues pour l'analyse de risque en fonction de la sensibilité des données concernées, comme nous pouvons sommairement le voir ci-contre dans la Figure 4. (13)



	Réalisation de l'opération		Support des données			
	Opération manuelle		Opération informatique		Opération papier	Etape critique
	Début/fin		Processus		Sous-processus	Document

*Figure 4 : Data Flow Mapping sur l'étape de compression d'un processus de fabrication*

Les Data Flow Mappings sont supposés évoluer en temps réel de concert avec l'ajustement des processus et doivent faciliter le discernement :

- Des éléments qui participent à la genèse des données
- Des caractéristiques de stockage et de protection des données sources et celles permettant de procéder à une restitution rapide et limpide
- Des lieux de transfert de données et des démarches entreprises pour s'assurer qu'il n'en découle pas de dégradations de la signification des données
- Des actions lancées pour contrôler ou mitiger les risques sur des thématiques ciblées
- Du cycle de vie intégral depuis la création jusqu'à l'archivage ou la suppression des données le cas échéant (16)

Le deuxième dispositif à instaurer est l'ATR, c'est-à-dire l'Audit Trail Review ou la Revue de Piste d'Audit, qui est un historique d'enregistrements sécurisé, recensant



de manière horodatée les changements effectués sur un système, et élaboré par le système lui-même (un ordinateur ou le logiciel de l'équipement si l'enregistrement est électronique). (3) Il assiste la sauvegarde sécurisée des détails du cycle de vie dans un dossier papier ou électronique sans masquer ou écraser le document original. (15) De prime abord, l'objectif de l'Audit Trail en soi est de collaborer à la reconstitution des événements relatifs à toute création, modification ou suppression d'une donnée critique, ce qui fait qu'il est assimilé en tant que métadonnée car il contribue à connaître le « quand », le « qui », le « quoi » et le « pourquoi » d'une modification, quelle que soit son support. (9) Cela se manifeste par le report de la date et de l'heure du changement, du nom de la personne qui l'a exécuté et la raison de cette opération et l'Audit Trail sert subséquemment à prévenir la perte ou l'altération des données, les anti-datations... (17)

L'Audit Trail doit de ce fait faire l'objet d'une revue pour témoigner qu'aucune modification non justifiée n'ait été accomplie, c'est l'Audit Trail Review. Il est recommandé que cet examen soit opéré par les personnels responsables de la revue des documents imprimés ou informatiques (celui supervisant l'activité peut également en être chargé) et cela doit être fait après chaque étape du processus de fabrication et lors de la revue du reste de la réglementation Qualité. En effet, l'analyse de routine des données globales devrait aussi inclure une étude des Audit Trails et la fréquence de ces procédures pourra être déterminée par l'évaluation des risques et l'impact sur la qualité des produits. (24) En cas de Système Informatisé, les Audit Trails sont censés être activés dès que le logiciel est installé et le demeurer à tout moment. Une vérification périodique que l'Audit Trail ait été maintenu enclenché au long du cycle de vie des données est attendue ainsi que des preuves de l'activation de l'Audit Trail et de la revue achevée grâce à des réunions automatiquement planifiées et des immortalisations du système interne et de ses paramètres. (25)

Quand un Audit Trail est dans l'incapacité d'être implémenté dans un système de par sa conception, des mesures alternatives compensatrices doivent être adoptées (comme des programmes complémentaires ou des tests papier) et leur pertinence sera à justifier et à documenter. (15)

### C. Niveau 3 de l'Intégrité des Données

Les derniers facteurs de maturité restant à entamer pour acquérir le Niveau 3 de l'Intégrité des Données sont, du côté de la gestion des données, le fait que les sujets d'Intégrité des Données s'intègrent à la démarche d'amélioration continue et que des objectifs soient fixés régulièrement. D'autre part, pour les procédés GMP, il faut que les descriptions des flux de données (les Data Flow Mappings) soient mises à jour annuellement et que le besoin de revues de données soit, de façon proactive, considéré comme faisant partie intégrante de la conception des procédés.

Il est nécessaire pour que le secteur des systèmes de données soit validé que ceux-ci soient alignés avec la stratégie d'Intégrité des Données du site et de la stratégie globale du service Informatique. Les points concernant le management des données sont l'instauration d'une équipe de management de l'Intégrité des Données, qui dirigerait la feuille de route assurant celle-ci, et l'incorporation des sujets d'Intégrité des Données dans les revues de management.

Ce management de l'Intégrité des Données observé dans sa totalité est appelé la Data Governance et correspond à l'ensemble des arrangements qui fournissent une garantie de la Qualité et de l'Intégrité des Données. Ces dispositions attestent que les données, peu importe le procédé, le format ou la technologie avec lesquels elles sont créées, sauvegardées, traitées, conservées, récupérées et utilisées, authentifient un enregistrement répondant aux principes ALCOA au cours du cycle de vie des données. (15) La Data Governance est entièrement connectée au Système Qualité Pharmaceutique et repose sur trois piliers qui sont le comportement, l'organisation et la technique. (3)

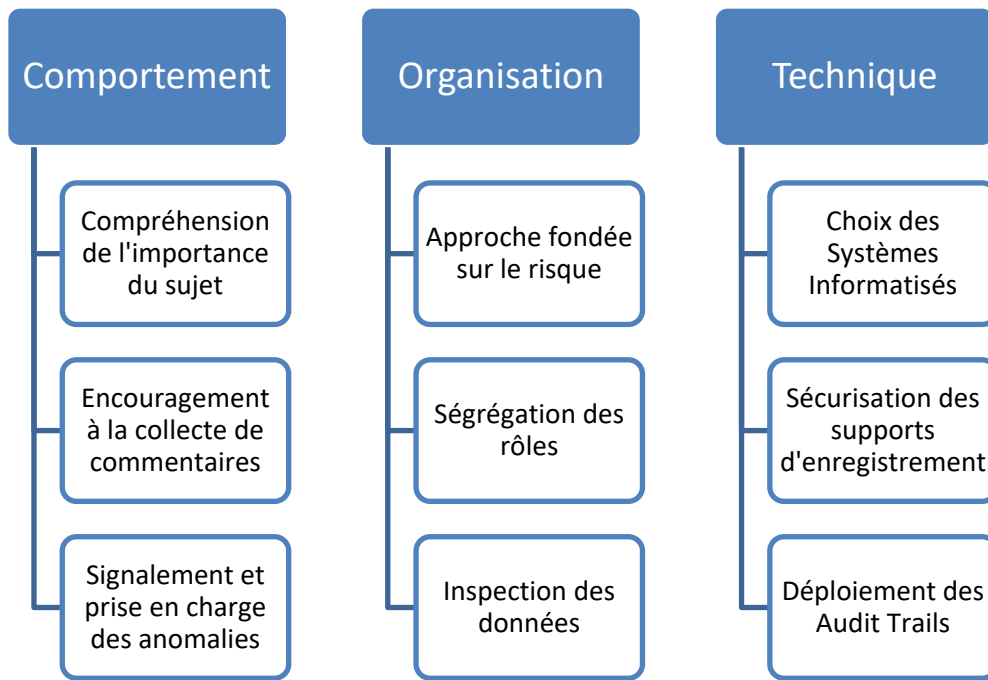
Le comportement est adaptable grâce à la compréhension de l'importance du sujet par tous les collaborateurs (par le biais de formations, de codes de conduite ou d'éthique), l'encouragement à la collecte de remontée de commentaires et à l'amélioration continue, et enfin le signalement et la prise en charge des erreurs, des déviations, des modifications non autorisées, des omissions et des résultats indésirables. (15) Le renouvellement de l'organisation peut être appréhendé en appliquant une approche fondée sur le risque, la ségrégation des rôles, l'inspection

des données et les vérifications de routine, et les révisions périodiques et la surveillance du système. Les dispositifs techniques porteront sur le choix de Systèmes Informatisés ou automatisés conformes et validés, la sécurisation des supports d'enregistrement, le déploiement des Audit Trails et le contrôle et suivi des accès.

Comme tout système, la Data Governance sera bien évidemment passée en revue dans le but de juger la bonne interaction entre les services et la mise en place des actions. (3)

Pour revenir sur le terme de comportement, ce dernier implique les notions de responsabilités du management, de culture d'entreprise et de leadership. (6) Afin de constater une bonne implication de tous les corps de métiers et du management, et une prise de conscience des risques au niveau de la société, une évolution de la culture d'entreprise est parfois vitale. Cette adaptation se traduit par une actualisation et une affirmation des responsabilités de la direction, et une modulation des cycles de formation et des procédures dans ce sens. Chacun des salariés devrait être libre d'avoir l'opportunité de challenger la hiérarchie dans la finalité de la meilleure protection des données. (26) Dans les faits, cela veut dire qu'il n'est pas périlleux de remettre en cause le management ou de reporter des anomalies et que les individus ou les groupes ne s'exposent pas à quelque forme de pressions ou de sanctions. (16)

Dans la Data Governance, il est important que les sponsors du management soient convenablement désignés (par la compréhension de la stratégie et des objectifs, la connaissance des budgets et des ressources humaines et l'expertise technique, entre autres), des indicateurs de performance sont sélectionnés, un véritable projet de mise en application est planifié et les revues périodiques de contrôles pourront entraîner d'éventuelles actions correctives et préventives (CAPA, tracking des incidents, etc.). Les éléments principaux de la Data Governance sont synthétisés dans la Figure 5.



*Figure 5 : Les piliers de la Data Governance*

## **II. L'INTÉGRITÉ DES DONNÉES DANS DIFFÉRENTES INDUSTRIES PHARMACEUTIQUES**

### **1. L'Intégrité des Données dans les industries pourvues d'anciens équipements**

#### **A. Informatique**

Avant toute chose, ces fondements, composantes et niveaux d'Intégrité des Données développés au long de cette première partie ne sont néanmoins peu ou prou extrapolables à tous les établissements ni à toutes les classes de machines. Effectivement, selon la modernité des appareils, les ressources mobilisables et l'engagement de la direction, les principes ALCOA et les demandes des institutions ne peuvent pas être respectés de la même manière.

Pourtant, l'augmentation de données récoltées (passant de 500 téraoctets par an dans le passé à 100 pétaoctets y compris pour une installation de taille moyenne) et l'occurrence d'opportunités découlent de la mondialisation des activités, de la multiplication des Systèmes Informatisés et de l'avènement des e-mails, des réseaux et de la numérisation. (27) Toutefois, ces progrès sont susceptibles de faciliter tout autant que de fragiliser l'Intégrité des Données en faisant apparaître des failles de sécurité et des risques d'erreurs dans les flux de processus de données.

La modernisation et la continuité de l'Intégrité des Données constituent donc un défi de taille pour la plupart des entreprises et plus précisément pour celles qui ont encore recours à un système papier (mais qui sont de plus en plus rares). En fait, des problèmes sont généralement rencontrés par les autorités de Santé lors des contrôles des dossiers papier car ils peuvent être aisément jetés ou perdus. Les autres difficultés souvent remontées évoquent le traitement des formulaires vierges et la conduite des Audit Trails, entre autres.

En outre, les enregistrements hybrides (autrement dit les cas où un instrument électronique est employé pour imprimer des résultats sur papier) sont également déconseillés par les autorités, comme en témoigne l'Annexe 5 de l'Organisation

Mondiale de la Santé stipulant que le remplacement de ces systèmes devrait être une priorité. (28) La guideline PI-041 du PIC/S déclare que les pratiques hybrides ne sont pas encouragées et sont supposées être changées dès que possible car elles requièrent des contrôles supplémentaires en raison de la complexité de l'ensemble des enregistrements et de la capacité accrue à manipuler les données. Une société pourvue d'anciens équipements et présentant toujours ces habitudes de travail est alors chargée de rédiger une description détaillée du système dans son entièreté, en incluant les principaux composants, la façon dont ils interagissent, la fonction de chacun et les contrôles choisis pour garantir l'Intégrité des Données. (29)

Que les approches soient papier ou hybrides, leurs complications du point de vue de l'Intégrité des Données sont l'absence de backup et de traçabilité, les modifications réalisables *a posteriori* et, une nouvelle, fois, l'impossibilité d'aménager des Audit Trails. (30) De surcroît, les modifications de données papier sont assez visibles à l'aide de l'émargement de la date et de la justification du changement, au contraire des enregistrements hybrides ou électroniques rudimentaires. Ces deux catégories de systèmes représentent un défi pour les notions ALCOA car elles ne permettent pas d'isoler l'identification d'un opérateur individuel dans les situations de comptes ou de rôles partagés sans avoir ajouté au préalable un paramètre de contrôle des changements. (31)

Pour ce qui est de l'informatique pure, la qualité et l'intégrité des résultats sont compromises par des logiciels non contrôlés et non validés et des instruments non qualifiés, domaine qui sera éclairci dans plusieurs paragraphes ultérieurs. Dans l'optique d'entreprendre cette amélioration, les industries disposant d'anciens équipements et systèmes devront commencer par jauger les priorités et se focaliser sur les systèmes devenant prochainement obsolètes ou cassés. (28)

## B. Équipements

Pour commencer, tout comme pour les Systèmes Informatisés, les établissements possédant des équipements désuets doivent débiter leur action en vérifiant que les équipements soient adaptés à l'usage souhaité. Cela s'effectue en passant en revue les équipements afin d'en coter les risques Qualité et par rapport aux patients, puis en décidant lesquels sont à renouveler parmi les plus archaïques, ceux arrivant en fin de vie et ceux sans Audit Trail activé ou comptes nominatifs. Durant ce laps de temps, il faut penser à établir des contrôles opérationnels additionnels pour pallier aux écarts et maîtriser les risques. (27)

À l'étape de l'acquisition d'un nouvel équipement, de nombreux facteurs vont être pris en compte découlant de l'attention soutenue accordée à l'évaluation proposée des contrôles de l'Intégrité des Données. Cela est compréhensible puisque 40% des citations de la FDA à la suite d'achats d'instruments inadéquats sont dues à l'absence de contrôles logiciels installés avant l'achat de l'appareil. Ces contrôles peuvent toucher à la déficience de sécurité, l'inaptitude à reconnaître et résoudre les conflits d'intérêts, l'absence d'Audit Trail, la gestion des utilisateurs de la machine...

En ce qui concerne ce dernier critère, une séparation stricte des tâches est indispensable pour que les administrateurs soient indépendants des opérateurs. Une liste recensant chaque utilisateur et son rôle est par conséquent censée être générée par un système capable, ce qui est tout à fait envisageable pour un équipement ou un système en réseau mais difficilement faisable pour un élément autonome. (29)

Le logiciel inclus a bien entendu l'obligation d'être prêt à l'emploi à la réception de l'instrument. (28)

Sur le terrain, c'est habituellement le transfert de données entre les systèmes et les équipements au cours du processus de fabrication qui conçoit et provoque des risques pour les données et les métadonnées associées essentielles pour préserver le contenu et la signification des exigences GMP. Comme explicité dans les pages précédentes, l'Intégrité des Données sollicite de définir et estimer les risques et protéger les données pendant leur cycle de vie. Cela se concrétise au sein des

entreprises pourvues d'anciens équipements par le fait d'investiguer et de renseigner un document argumentant et appuyant chacun des transferts de la création initiale de l'identification des matières premières jusqu'à la mesure, l'enregistrement et la déclaration de tous les paramètres critiques des processus et Attributs Qualité Critiques. Les ultimes stades aboutiront à l'examen minutieux des données de libération des lots et des rapports d'exception rassemblés de l'intégralité du processus de fabrication, et la conservation à long terme de ces données. (30)

Pour poursuivre sur le contrôle, la validation et la qualification des instruments mentionnés ci-dessus, l'étalonnage est le palier consécutif à l'achat d'appareils satisfaisants sur l'aspect de l'Intégrité des Données. (21) L'étalonnage prévient les résultats inexacts ou erronés et joue ainsi un rôle clé dans la réduction des erreurs de laboratoire, ce qui amène à une diminution des coûts, une augmentation de la productivité, une baisse des remarques lors d'audits et une considération des normes réglementaires en matière de développement de médicaments (en assurant la traçabilité et l'intégrité des données du début à la fin du processus de développement).

L'étalonnage est l'un des moyens les plus fiables et répandus pour faire perdurer la précision et l'exactitude de la machine vu qu'il est crucial de synthétiser des résultats reproductibles et de maintenir l'Intégrité des Données pour contribuer à atténuer le risque d'erreurs. Un système de gestion de l'étalonnage est amené à être utilisé, de préférence implanté au cœur d'un ELN (pour Electronic Lab Network, soit Réseau de Laboratoire Électronique), dans l'objectif d'assister les laboratoires à suivre et à reproduire la méthode d'étalonnage. (32) Cette option comprend la programmation d'un calendrier de maintenance et d'étalonnage et permet l'exploration des erreurs de production. En effet, des équipements non étalonnés, surtout s'ils sont trop vétustes, peuvent être à l'origine de perturbations telles qu'une augmentation du temps d'arrêt, des défaillances inattendues, un endommagement d'autres parties d'instruments, un gaspillage, un protocole non sécurisé, etc.

Une normalisation internationale des standards et procédés d'étalonnage est à relever, supportant une plus grande cohésion entre les sociétés dispersées d'un



même groupe ou d'entités distinctes et simplifiant l'achat d'un appareil approprié dans le cadre de la remise à niveau de l'inventaire approuvé par la direction. (33)

### C. Management

De prime abord, dans le cas des industries disposant de machines, techniques ou systèmes révolus, une documentation papier existe encore, et le service Qualité sera de ce fait missionné pour examiner les formulaires vierges, les modèles et patrons, les supports, etc. dans le but d'en certifier leur sûreté s'ils ne peuvent absolument pas être remplacés ou déplacés électroniquement. (29)

Le haut management doit superviser la transition et la disparition des dossiers papier mais il ne faut pas non plus que les solutions de substitution soient mal intégrées, comme des feuilles de calculs non protégées qui nécessitent un transfert d'informations à la main entre les systèmes et les instruments par exemple. Ce type de manipulation manuelle limite l'accessibilité, demande beaucoup de temps et de main-d'œuvre et rend les données vulnérables aux erreurs. (34)

Les responsables devront aussi garantir que les données de même que les métadonnées soient disponibles dans un format lisible et récupérable durant la durée de la période de conservation de ces données. Quant aux autres principes ALCOA et ALCOA +, les systèmes à compléter à la main par les opérateurs se révèlent souvent dans l'incapacité de constituer un enregistrement contemporain ou d'être originaux, précis et entiers, or il est primordial d'attester que les documents soient originaux, que leurs versions soient papier ou électroniques.

Le statut vital de la direction est de gérer et de maîtriser le risque dans l'intention de ne pas laisser ce dernier affecter la sécurité des patients. Pour ce faire, il lui est nécessaire d'avoir une culture de la Qualité et des procédures conformes et de vérifier si le personnel analyse correctement les données et détecte les problèmes avant qu'ils n'aient un impact sur la qualité des produits et, en fin de compte, sur la sécurité des patients. (31)

Pour finir, à cet échelon-ci, certaines entreprises ont entamé la mise en place d'une architecture IT (Information Technology, se traduisant par Technologie de l'Information) avec des serveurs sécurisés, la revalidation des applications selon leurs cibles et leurs influences, l'éclaircissement des rôles et des habilitations, la configuration d'Audit Trails pour la traçabilité et la signature d'un contrat d'infogérance spécifique auprès d'un prestataire choisi sur la base de critères d'Intégrité des Données. (27)

## 2. L'Intégrité des Données dans les industries disposant d'équipements modernes

### A. Informatique

La première étape à enclencher pour les établissements en possession d'appareils récents est, à l'aide des Data Flow Mappings de processus, de déceler la criticité et, encore plus importante, la vulnérabilité des données extraites de chaque Système Informatisé. Cela regroupe les conditions d'identités partagées des utilisateurs ou bien le fait que des fichiers de données soient stockés dans des répertoires qui peuvent être supprimés. Ce genre de vulnérabilités sera à corriger avec l'assistance de contrôles techniques. Par ailleurs, il est à noter que même si un système est étalonné, qualifié et validé, le besoin de protéger les données demeure intact et il faudra donc mettre des efforts en œuvre pour amoindrir les vulnérabilités discernées. (29)

Pour continuer avec notre exemple cité plus haut, un des moyens d'amélioration les plus abordables en termes de finances et de temps et *de facto*, un des plus populaires, provient du fait que les systèmes électroniques automatisés sont perfectibles s'ils restreignent l'accès à leurs fonctionnalités et s'ils témoignent que les entrées et sorties sont attribuables. (35) Par conséquent, l'investissement majoritaire est fréquemment l'instauration de contrôles sur les ordinateurs pour empêcher la suppression ou le changement de nom des dossiers ou la modification de la date d'un enregistrement.

Une préoccupation particulière est la recherche de contrôles pour devancer les « données orphelines », c'est-à-dire les résultats qui sont acquis mais qui ne sont pas renseignés ou examinés. Un bon aperçu de données orphelines est lorsque des tests sont exécutés sous les auspices d'une investigation ou en préparation de l'exécution d'un échantillon qui ne sera jamais inclus dans l'enquête formelle ou le rapport d'exécution.

Le danger pour l'Intégrité des Données est que ces résultats d'échantillons non déclarés sont susceptibles, délibérément ou non, de dissimuler la découverte de données défailtantes ou de servir de moyen pour un collaborateur de transformer les conditions de fonctionnement dans le but d'obtenir un résultat correct, d'où l'intérêt de trouver les contrôles opportuns à sélectionner. (31)

Les données auto-enregistrées, autrement dit les données qui ne sont pas saisies instantanément à partir d'un système d'automatisation en réseau, représentent une autre source d'inquiétude. C'est pourquoi, quelles que soient les données ou les situations, il est impératif de bien réfléchir au moment où le principe des « quatre yeux » devrait être employé et quand une « deuxième vérification » est à appliquer.

Il est recommandé de lancer ces évolutions en se concentrant tout d'abord sur les petites technologies et les systèmes et équipements minimes à faible impact GMP, comme de la maintenance préventive, de la surveillance environnementale ou des économies d'énergie... (36)

De plus, pour les sociétés recensant des équipements et des systèmes modernes, il convient de sauvegarder toutes les données des ordinateurs présents en production et en analyse. Ceci est possible de deux manières différentes : la première consiste à se reposer sur un logiciel de sauvegarde et de gestion des données qui préservera sur un serveur la totalité des informations et valeurs du PC. (35) Cette idée requiert quelques exigences comme un poste suffisamment récent ou connecté au réseau.

La seconde façon revient à travailler de concert avec le service Informatique et à directement récupérer le disque dur de l'ordinateur en vue de le copier en toute sécurité. L'intervalle de choix pour la réitération des enregistrements sera apprécié selon des critères de risque variés et pourra aller d'une sauvegarde journalière à annuelle.

À cette phase-ci et d'après la modernité des locaux et des machines, les obstacles à l'intégrité des Données persistants sont l'absence d'alarme automatique en cas d'excursion et la carence en Audit Trails. (28)

## **B. Équipements**

Dans la continuité des systèmes contemporains décrits précédemment, les agences de régulation préconisent de relier les équipements à des PC, par exemple par l'intermédiaire de plates-formes logicielles. Ces passerelles sont ajustables si une connexion avec plusieurs instruments est voulue, au travers d'un seul programme standard commun. Un poste externe à l'appareil permet de mieux collecter les résultats et les données brutes, de visualiser les méthodes et les connexions des utilisateurs, de gérer et d'approfondir les risques de conformité et d'éliminer la plupart des risques par contrôles techniques. Enfin, cela facilite le processus de validation puisqu'il ne sera effectué qu'à une reprise. (28)

Pour aller plus loin, les systèmes de gestion de l'étalonnage performant plus efficacement en tandem avec un ELN (mentionnés dans une sous-partie antérieure) peuvent être agrémentés d'options telles que la jonction de la machine aux expériences et aux protocoles et sa traçabilité en direct de cette dernière à partir de la page de l'expérience. (33)

Le contrôle des équipements actuels se fait également en passant par la centralisation des données, la simplification et la sécurisation des processus pour les salariés en première ligne et l'incorporation d'un ERP (pour Enterprise Resource Planning, retranscrit en Progiciel de Gestion Intégré). Ce système de gestion de la production sert à sécuriser l'historique et les résultats et il est joignable à d'autres logiciels pour accéder à une visibilité complète du procédé d'étude. (27)

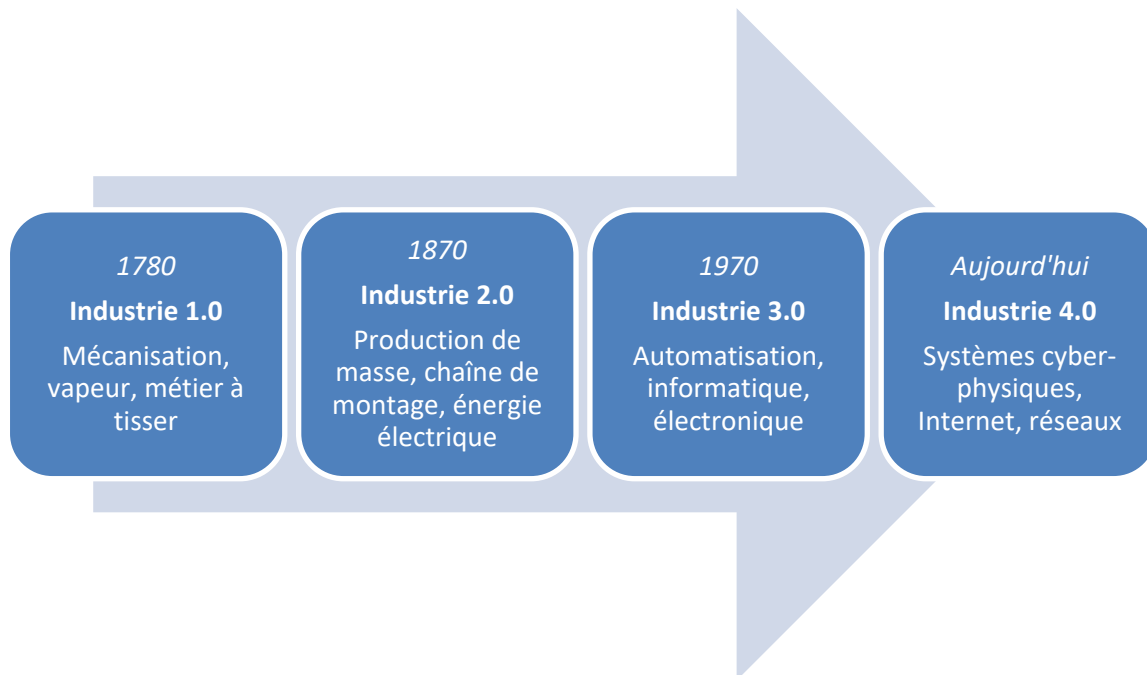
Pour la sécurité des systèmes et des appareils, le PIC/S écrit qu'il est préférable d'avoir une séparation stricte des tâches avec des administrateurs indépendants des utilisateurs, y compris pour les systèmes autonomes. La guideline PI-041 informe de surcroît sur les contrôles des périphériques USB sous forme de clés USB ou de disques durs externes mais aussi d'appareils photos, de smartphones, etc., dont les canaux de communication et les ports concernés doivent être désactivés par défaut et activés uniquement si besoin. Effectivement, verrouiller la reconnaissance d'outils extérieurs sur les instruments ou utiliser des dispositifs dédiés réduit l'introduction de programmes malveillants corrompant les données dans une organisation.

Ensuite pour les équipements modernes, les systèmes de codages ont souvent des propriétés d'Audit Trail ou « d'historique » et il sera finalement nécessaire de les activer. À ce niveau de modernité et d'impératifs, dans certains cas, si les systèmes internes ne disposent pas de ce qui est demandé, comme l'aptitude à capturer des données à l'instant de l'analyse ou de l'activité, une refonte du logiciel deviendra obligatoire. (29)

Chaque stade du processus de fabrication est supposé être surveillé plus attentivement avec la production continue. Des approches semblables à la PAT (Process Analytical Technology pour Technologie Analytique des Procédés) et aux flux de travail de la MAM (Multi-Attribute Method ou Méthode Multi-Attributs, qui caractérise et quantifie les attributs qualité des produits) seront donc utiles pour aider les industriels à régenter et protéger leurs données.

Ce passage du traitement traditionnel par lots au traitement continu suscitant un intérêt accru est corrélé à la montée en puissance des concepts pharmaceutiques 4.0. Pour situer le contexte et cette notion, dans un premier temps, l'industrie 1.0 des années 1780 tournait autour de la mécanisation, de la vapeur et du métier à tisser avant de progresser vers la production de masse, la chaîne de montage et l'énergie électrique aux environs de 1870 avec l'industrie 2.0. (37) L'industrie 3.0 de 1970 se basait sur l'automatisation, l'informatique et l'électronique pour aboutir aux systèmes

cyber-physiques, à Internet et aux réseaux de l'industrie 4.0 de nos jours. (38) Ces progrès peuvent être constatés dans la Figure 6.



*Figure 6 : L'évolution de l'industrie dans le temps*

Ainsi, les processus continus peuvent être configurés et accomplis plus rapidement que les procédures par lots traditionnels, ils diminuent le besoin d'intervention de l'opérateur sur la machine et ont recours à la surveillance en ligne pour que des améliorations puissent être apportées pendant la production. Cependant, en amont, les méthodes continues réclament plus de connaissances sur le processus de production, elles-mêmes ne découlant que de l'analyse des données de développement convenablement récoltées.

Cette modération du niveau d'intervention manuelle en ligne que les scientifiques sont tenus de réaliser au long de tous les processus et cette transition pour une fabrication modulaire où des ajustements et améliorations continus peuvent être essayés (sur la base de capteurs en ligne et de surveillance des processus) sont au final envisageables grâce aux technologies innovantes. De cette façon, les données numériques et leur intendance gagnent en importance pour optimiser la fabrication pharmaceutique et fournir des produits de haute qualité. (39)

### C. Management

À partir du moment où une entreprise possède des instruments récents, son comité de management participera au verdict portant sur le remplacement d'une opération manuelle par un Système Informatisé. Les membres impliqués tiendront compte de quatre conditions qui sont « aucune diminution de la qualité du produit », « pas de niveau réduit de contrôle des processus », « aucune norme abaissée d'Assurance Qualité », « aucune augmentation du risque global associé au produit ». (40)

D'un point de vue plus général, la direction d'un établissement est en charge de définir une stratégie de sélection et d'adoption de systèmes de rang supérieur. (41)

Les divers responsables nommés de la société ont pour mission d'aligner les attentes sur la capacité d'un processus, d'un site ou même d'une personne. Si l'infrastructure ou les ressources ne sont pas prévues et à disposition, des erreurs peuvent en résulter et il peut s'ensuivre une plus grande probabilité de falsifications des données pour tenter d'accéder aux objectifs.

De ce fait, établir et rester dans les limites d'un espace de conception (dans le cadre d'une approche Quality by Design) qui conduit à un produit sûr et efficace est fondamental pour des programmes significatifs de l'Intégrité des Données et Data Governance. Compte tenu de la variabilité de la technologie, les industries devraient être conscientes des buts pouvant être atteints dans une mesure réaliste et faire concorder leurs critères de réussite (ni trop ambitieux, ni trop laxistes).

Par ailleurs, il est du devoir des équipes de commencer à réfléchir à la manière dont les fichiers seront conservés dans un format accessible une fois que le système aura atteint son obsolescence dès l'étape de la conception dudit Système Informatique ou d'une automatisation. En effet, l'atténuation des périls en lien avec l'archivage, le transfert de technologie, la stabilité et la validation et vérification continue des processus dépend d'une planification éclairée de l'obsolescence. (31)

Comme abordé plus tôt, la vigilance du haut management vis-à-vis des données orphelines est censée comprendre un assemblage de politiques, de procédures, de formations, de surveillances et de mesures telles que des inspections régulières. La visée de ces visites est de s'assurer qu'aucune donnée orpheline n'est relevée et d'attester que toutes les opérations soient conformes aux politiques et procédures prévues.

Pour se pencher sur les Audit Trails du côté managérial, celui-ci doit être exécuté par des gens formés et préférentiellement par la fonction métier. En pratique, cela veut dire que le choix se dirigerait plutôt vers des opérateurs, des ingénieurs ou des analystes mais pas le groupe IT (qui, avec le service Qualité, a tout à fait le droit de les superviser en revanche).

C'est un examen fondé sur les risques qui réclame une compréhension des processus et se focalise par conséquent sur les changements apportés aux données, mais également aux métadonnées, susceptibles d'avoir une incidence sur la production.

L'équipe Qualité, pour sa part, valide les indicateurs et le système d'audit pour prouver que le système répond aux besoins et qu'il est adapté à l'objectif ciblé, c'est-à-dire qu'il offre un contrôle technologique de l'Intégrité des Données. (31)

### **3. L'Intégrité des Données dans les industries 4.0**

#### **A. Informatique**

Pour finir, au vu du degré technologique démontré par les industries pharmaceutiques 4.0, le PIC/S a décrété dix considérations particulières relatives à l'Intégrité des Données. Les directives obligatoires parmi elles à la suite de leur rattachement aux règlements officiels sont celles en rapport avec la validation des systèmes, leur inventaire, l'évaluation périodique, le transfert de données et l'Audit Trail. À ce palier, l'étalonnage, la qualification et la validation sont encore plus rigoureux en incluant des Systèmes Informatisés mis à jour durant des périodes



opportunes sans oublier les correctifs de sécurité et les nouvelles versions des applications. (29)

De plus, les Audits Trails ont désormais pour consigne de couvrir au moins trois catégories principales :

- Les instruments (sur leur configuration et de leur fonctionnement)
- Les données (à propos du suivi de méthodes d'instruments, de séquences, de rapports électroniques...)
- L'administration des utilisateurs (pour enregistrer les utilisateurs et quand ils activent le système) (38)

Néanmoins, certaines de ces attentes, y compris les facultatives, sont estimées comme surpassées dans la guideline PI-04 selon quelques spécialistes prenant par exemple appui sur les recommandations d'enregistrer les connexions mais aussi les déconnexions. Le fait de considérer comme critère « objectif » la durée entre la disponibilité d'un correctif logiciel et l'instant où le correctif est appliqué semble également excessif car réduire implicitement l'efficacité d'une stratégie de cybersécurité au temps nécessaire au déploiement d'un correctif de sécurité est restrictif. Nous voyons ici qu'à ce seuil élevé d'Intégrité des Données, il peut finalement y avoir des contraintes et des exigences mais il faut surtout retenir que chacun des risques doit être évalué et que toutes les approches doivent être justifiées et documentées. (29)

Dans le prolongement de cette idée, il est essentiel de penser à la cybersécurité, qui est la démarche de protéger les valeurs des procédés, les recettes et méthodes et tout ce qui touche à la propriété intellectuelle des accès non autorisés ou malveillants (qu'ils soient physiques par le biais de matériels USB ou électroniques par des connexions réseaux et digitales).

D'autres référentiels semblables à l'ISA/IEC 62443 indiquent les processus et procédures facilitant l'obtention du niveau de sécurité désiré à l'installation du système puis en cours de phase opérationnelle. Cela englobe le conseil de ne pas se placer sur un réseau avec un accès direct à un Internet public mais privilégier un

segment de réseau cloisonné par un pare-feu et séparé de l'Internet public et des réseaux d'affaires locaux par une « zone démilitarisée ».

Des outils perfectionnés de la classe des algorithmes sont capables de détecter une activité réseau excessive et d'aider à certifier que les ressources d'un périphérique sont priorisées sur la stratégie de contrôle et d'enregistrement au lieu de servir le trafic réseau. L'efficacité de la maintenance peut sur cette lancée être améliorée en tirant parti de l'habilité des logiciels à se connecter à des experts en temps réel. (42)

Au fur et à mesure, de plus en plus de technologies innovantes font leur apparition au service des Sciences Pharmaceutiques telles que l'Intelligence Artificielle, l'apprentissage automatique, le Cloud computing, l'IOT (l'Industrial Internet Of Things, soit l'IIDO, l'Internet Industriel Des Objets, terme qui sera expliqué ci-dessous), l'analyse de données avancée, la réalité augmentée, le jumeau numérique, l'impression 3D pour des prestations plus personnalisées, le traitement des mégadonnées, l'interconnectivité, la robotique collaborative et bien plus. (43)

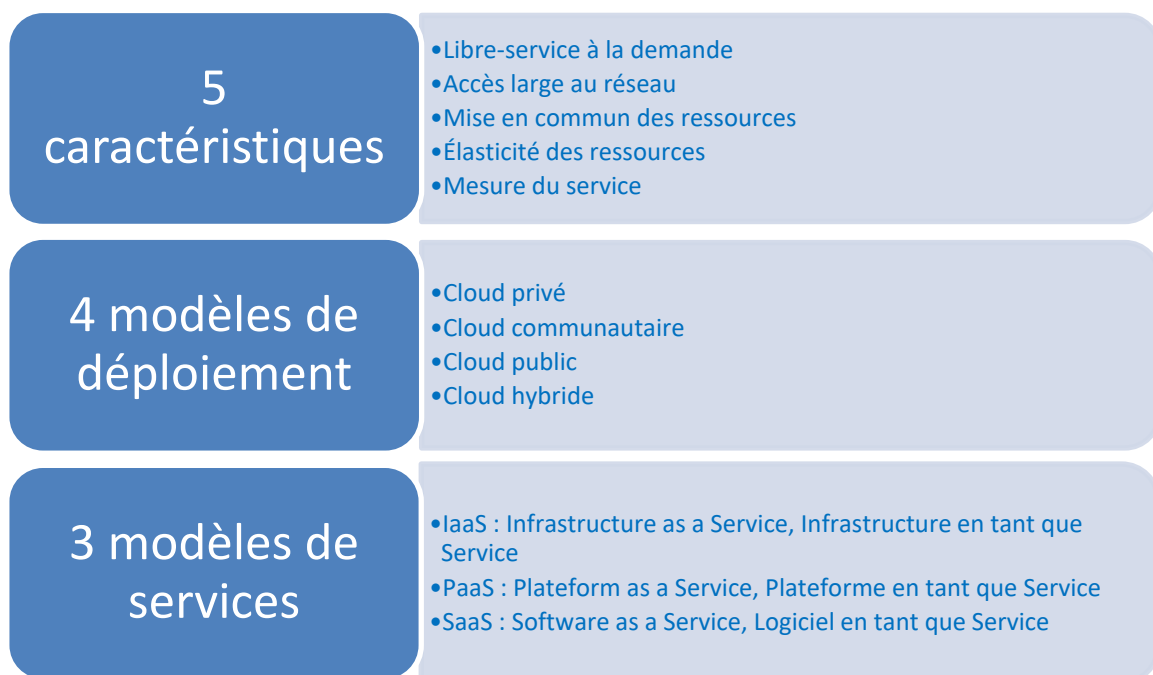
En premier lieu, l'IOT décrit la numérisation des actifs, des opérations et des processus industriels. Cela fait référence à une chaîne d'approvisionnement digitale qui permet à d'énormes volumes d'ensembles de données de sortir des systèmes industriels d'une usine et de se retrouver entre les mains de professionnels aptes à interpréter et transformer ces informations en solutions commerciales intelligentes. (44)

Quant au jumeau numérique, il s'agit d'une simulation virtuelle qui analyse les données immédiatement afin d'éviter les problèmes avant qu'ils ne surviennent. Les fabricants vont pour cela comparer continuellement les données du processus réel avec les données attendues par le jumeau numérique et ajuster le processus de fabrication si besoin. (38)

En outre, les outils, appareils et Systèmes Informatisés ont pour spécifications d'être sur une plate-forme ouverte, basée sur le Cloud avec des standards de données communs, pour connecter les instruments et équipements choisis, épauler le partage

de données et empêcher la perte de données dans le lot de production ou le système de surveillance environnementale. (39) Ce Cloud est composé de 5 caractéristiques essentielles (un libre-service à la demande, un accès large au réseau, une mise en commun des ressources, une élasticité rapide et une mesure du service), de 4 modèles de déploiement (un Cloud privé, un Cloud communautaire, un Cloud public et un Cloud hybride) et de 3 modèles de services. (45) Ces trois options sont listées ci-dessous ainsi que dans la Figure 7 :

- L'IaaS (Infrastructure as a Service, Infrastructure en tant que Service) qui externalise le matériel physique et la logique requise à sa maintenance
- La PaaS (Platform as a Service, Plateforme en tant que Service) acceptant le développement et le déploiement de logiciels sans avoir besoin de les acheter
- Le SaaS (Software as a Service, Logiciel en tant que Service) exécute, lui, des applications logicielles sur une plateforme basée sur le Cloud et aucun logiciel n'est installé localement



*Figure 7 : Le Cloud*

Quel que soit le module, la sécurité sera intégrée, l'accès sera global, l'Audit Trail inhérent et l'AI (Artificial Intelligence ou Intelligence Artificielle) pourra être employée. (36)

Ensuite, la nouveauté de la Pharma 4.0 est sa spécificité à ne pas attendre de vérifier le produit uniquement à la fin du processus de fabrication mais de passer à la surveillance en temps réel à la place. Dans cette optique, il est possible de s'accompagner de systèmes connectés pour instaurer un système de production continue vraiment agile où les procédés s'ajustent automatiquement en fonction des données collectées. (35) Le contrôle des procédés de fabrication sera toujours présent en automatisant et éliminant toute intervention humaine ou manuelle grâce à l'exploitation de logiciels qui prendront des décisions basées sur les informations récoltées à partir des systèmes connectés susmentionnés (et, si possible, en pilotant machinalement les actions comme les modifications effectuées sur le processus de production).

Enfin, un de ces systèmes ajoutera des simulations compatibles avec l'AI pour accentuer le Machine Learning (ou ML, traduit par l'Apprentissage automatique) et le Deep Learning (autrement dit DL, littéralement l'Apprentissage Profond) menant à un système d'auto-apprentissage constant qui propose des solutions et prend des mesures pour optimiser la qualité des produits. Les systèmes d'information sont donc la base de l'intégration et de la traçabilité ainsi que de l'automatisation, écartant les interventions manuelles ou humaines inutiles et diminuant la surveillance réglementaire. (39)

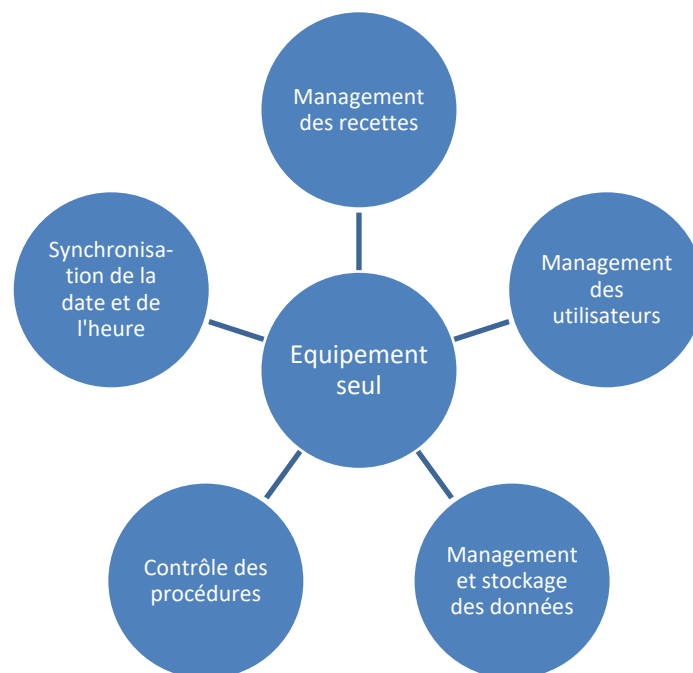
Pour revenir sur les thématiques précédentes, le Machine Learning représente un moyen d'atteindre l'AI par « force brute », ce qui équivaut à un calcul ultrarapide perpétuel qui juge toutes les options à la recherche d'une issue. Le Deep Learning, de son côté, correspond à des algorithmes reposant sur la structure et la fonction de l'apprentissage humain pour cascader et transformer les données à travers des couches de traitement.

En synthèse de ces technologies, l'AI peut apprendre des activités humaines comme la planification, la compréhension du langage et la résolution de problèmes et, de ce fait, offrir des analyses avancées pour produire des conclusions et des prédictions significatives à partir d'ensembles de données. À cette fin, il est avantageux de

statuer en amont sur la conception et l'architecture du système, la capture et le stockage des données et l'implémentation et l'automatisation des Audit Trails suivant les directives pour mieux donner l'opportunité à l'AI d'analyser les données recueillies et de déclencher des alertes en cas de non-conformités, d'erreurs inattendues, d'incohérences ou de soucis d'Intégrité des Données. (36)

## B. Équipements

Historiquement, le fonctionnement autonome des équipements fut l'approche de conception la plus couramment pratiquée dans l'environnement de production pharmaceutique, assignant des tâches pour générer, stocker et reporter des données en interne. Le principe était de considérer chaque pièce de machine comme une « île » autonome et indépendante mais cela entraînait de la complexité et de l'inefficacité au sein d'un atelier de fabrication bondé. Les différents aspects d'un système autonome articulé autour d'un équipement sont dessinés dans la Figure 8.



*Figure 8 : Le fonctionnement parcellisé d'un système autonome*

Cela est en partie expliqué par l'attribution de toutes les exigences caractéristiques de contrôles de connexions avancées dans chaque unité autonome, ce qui conduit à

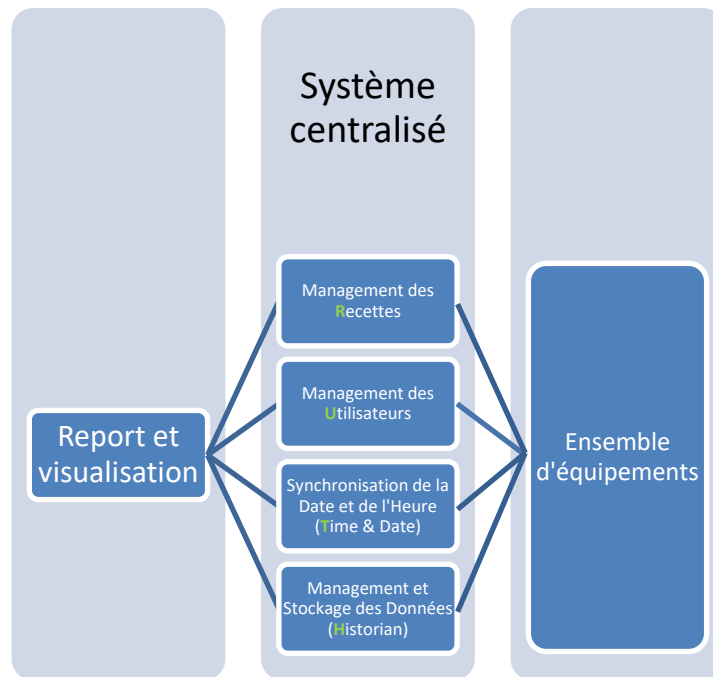
un processus fragmenté, coûteux et compliqué à qualifier et à maintenir dans l'environnement de travail. Ces attributions regroupent les identifiants utilisateurs et les mots de passe uniques, les privilèges d'accès conçus pour séparer les tâches, la gestion adéquate des méthodes, les variables date et heure, le système de stockage, les Audit Trails et les reporting personnalisables.

La normalisation des appareils peut bien évidemment restreindre la variété des modèles, des fournisseurs et des systèmes, mais la variation elle-même ne peut être dissipée. (41)

Les technologies innovantes délivrent alors de nos jours des solutions et opportunités avec le soutien des progrès sur les réseaux, les interfaces et les protocoles de connectivité, ce qui permet l'intégration verticale des logiciels et des processus d'instruments. L'intégration verticale mène les équipements et les systèmes de différents fabricants à évoluer ensemble efficacement tout en respectant les réglementations des autorités sanitaires. Effectivement, ces systèmes de niveau supérieur facilitent la séparation et la spécialisation des fonctions telles que les rapports de données, le stockage et la création de données.

Concrètement, chaque unité intégrée verticalement est unie à un système centralisé où les données de Bonnes Pratiques et les contrôles de gestion associés sont incorporés. Ces systèmes et contrôles se matérialisent par des interfaces qui induisent un échange automatique de données et font que l'intégration verticale ne repose pas sur le contrôle central d'un opérateur.

En accord avec l'Intégrité des Données, les unités citées ci-dessus sont accessibles via des identifiants et des mots de passe de connexion utilisateurs uniques, leurs recettes sont gérées par le système de gestion central, la date et l'heure sont synchronisées de manière centralisée également, de même que le stockage des données. Tout ceci forme l'acronyme RUTH (Recipe management, User management, Time & date synchronization, Historian data storage & management) et rend la machine « plus légère », la laissant seulement génératrice de données, tout comme nous pouvons l'observer dans la Figure 9.



*Figure 9 : Les paramètres du système vertical RUTH*

Nous pouvons voir que les spécifications dans le domaine des données ALCOA+ peuvent être satisfaites presque entièrement par RUTH, ce qui réduit l'effort global et les coûts de développement, de mise en œuvre, de qualification et de maintenance de l'instrument dans l'environnement de travail. (41)

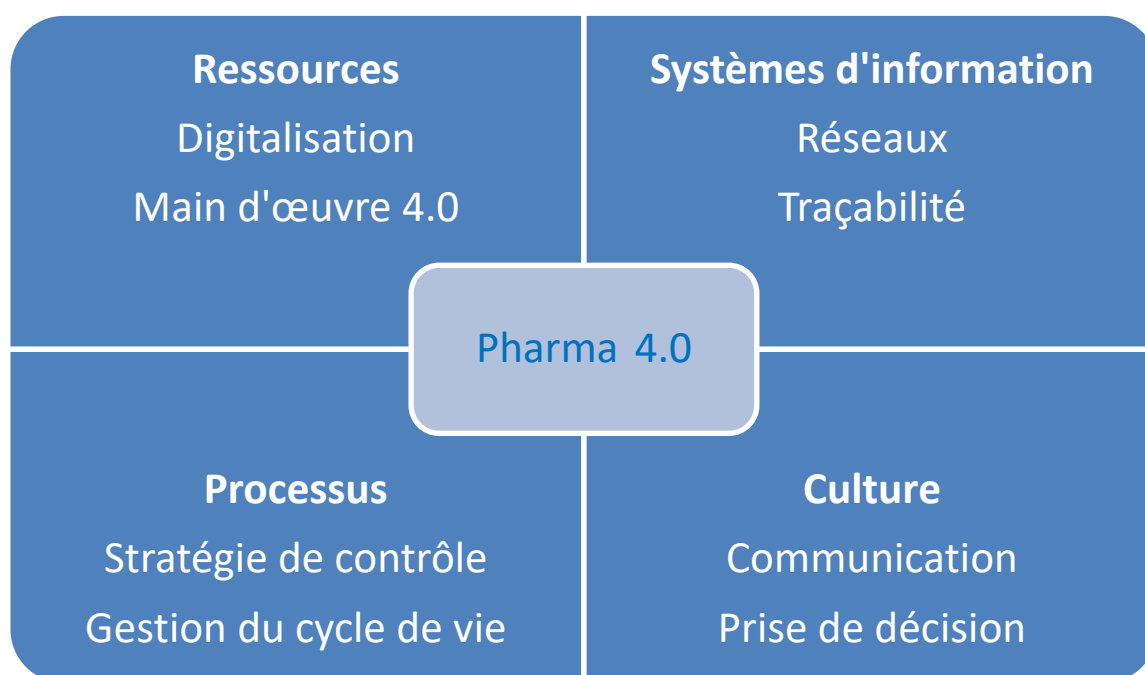
De cette mise en réseau verticale des systèmes de production intelligents cyber-physiques découle l'installation de capteurs conçus pour garantir des données de production ou logistique rapidement disponibles. Ils permettent ainsi des décisions plus promptes, une utilisation des ressources plus rentable, une réaction rapide aux niveaux de stock et une anticipation des soucis de maintenance. (34)

Au final, ces dispositifs sont supposés simplifier et perfectionner les examens en soulignant ce qui est essentiel lorsque le système est validé, comme où trouver des données et des métadonnées significatives à extraire ou des modifications apportées aux données critiques. (31)

### C. Management

D'après l'ISPE, une organisation nécessite quatre éléments pour passer dans la catégorie des établissements pharmaceutiques 4.0, catégorie construite sur un certain degré de maturité numérique et situe l'Intégrité des Données By Design à sa racine. Ces quatre socles sectorisés dans la Figure 10 sont les ressources (comprenant la digitalisation et une main d'œuvre 4.0 disponible et qualifiée), les systèmes d'informations (incluant les réseaux et la traçabilité), les processus (englobant la stratégie de contrôle et la gestion du cycle de vie) et la culture (avec la communication et la prise de décision).

En ce qui concerne ce dernier point, une culture de communication forte, avec un leadership désireux d'engendrer des expériences positives grâce à la technologie, est primordiale. (39)



*Figure 10 : La maturité numérique de l'Intégrité des Données By Design dans la cadre de la Pharma 4.0, d'après <https://ispe.org/initatives/pharma-4.0>*

De plus, des stratégies de contrôle sophistiquées aident à manipuler de multiples Attributs Qualité Critiques et à répondre aux revendications d'un portefeuille de produits et de modalités complexe. (34)



Aussi, avec les nouvelles technologies, les données ne sont plus exclusivement exploitées pour garantir la conformité mais pour obtenir des informations sur les processus et les opérations. Elles sont par conséquent transformées en connaissances sur les activités critiques et sont profitables pour l'optimisation des procédés, l'amélioration continue, l'excellence opérationnelle, la publication en temps réel et la validation continue.

Celle-ci est constituée d'enregistrements et de surveillances en continu des sources de données des processus pour les faire devenir plus pratiques, réalisables et rentables en ayant recours à des techniques analytiques avancées fondées sur le Cloud et l'Intelligence Artificielle. (36)

Pour poursuivre sur les divers abords du management général dans les entreprises 4.0, il existe une vérification judiciaire dans le but de sélectionner des cibles à risque élevé (selon des critères de déclenchement fixés au préalable en commun avec les membres directeurs). Puis, ces cibles seront examinées et tracées de la source de données initiale à la sortie finale pour détecter tout acte répréhensible. Cette approche peut être proactive dans le cadre de la supervision associée aux contrôles de gestion du site, ou en réponse à une défaillance connue spécifique ou un acte condamnable présumé. (31)

D'autre part, il est attendu de la direction qu'elle soutienne les salariés dans tous les aspects de la société, ce qui se manifeste par une gouvernance solide de l'Intégrité des Données en détectant et atténuant les risques en amont, en facilitant la communication, en promouvant la formation avec plusieurs outils et niveaux d'apprentissage, et en améliorant les technologies et les systèmes. (41)

Pour un dévouement à la Qualité de façon proactive et que le personnel ait le sentiment d'en être propriétaire, ou du moins d'en être participants et influenceurs, il est préconisé de lier la Qualité à des valeurs fondamentales, de distribuer un code d'éthique et de pourvoir un environnement transparent et ouvert pour signaler les

problèmes. (46) Ce code d'éthique ou de conduite devra être défini en priorité et approuvé par tous les employés pour que les collaborateurs se rendent compte de leur importance dans la chaîne de procédures spécifiques.

Pour aller plus loin, des investissements dans des formations pour initier un véritable changement dans les mentalités et les habitudes peuvent être décidés. Tous les échelons de l'industrie doivent assumer pleinement la propriété et la responsabilité de leurs propres données et de la documentation. (27)

### **III. L'INTÉGRITÉ DES DONNÉES RÉGLEMENTÉE DANS DIVERSES RÉGIONS DU GLOBE**

#### **1. L'Intégrité des Données en Chine**

##### **A. Les ressemblances avec l'Europe et les États-Unis**

Pour exposer brièvement la situation, la Chine, le Japon et l'Inde comptent des populations nombreuses et un marché de consommation développé et sont des zones de fabrication capitales pour les produits pharmaceutiques. (47) En effet, pléthores de firmes du secteur de la Santé dénombrent majoritairement des usines dans les pays évoqués ci-dessus, l'Intégrité des Données est donc à inspecter dans ces ateliers.

Les lobbyistes de l'industrie américains avancent que les producteurs de médicaments à faible coût opérant à l'étranger respectent les mêmes règles strictes que les concepteurs localisés aux États-Unis. Ils affirment de surcroît que les cas de fraudes de préparation ou de pratiques négligentes sont terminés depuis 2013, quand la plus grande société pharmaceutique indienne a plaidé coupable aux États-Unis de sept crimes en lien avec la falsification de données de fabrication. (48)

Nonobstant, des transgressions perdurent d'après le Sous-Comité de la Santé du Comité de l'Énergie et du Commerce de la Chambre des Représentants, ce qui a amené la NMPA chinoise (c'est-à-dire la National Medical Products Administration, l'Administration Nationale des Produits Médicaux) à publier trois nouveaux documents portant sur l'Intégrité des Données. Le premier, paru en mai 2015, est une annexe GMP du Système Informatisé et détaille les exigences relatives à la construction, à la validation, à la maintenance et à l'utilisation des Systèmes Informatisés pour les fabricants d'articles pharmaceutiques.

Le deuxième texte sorti en 2017 s'intitule « Les Bonnes Pratiques de Laboratoire Non Cliniques » et adjoint des sections de validation des Systèmes Informatisés et de données électroniques lors de la révision. Pour finir, « La Gestion des Dossiers et des Données sur les Médicaments (essai) » datant de décembre 2020 résumant

d'autres restrictions pour la création, l'utilisation et la maintenance des données électroniques et des Systèmes Informatisés.

Ces trois écrits adoptent une approche GAMP 5 pour statuer sur les réglementations et encadrer le cycle de vie des Systèmes Informatisés.

Subséquemment, des procédures de changement appropriées doivent décrire et traiter toute modification dans le cycle de vie d'un système, l'état de performance de celui-ci est censé être observé et les moyens de consulter les incidents du système et de résoudre les problèmes devraient être précisés. Par ailleurs, il est obligatoire que toutes les données des Systèmes Informatisés puissent être consultées et tracées au cours de la période de rétention déterminée. (47)

## **B. Les différences avec l'Europe et les États-Unis**

Malgré la mise en place de ces directives, certaines nuances et points non élucidés subsistent. Par exemple, dans le Projet de Norme sur la Gestion des Données des Médicaments de l'ancienne NMPA, à ce moment-ci appelée la CFDA (pour la Chinese Food and Drug Administration, autrement dit l'Administration Chinoise des Aliments et des Médicaments), l'acronyme ALCOA existe mais avec des termes distincts. Effectivement, il est seulement composé des quatre mots « Vérité, Exactitude, Rapidité et Traçabilité » et plus « Attribuable, Lisible, Contemporain, Original et Exact (Accurate) », comme il est possible de le comparer dans la Figure 11.



*Figure 11 : Les principes ALCOA en Chine*

Ensuite, l'article 12 parle de « techniques avancées encouragées pour contrôler les risques liés à l'Intégrité des Données » mais il n'explique pas quelles sont ces « techniques avancées ». De manière plus générale, les définitions de certaines notions semblent être légèrement différentes de celles d'autres lignes directrices d'organismes de régulation. Il est entre autre possible de prendre pour témoin les désignations de « dépôt » en comparaison avec « archivage » ou encore de « cadre supérieur » assimilé à « haute direction ».

Un dernier cas de figure est l'absence de mention et d'éclaircissement à propos du concept « d'enregistrement primaire » contrairement aux autres ouvrages. Cela est donc source de confusion et de mauvaise interprétation. (49)

En fin de compte, même si beaucoup de chapitres sont identiques, le constat le plus sujet à une divergence est le fait que la Chine ne diffuse toujours pas tous ses rapports d'inspections ou ses mesures de conformité.

Ceci constitue un problème important car les dossiers de la FDA montrent que les violations de l'Intégrité des Données sont persistantes et continues dans les

établissements de synthèse de produits pharmaceutiques à l'étranger. Plus alarmant, ces transgressions ont lieu à un rythme plus fréquent que sur les sols européens et américains.

En effet, les altérations et manipulations de données sont deux fois plus importantes en Chine ou en Inde puisque sur 12 000 examens de la FDA aux États-Unis, environ 15% ont révélé des infractions des principes de l'Intégrité des Données tandis que ces pourcentages oscillent au-dessus de 32% en Chine et s'élèvent à 25% en Inde.

De plus, la nature des actes délictueux est également dissemblable car ceux-ci sont plus significatifs et moins discrets en Chine et en Inde qu'en Europe et aux États-Unis. De récentes affaires de partages d'informations de connexion entre quelques analystes (traduisant des Systèmes Informatiques non protégés) relèvent ainsi de la négligence alors que des suppressions coutumières de résultats de tests irréguliers ou des éliminations de données brutes suggèrent plutôt une fraude. (48)

Cela n'a aucune mesure avec les fautes occidentales surtout reliées à la documentation (et donc estimées comme moins « graves »).

### C. Exemples d'infractions

Afin d'approfondir sur la différence entre les pratiques négligentes et flagrantes entre la Chine et les États-Unis et la multitude de types de manquements, des statistiques ont été réalisées sur les rapports d'intervention ayant réussi à être récupérés. De ce fait, approximativement 28% des entreprises américaines épinglées pour des soucis d'Intégrité des Données affichaient un comportement réellement trompeur au travers de falsifications, destructions et anti-datations. Par opposition, ce nombre stagne autour de 65% pour la Chine et 55% pour l'Inde. (48)

En réalité, cela se concrétise par une première référence de lettre d'avertissement de la FDA d'avril 2017 à l'intention d'un sous-traitant chinois mettant en évidence deux classes d'anomalies : la déficience de capacité à empêcher l'accès non autorisé ou les modifications apportées aux données et l'échec de conservation des données

complètes provenant de tous les tests effectués pour assurer la conformité aux spécifications et aux normes établies.

Le premier défaut a été décelé à la suite du remaniement des réglages de la date et de l'heure par des techniciens de laboratoire, la répétition des analyses pour des raisons non justifiées après avoir reculé le temps et l'écrasement ou l'effacement des résultats de l'échantillon initial, les rendant indisponibles pour l'examen des enquêteurs. Le contrôle des connexions inadéquat était quant à lui dû aux comptes partagés pour accéder aux systèmes et à la fonctionnalité commune d'Audit Trail alors même que celle-ci était désactivée.

La seconde omission était caractérisée par la suppression de chromatogrammes d'HPLC (soit High Performance Liquid Chromatography, ou Chromatographie en Phase Liquide à Haute Performance), le retest de produits jusqu'à ce que des conclusions acceptables soient obtenues et, par conséquent, la libération de lots appuyée sur des secondes analyses sans argumentaire documenté ni enquête. (50)

Une autre lettre d'avertissement de la FDA a été envoyée en juin 2018 à une antenne chinoise d'un groupe pharmaceutique américain, consécutivement à une visite du 11 au 14 décembre 2017. L'agence a déclaré que la société n'avait pas passé en revue ni approuvé des documents affiliés à la Qualité et que des dossiers de fabrication de lots vierges et des timbres d'émission de registres ont été aperçus dans le bureau de l'atelier. Ces derniers n'étaient pas régulés bien que la procédure opérationnelle standard stipule que seul le service Qualité est habilité à la relecture des fichiers pour attester que les renseignements saisis sur les formulaires sont corrects et fiables avant leur publication, au risque de menacer l'Intégrité des Données.

Cette industrie n'a pas non plus maintenu ses données brutes de tests de laboratoires, ce qui devra aboutir à un remplacement d'appareils et de logiciels et à la mise en œuvre de procédures et systèmes appropriés pour certifier que les informations sont préservées. (51)

L'exemple final concernant la Chine est un courrier de sanction du 2 août 2019 (de la part des autorités américaines venues superviser une de leurs branches) annonçant d'importantes violations de l'Intégrité des Données en la présence de documents de Qualité falsifiés tels que des rapports de validation de nettoyage, des dossiers de lots et des examens annuels de produits. Il a aussi été noté que le personnel n'avait pas été en mesure de fournir des dossiers à l'appui des exigences GMP actuelles pour la qualification des instruments, la stabilité des médicaments, la validation des procédés, etc. (52)

## **2. L'Intégrité des Données au Japon**

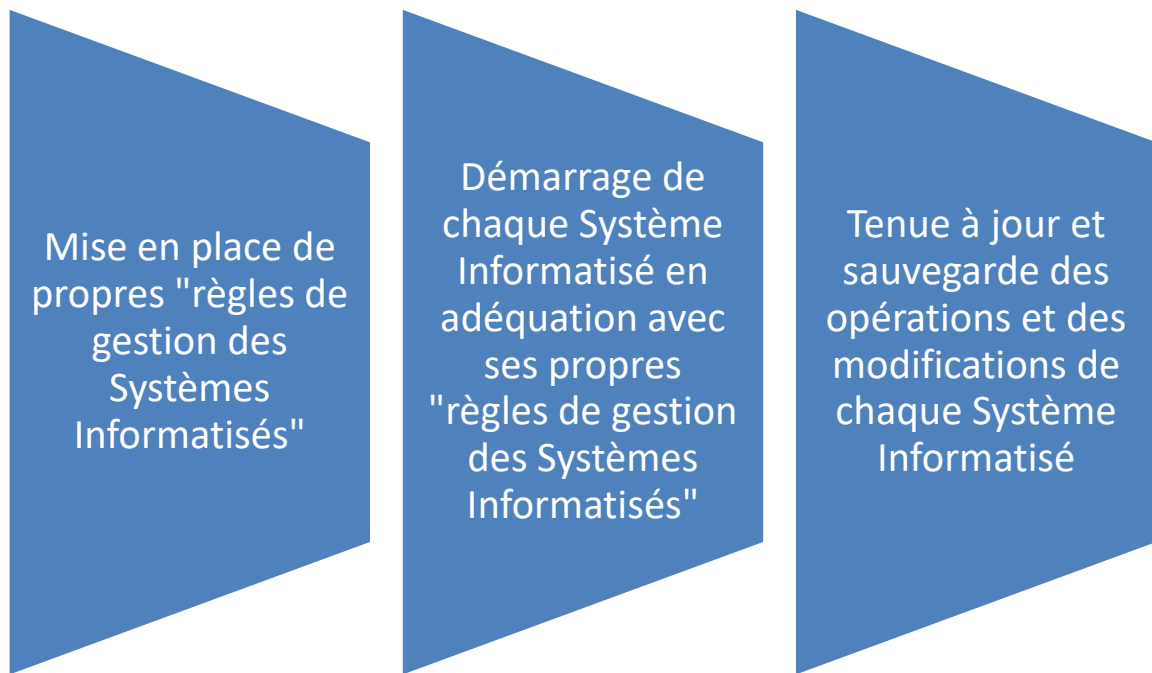
### **A. Les similitudes avec l'Europe et les États-Unis**

Au commencement des années 1990, le Ministère de la Santé, du Travail et des Affaires Sociales avait écrit les « Lignes Directrices pour la Bonne Gestion des Usines de Fabrication de Produits Pharmaceutiques Utilisés par Ordinateur » mais celle-ci fut abolie en 2005.

Dans cette lignée, les « Directives pour la Bonne Gestion des Systèmes Informatisés chez les Fabricants de Produits Pharmaceutiques et Quasi-Pharmaceutiques » ont été dévoilées en 2010 et sont appliquées depuis le 1<sup>er</sup> avril 2012. Il s'agit d'une version révisée des guidelines de 1992 pour s'accorder et être conforme aux normes mondiales comme GAMP 5 et la 21 CFR Partie 11.

Ce nouvel ouvrage comporte trois exigences principales résumées dans la Figure 12 : la mise en place de propres « règles de gestion des Systèmes Informatisés », le démarrage de chaque Système Informatisé en adéquation avec ses propres « règles de gestion de Système Informatisé » et la tenue à jour et la sauvegarde des opérations et des modifications de chaque Système Informatisé. (47)





*Figure 12 : Les trois exigences de la réglementation japonaise*

Un texte complémentaire, en l'occurrence la Demande d'Homologation des Médicaments (Directive DESE), a été développé. Cet ajout, abordant la génération et le stockage des documents électroniques, correspond étroitement aux buts de la 21 CFR Partie 11 et veut dire que les firmes qui adhèrent à cette loi seront en conformité avec la directive DESE. Toutefois, des précautions devront être de mise par les équipes japonaises pour totalement respecter la 21 CFR Partie 11 afin de pouvoir vendre des médicaments aux États-Unis. (53)

De son côté, la PMDA (pour Pharmaceuticals and Medical Devices Agency, retranscrit en Agence des Médicaments et des Dispositifs Médicaux) indique que le Japon est compris dans la Déclaration Conjointe sur la Transparence et l'Intégrité des Données de l'IMCRA (équivalent à l'International Coalition of Medicines Regulatory Authorities, ou la Coalition Internationale des Autorités de Réglementation des Médicaments) et du WHO. Cet édit précise que les données doivent être robustes, exhaustives et vérifiables et que des systèmes d'accès doivent être créés même si la normalisation de celles-ci n'est pas une sommation. (54)

Enfin, la JPMA (c'est-à-dire la Japan Pharmaceutical Manufacturers Association pour Association Japonaise de l'Industrie Pharmaceutique) a contribué à instaurer un plan directeur (un DIMM), une fiche d'évaluation de la conformité de l'Intégrité des Données, des outils d'évaluation pour les équipements et les systèmes et des matériels d'éducation et de formation dans les activités réelles. (55)

## **B. Les distinctions avec l'Europe et les États-Unis**

Tout d'abord, les objectifs de spécifications ont beau être analogues, plusieurs décrets demeurent contradictoires ou entrent en vigueur plus tardivement dans certains pays que d'autres. En témoigne le retour d'un établissement japonais après la réception d'une lettre d'avertissement de la FDA en janvier 2017 qui stipulait que, jusqu'au 1<sup>er</sup> juin 2016, la récurrence des tests sans prétexte ni documentation était autorisée sans contrainte de conservation des données. (56)

Puis, nous avons constaté que le Japon se basait sur les « Directives pour la Bonne Gestion des Systèmes Informatisés chez les Fabricants de Produits Pharmaceutiques et Quasi-Pharmaceutiques », elles-mêmes tirées du GAMP5. Cependant, quelques points de ce standard sont un peu plus détaillés que ceux de l'annexe 11 de la directive de l'EU (European Union, soit Union Européenne) sur les GMP. Ces items portent sur les thématiques suivantes (57) :

- Les principes généraux
- Le champ d'application
- La documentation sur le développement, la validation et la gestion des opérations des Systèmes Informatisés
- Les opérations de développement
- Les activités de validation
- Les activités relatives à la gestion des opérations
- La vérification interne
- Le retrait des Systèmes Informatiques
- La gestion des documents et des dossiers

- La terminologie

De surcroît, il est à remarquer que les lettres d'avertissement sur les médicaments ont généralement pour source les chapitres concernés de la section 21 du CFR Partie 11, alors que les lettres d'avertissement sur les principes actifs font ordinairement référence à la ligne directrice Q7 de l'ICH. (58)

### C. Exemples d'écarts

Dans le prolongement des paragraphes précédents, nous pouvons observer que les causes des scandales en lien avec l'Intégrité des Données au Japon par rapport à l'Europe et aux États-Unis sont par ailleurs divergents. En effet, les motifs de lettres d'avertissement traitent particulièrement de problèmes découlant des séismes et des fuites de gaz. (59)

Un premier exemplaire de lettre d'avertissement peut être celui d'août 2018 consécutif à une enquête du 4 au 8 septembre 2017. Les failles résidaient dans l'Intégrité des Données et la manipulation des données à cause de la répétition de nouvelles analyses et le remaniement de données après la collecte de résultats hors tendances.

Les salariés audités avaient eux-mêmes annoncé un manque de conscience de la gravité des déviations GMP dans leur entreprise et un environnement où les données de tests étaient susceptibles d'être facilement détournées. *De facto*, la société a été chargée de procurer une évaluation du Système Qualité et de réaliser un examen rétrospectif de tous les lots distribués.

De plus, un manque de contrôle de l'Intégrité des Données a également été cité par les inspecteurs de la FDA car les essais sur les systèmes HPLC étaient inadaptés et des feuilles de calcul non protégées étaient employées pour exécuter des calculs et des évaluations statistiques des données de production. Ces tables étaient ainsi

sensibles aux modifications non autorisées et ne disposaient pas d'historique des changements.

Les équipes se sont donc engagées à délivrer des comptes-rendus de contrôles et de procédures et à décider d'actions correctives détaillées et de plans d'actions préventifs. (60)

Pour dresser un bilan des transgressions liées à l'Intégrité des Données au Japon parallèlement aux États-Unis, ces dernières sont en diminution en Occident depuis 2015 mais restent au-dessus de 40%. Cependant, les déficiences dans les documents d'expertise et les enregistrements ont rapidement augmenté au Japon, notamment entre 2016 et 2017 en passant de 25 à 41. (59)

### **3. L'Intégrité des Données dans d'autres contrées**

#### **A. L'Intégrité des Données en Inde**

Pour commencer, dans ce pays, le CDSCO (l'acronyme de la Central Drugs Standard Control Organization, représentant l'Organisation Centrale de Contrôle des Normes Pharmaceutiques) du Ministère de la Santé et du Bien-être familial est en cours de révision et de mise à niveau de l'annexe M depuis quelques années. Cette annexe M (Bonnes Pratiques de Fabrication et Exigences des Locaux, des Usines et des Équipements pour les Produits Pharmaceutiques) fait partie de la loi de 1940 sur les médicaments et les cosmétiques et a ensuite été modifiée de façon importante en 2001.

Elle fait donc office de GMP mais, de nos jours, la majorité des petits et moyens préparateurs de médicaments en Inde se plient à l'annexe M tandis que seulement 20% des sites répondent aux réglementations GMP de l'Organisation Mondiale de la Santé, ce qui mène à deux modèles de Qualité. (47) En sus, 33% des répondants à un sondage indien ont admis ne pas avoir lancé d'audit, de revue ou de vérification dans l'optique de jauger les lacunes potentielles dans le maintien de l'Intégrité des Données. (61)

Subséquemment, les infractions de l'Intégrité des Données les plus couramment rencontrées par les spécialistes de la FDA à l'occasion d'audits sont le manque de sauvegarde et de restauration des données, le partage des identifiants de connexion, l'inactivation des Audit Trails et les droits d'accès des utilisateurs non restreints, ce qui favorise les modifications et les suppressions de résultats de tests et de données.

(62)

Cela transparaît dans deux lettres d'avertissement datant de 2019. Par exemple, celle de janvier à Goa a révélé qu'une enseigne de fabrication pharmaceutique avait altéré les données de ses dossiers de production de lots pour permettre la mise sur le marché de son médicament contre le diabète.

Or, les données brutes des analyses ont prouvé que le médicament ne correspondait pas aux critères de Qualité. Certaines de ces violations peuvent aller jusqu'à la déchirure de dossiers de tests, l'invention de données de stérilité obligatoires en l'absence de réalisation d'analyses microbiennes des surfaces, de l'air et de l'eau.

(48)

Le second courrier de notification a été envoyé le 4 mai de cette même année à la suite d'une visite du 22 au 26 octobre 2018 au Gujarat. La raison était un manque de contrôle sur les Systèmes Informatiques et un non respect des procédures de nettoyage et d'entretien des équipements.

Dans les faits, des documents lacérés contenant des données de feuilles de tests et de formulaires de rejet ont été retrouvés dans des poubelles et des anti-datations de fichiers vierges d'études de stabilité ont été constatées.

D'autre part, les opérateurs ont été en position d'apporter des changements à la libération des lots et aux équipements d'analyses sans autorisation au travers de partages de noms d'utilisateurs et de mots de passe entre les techniciens du Contrôle de la Qualité, les dirigeants de la zone de production et les fournisseurs de services logiciels.

En outre, l'établissement avait recours à des équipements polyvalents n'ayant pas été convenablement nettoyés et à des procédures de nettoyage et une stratégie de validation du nettoyage non évaluées. (63)

## B. L'Intégrité des Données en Russie

En préambule, les institutions de Santé en Russie reposent sur l'agence du FSID & GP (qui est le Federal State Institute of Drugs and Good Practices, l'Institut Fédéral des Médicaments et des Bonnes Pratiques), fondé en 1973. Cette division dérive du Pharmaceutical and Medical Development Department (le Département du Développement Pharmaceutique et Médical) du Minpromtorg, autrement dit le Ministry of Industry and Trade of Russian Federation (le Ministère de l'Industrie et du Commerce de la Fédération de Russie).

Avec le support d'un cabinet de conseils en technologie, en qualité et en conformité, ces organismes d'encadrement ont rédigé des guidelines intitulées « Data Integrity & Computer System Validation » (Intégrité des Données et Validation des Systèmes Informatiques), récemment actualisées en 2022. Cette publication mentionne des thèmes familiers comme l'ALCOA +, la Data Governance, le cycle de vie des données... (64) Elle sera *in fine* un guide pour l'Intégrité des Données industrielles en énonçant des spécifications faisant écho aux Good Manufacturing Practices.

Il est à noter que ce nouveau partenariat entre le bureau d'experts et l'État reflète l'évolution des conditions du marché, une tendance croissante à l'internationalisation dans le secteur pharmaceutique et une envie d'adaptation vis-à-vis de ces transformations. Entre autres, les propriétaires de certificats d'enregistrement ont désormais l'obligation d'introduire dans leur quotidien un ensemble de Systèmes Informatiques pour l'enregistrement, l'authentification, la conservation et l'échange de rapports de données fiables sur les produits avant leur mise sur le marché.

Pour finir, le Federal State Institute of Drugs and Good Practices a été choisi comme autorité publique confirmée pour effectuer des audits et aussi des inspections des firmes pharmaceutiques sur le respect des GMP. (65)

### C. L'Intégrité des Données au Canada

Avant toute chose, malgré le fait que le Canada soit sur le continent Nord-Américain comme son voisin, les textes de cette région placent la responsabilité de la conformité sur l'individu alors que la codification de la 21 CFR Partie 11 des États-Unis propose une série de consignes sans identifier exactement les membres responsables. (53)

Les préceptes canadiens sont relatés dans le Food and Drugs Act (traduit par la Loi sur les Aliments et Drogues et dont le nom intégral est la Loi concernant les Aliments, Drogues, Cosmétiques et Instruments Thérapeutiques), initialement adopté en 1920 puis révisé et entré en vigueur en 1985. La partie « Food and Drug Regulations » renferme sept sections de A à J (Administration, Aliments, Vitamines, Édulcorants, etc.), elles-mêmes scindées en multiples divisions.

Celle qui nous intéresse est la Part C « Drugs », et en particulier la Division 2 « Good Manufacturing Practices ». Les différents paragraphes abordent bien les questions des données affiliées aux équipements, au personnel, à la gestion des échantillons et de la stabilité et aux analyses des matières premières, des produits finis et des matériaux de packaging... (66)

Enfin, le fonctionnement du droit canadien applique également le principe des Accords de Reconnaissance Mutuelle avec les nations dont les directives sont « de portée et de profondeur équivalentes » entre elles (en comparaison avec les États-Unis ou l'Union Européenne par exemple), ce qui rend l'importation et l'approbation des matières premières et des produits finis plus rapides entre les pays impliqués. (53)

#### D. L'Intégrité des Données au Mexique

Sur le même modèle que les gouvernements précédents, l'organisation de réglementation sanitaire au Mexique est la COFEPRIS, la Comisión Federal para la Protección contra Riesgos Sanitarios (signifiant la Commission Fédérale pour la Protection contre les Risques Sanitaires).

Le périmètre de cette branche compétente est de ce fait toutes les activités apparentées à la production, la distribution, la commercialisation, l'importation et l'exportation et la publicité et la vente des médicaments, des aliments, des produits du tabac, d'autres articles de santé (dispositifs médicaux, vaccins, sang et tissus, etc.), des cosmétiques et divers biens de consommation, des pesticides...(67)

Tout comme les politiques russes, les pouvoirs latins se sont alliés avec le même groupe de consultants dans l'optique de créer un chapitre sur l'Intégrité des Données dans leurs GMP, dénommées NOM 059. (65)

Effectivement, il existe une norme officielle mexicaine sur les Buenas Prácticas de Fabricación de Medicamentos (Bonnes Pratiques de Fabrication des Médicaments), la NOM-059-SSA1-2015, et dont deux annexes ont été écrites par le PIC/S : le Guía para las Buenas Prácticas de Fabricación de Medicamentos (le Guide des Bonnes Pratiques de Fabrication des Médicaments) et les Notas explicativas para los fabricantes farmacéuticos sobre la preparación del Archivo Maestro en el Sitio (les Notes explicatives à l'intention des fabricants de produits pharmaceutiques sur la préparation de Fichier maître sur site) qui reprennent tous deux les critères européens et américains de l'Intégrité des Données. (68)



## E. Synthèse de l'Intégrité des Données entre les nations

	Réglementation principale	Points communs	Différences
<b>Chine</b>	Annexe GMP du Système Informatisé	<ul style="list-style-type: none"> <li>- Basé sur le GAMP 5</li> <li>- Utilisation du cycle de vie des données</li> <li>- Traçabilité sur une période de rétention</li> <li>- Sauvegarde des modifications</li> <li>- Utilisation d'Audit Trails</li> <li>- Gestion des accès des utilisateurs</li> <li>- Évaluation des équipements</li> </ul>	<ul style="list-style-type: none"> <li>- ALCOA différent</li> <li>- Archivage différent</li> <li>- Pas d'enregistrement primaire</li> </ul>
<b>Japon</b>	Directives pour la Bonne Gestion des Systèmes Informatisés chez les Fabricants de Produits Pharmaceutiques et Quasi-Pharmaceutiques		<ul style="list-style-type: none"> <li>- Pas d'ALCOA</li> <li>- Conservation différente</li> </ul>
<b>Inde</b>	Annexe M (Bonnes Pratiques de Fabrication et Exigences des Locaux, des Usines et des Équipements pour les Produits Pharmaceutiques)		<ul style="list-style-type: none"> <li>- Pas appliquée dans tout le pays</li> </ul>
<b>Russie</b>	Intégrité des Données et Validation des Systèmes Informatiques		<ul style="list-style-type: none"> <li>- Pas encore déployée donc pas d'ALCOA, de Data Governance...</li> </ul>
<b>Canada</b>	Loi concernant les Aliments, Drogues, Cosmétiques et Instruments Thérapeutiques		<ul style="list-style-type: none"> <li>- Responsabilité sur l'individu</li> </ul>
<b>Mexique</b>	Bonnes Pratiques de Fabrication des Médicaments		<ul style="list-style-type: none"> <li>- Pas encore finalisées</li> </ul>

Figure 13 : Tableau comparatif de l'Intégrité des Données parmi les pays abordés

## CONCLUSION

Tout au long de ces pages, nous avons donc défini que de nombreux codes et lignes directrices centrés sur l'Intégrité des Données ont été entérinés par des administrations variées telles que la FDA, l'ISPE ou encore le WHO, car cette Intégrité des Données englobe pléthore d'applications. Pour ce faire, l'acronyme ALCOA + est à prendre en compte du début à la fin du cycle de vie des données et dans chaque aspect du management des risques.

Qui plus est, les trois niveaux d'accomplissement de l'Intégrité des Données ont été démontrés comme étant atteignables dans différentes sortes d'exploitations, que ces dernières soient pourvues d'anciennes machines et systèmes ou équipées d'appareils et programmes actuels ou bien possédant une technologie de pointe 4.0. Les commandements de l'Intégrité des Données peuvent de surcroît être déployés dans les domaines de l'informatique, des équipements eux-mêmes et du management.

Dans un autre registre, nous nous sommes ensuite concentrés sur les interprétations et le suivi de l'Intégrité des Données dans le monde, et notamment dans quelques pays d'Asie et d'Amérique du Nord. En effet, chacun de ces états a entamé une démarche de mise en œuvre de l'Intégrité des Données, le plus souvent en travaillant conjointement avec une institution publique ou une chaîne de conseils privée. Ainsi, il faudra désormais surtout veiller à une homogénéité de l'Intégrité des Données entre les multiples régions.

Nous pouvons conclure en supputant que, du fait de l'importance du sujet et du développement de l'informatique, les législations sur l'Intégrité des Données seront amenées à être durcies dans le futur.

## BIBLIOGRAPHIE

1. Rogers CA, Ahearn JD, Bartlett MG. Data Integrity in the Pharmaceutical Industry: Analysis of Inspections and Warning Letters Issued by the Bioresearch Monitoring Program Between Fiscal Years 2007–2018. *Ther Innov Regul Sci*. 1 sept 2020 [cité 3 août 2023];54(5):1123-33. Disponible sur: <https://doi.org/10.1007/s43441-020-00129-z>
2. Intégrité des données : risques et bonnes pratiques. Comment la garantir ? [Internet]. Blueway. 2020 [cité 25 juill 2022]. Disponible sur: <https://www.blueway.fr/blog/integrite-donnees>
3. PELLETIER L. A3P - Industrie Pharmaceutique & Biotechnologie. 2018 [cité 25 juill 2022]. Data Integrity : vers la mise en place d'un Data Management. Disponible sur: <https://www.a3p.org/data-integrity-vers-la-mise-en-place-dun-data-management/>
4. Smalley CJ. Why is There a Problem with Data Integrity? *PDA J Pharm Sci Technol*. 1 mai 2017 [cité 31 juill 2023];71(3):170-1. Disponible sur: <https://doi.org/10.5731/pdajpst.2017.001101>
5. GOV.UK [Internet]. 2015 [cité 31 juill 2023]. Good Manufacturing Practice (GMP) data integrity: a new look at an old topic, part 3 - MHRA Inspectorate. Disponible sur: <https://mhrainspectorate.blog.gov.uk/2015/08/27/good-manufacturing-practice-gmp-data-integrity-a-new-look-at-an-old-topic-part-3/>
6. WYN S. New GAMP Data Integrity Good Practice Guidance and Experience from the Field - PPT - 31 May 2019 (FINAL).pdf [Internet]. 2019 mai 29 [cité 25 juill 2022]. Disponible sur: [https://ispe.org/sites/default/files/Webinar/New%20GAMP%20Data%20Integrity%20Good%20Practice%20Guidance%20and%20Experience%20from%20the%20Field%20-%20PPT%20-%2031%20May%202019%20\(FINAL\).pdf](https://ispe.org/sites/default/files/Webinar/New%20GAMP%20Data%20Integrity%20Good%20Practice%20Guidance%20and%20Experience%20from%20the%20Field%20-%20PPT%20-%2031%20May%202019%20(FINAL).pdf)
7. McLaughlin E. Guidance for Industry. *Quest Answ* [Internet]. 2018 [cité 25 août 2022];17. Disponible sur: <https://www.fda.gov/media/119267/download>
8. Talend - A Leader in Data Integration & Data Integrity [Internet]. [cité 26 juill 2022]. Intégrité des données : comment la garantir ? Talend. Disponible sur: <https://www.talend.com/fr/resources/what-is-data-integrity/>
9. MasterControl [Internet]. [cité 26 juill 2022]. Recommandation de la FDA : FDA questions et réponses sur la Data Integrity. Disponible sur: <https://www.mastercontrol.com/fr/gxp-lifeline/fda-questions-et-reponses-sur-la-data-integrity>

10. GOV.UK [Internet]. 2015 [cité 1 août 2023]. Good Manufacturing Practice (GMP) data integrity: a new look at an old topic, part 2 - MHRA Inspectorate. Disponible sur: <https://mhrainspectorate.blog.gov.uk/2015/07/14/good-manufacturing-practice-gmp-data-integrity-a-new-look-at-an-old-topic-part-2/>
11. CHOUDHARY A. pharmaceutical guidelines. 2021 [cité 30 juill 2022]. ALCOA to ALCOA Plus for Data Integrity: Pharmaguideline. Disponible sur: <https://www.pharmaguideline.com/2018/12/alcoa-to-alcoa-plus-for-data-integrity.html>
12. Beckman Coulter Life Sciences [Internet]. [cité 30 juill 2022]. FDA ALCOA Data Integrity Guidance. Disponible sur: <https://www.mybeckman.uk/resources/industry-standards/alcoa>
13. PIC/S Secretariat. GOOD PRACTICES FOR DATA MANAGEMENT AND INTEGRITY IN REGULATED GMP/GDP ENVIRONMENTS [Internet]. 2021 [cité 12 août 2022]. Disponible sur: <https://picscheme.org/docview/4234>
14. Rattan AK. Data Integrity: History, Issues, and Remediation of Issues. PDA J Pharm Sci Technol. 1 mars 2018 [cité 14 août 2022];72(2):105-16. Disponible sur: <https://doi.org/10.5731/pdajpst.2017.007765>
15. World Health Organization. Annex 4 - Guideline on data integrity [Internet]. oct 10, 2021. Disponible sur: [https://cdn.who.int/media/docs/default-source/medicines/norms-and-standards/guidelines/inspections/trs1033-annex4-guideline-on-data-integrity.pdf?sfvrsn=6218a4e6\\_4&download=true](https://cdn.who.int/media/docs/default-source/medicines/norms-and-standards/guidelines/inspections/trs1033-annex4-guideline-on-data-integrity.pdf?sfvrsn=6218a4e6_4&download=true)
16. A3P - Industrie Pharmaceutique & Biotechnologie [Internet]. 2018 [cité 18 août 2022]. Le lien entre réglementation, système qualité & Data Integrity. Disponible sur: <https://www.a3p.org/le-lien-entre-reglementation-systeme-qualite-data-integrity/>
17. Barkow S, Takahashi K. Current expectations and guidance, including data integrity and compliance with CGMP. 30 mars 2017 [cité 25 août 2022];58. Disponible sur: [https://elsmar.com/Cove\\_Members/CDER-OMQ\\_CGMP\\_Guidance\\_Plenary\\_3-20-2017\\_S508.pdf](https://elsmar.com/Cove_Members/CDER-OMQ_CGMP_Guidance_Plenary_3-20-2017_S508.pdf)
18. Rodriguez-Perez P. vdocument.in. [cité 25 août 2022]. Current Expectations and Guidance Data Integrity & PDF file Data Integrity: Not a New Concept API-ICH Q7 Rev 1 Computerized Systems (5.4) GMP-related computerized systems should be - [PDF Document]. Disponible sur: <https://vdocument.in/current-expectations-and-guidance-data-integrity-data-integrity-not-a-new-concept.html>
19. What is Data Integrity? [Internet]. 2019 [cité 28 août 2022]. Disponible sur: <https://afteracademy.com/blog/what-is-data-integrity>
20. McDowall R. Data Integrity Focus, Part 1: Understanding the Scope of Data Integrity. LCGC N Am [Internet]. 1 janv 2019 [cité 28 août 2022];37(1):44-51.

Disponible sur: <https://www.chromatographyonline.com/view/data-integrity-focus-part-1-understanding-scope-data-integrity>

21. GOV.UK [Internet]. 2015 [cité 1 août 2023]. Good Manufacturing Practice (GMP) data integrity: a new look at an old topic, part 1 - MHRA Inspectorate. Disponible sur: <https://mhrainspectorate.blog.gov.uk/2015/06/25/good-manufacturing-practice-gmp-data-integrity-a-new-look-at-an-old-topic-part-1/>

22. What is Data Integrity In Pharmaceutical Industry...??? [Internet]. Pharmaguideline. 2018 [cité 27 sept 2022]. Disponible sur: <https://www.pharmaguideline.net/what-is-data-integrity-in-pharmaceutical-industry/>

23. Medicines & Healthcare products Regulatory Agency (MHRA). 'GXP' Data Integrity Guidance and Definitions [Internet]. 2018 [cité 1 août 2023]. Disponible sur: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/687246/MHRA\\_GxP\\_data\\_integrity\\_guide\\_March\\_edited\\_Final.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/687246/MHRA_GxP_data_integrity_guide_March_edited_Final.pdf)

24. CHOUDHARY A. FDA New Data Integrity Guidelines: Highlights : Pharmaguideline [Internet]. [cité 12 nov 2022]. Disponible sur: <https://www.pharmaguideline.com/2019/01/fda-new-data-integrity-guidelines.html>

25. Steinwandter V, Herwig C. Provable Data Integrity in the Pharmaceutical Industry Based on Version Control Systems and the Blockchain. PDA J Pharm Sci Technol. 1 juill 2019 [cité 1 août 2023];73(4):373-90. Disponible sur: <https://doi.org/10.5731/pdajpst.2018.009407>

26. GOV.UK [Internet]. 2017 [cité 2 août 2023]. Too much pressure: a behavioural approach to Data Integrity (Part 1) - MHRA Inspectorate. Disponible sur: <https://mhrainspectorate.blog.gov.uk/2017/03/10/too-much-pressure-a-behavioural-approach-to-data-integrity-part-1/>

27. Seratec [Internet]. 2020 [cité 8 janv 2023]. La montée en puissance de la Data Integrity. Disponible sur: <http://www.serateclab.com/?q=montee-en-puissance-data-integrity>

28. JANSEN C. News-Medical.net. 2019 [cité 15 janv 2023]. Data Integrity in the Pharmaceutical Industry. Disponible sur: <https://www.news-medical.net/news/20190729/Data-Integrity-in-the-Pharmaceutical-Industry.aspx>

29. McDowall R. Informatics from Technology Networks. 2021 [cité 15 janv 2023]. The Latest Regulatory Guidance for Data Integrity and Regulatory Compliance. Disponible sur: <http://www.technologynetworks.com/informatics/articles/the-latest-regulatory-guidance-for-data-integrity-and-regulatory-compliance-353714>

30. WAKEHAM C. ISPE | International Society for Pharmaceutical Engineering. 2019 [cité 15 janv 2023]. Data Integrity for Manufacturing Records. Disponible sur:

<https://ispe.org/pharmaceutical-engineering/ispeak/data-integrity-manufacturing-records>

31. Markarian J. Data Integrity Challenges in Manufacturing. Pharm Technol [Internet]. 2 juill 2016 [cité 15 janv 2023];40(7):50-4. Disponible sur: <https://www.pharmtech.com/view/data-integrity-challenges-manufacturing>
32. Alosert H, Savery J, Rheaume J, Cheeks M, Turner R, Spencer C, et al. Data integrity within the biopharmaceutical sector in the era of Industry 4.0. Biotechnol J. 1 juin 2022 [cité 4 août 2023];17(6):2100609. Disponible sur: <https://doi.org/10.1002/biot.202100609>
33. Newmarker C. Pharmaceutical Processing World. 2020 [cité 15 janv 2023]. Why equipment calibration is important for maintaining data integrity. Disponible sur: <https://www.pharmaceuticalprocessingworld.com/why-equipment-calibration-is-important-for-maintaining-data-integrity/>
34. Torres SR. The Connected Lab. 2021 [cité 16 janv 2023]. Pharma 4.0: How Networked Digital Technologies and Advanced Automation are Reshaping the Pharmaceutical Value Chain. Disponible sur: <https://www.thermofisher.com/blog/connectedlab/pharma-4-0-how-networked-digital-technologies-and-advanced-automation-are-reshaping-the-pharmaceutical-value-chain/>
35. CHAROO N, KHAN M, RAHMAN Z. Data integrity issues in pharmaceutical industry: Common observations, challenges and mitigations strategies. Int J Pharm. 25 janv 2023 [cité 3 août 2023];631:122503. Disponible sur: <https://doi.org/10.1016/j.ijpharm.2022.122503>
36. MANZANO T, LANGER G. ISPE | International Society for Pharmaceutical Engineering. 2018 [cité 20 janv 2023]. Getting Ready for Pharma 4.0<sup>TM</sup>. Disponible sur: <https://ispe.org/pharmaceutical-engineering/september-october-2018/getting-ready-pharma-40tm>
37. Steinwandter V, Borchert D, Herwig C. Data science tools and applications on the way to Pharma 4.0. Drug Discov Today. 1 sept 2019 [cité 1 août 2023];24(9):1795-805. Disponible sur: <https://doi.org/10.1016/j.drudis.2019.06.005>
38. ZIPFELL P. PharmTech. 2021 [cité 22 janv 2023]. Strengthening Data Integrity and Traceability. Disponible sur: <https://www.pharmtech.com/view/strengthening-data-integrity-and-traceability>
39. Gardner N. The Connected Lab. 2021 [cité 22 janv 2023]. Data Integrity and Pharma 4.0. Disponible sur: <https://www.thermofisher.com/blog/connectedlab/data-integrity-and-pharma-4-0/>

40. Beckman Coulter Life Sciences [Internet]. [cité 22 janv 2023]. EU GMP Annex 11. Disponible sur: <https://www.mybeckman.uk/resources/industry-standards/eu-gmp-annex-11>
41. LINCIANO A, BUENDIA A. ISPE | International Society for Pharmaceutical Engineering. 2019 [cité 22 janv 2023]. Data Integrity: A Vertical Journey. Disponible sur: <https://ispe.org/pharmaceutical-engineering/january-february-2019/data-integrity-vertical-journey>
42. Girard S, Watkin A. Meeting Data Integrity ALCOA+ Principles Using Digital Data Management Solutions. Life On [Internet]. 1 nov 2020 [cité 23 janv 2023]; Disponible sur: <https://www.eurotherm.com/?wpdmdl=103697>
43. ProPharma [Internet]. 2020 [cité 29 janv 2023]. How Data Integrity Supports a Smooth Transition to Pharma 4.0. Disponible sur: <https://www.propharmagroup.com/thought-leadership/how-data-integrity-supports-a-smooth-transition-to-pharma-4-0>
44. ABS Group [Internet]. [cité 29 janv 2023]. Industry 4.0: Improving Mechanical Integrity and Reliability with Data Analytics. Disponible sur: <https://www.abs-group.com/Knowledge-Center/Insights/Industry-40-Improving-Mechanical-Integrity-and-Reliability-with-Data-Analytics/>
45. JOUVE JL, FRANCKX G, DUFRASNE JS. A3P - Industrie Pharmaceutique & Biotechnologie. 2018 [cité 29 janv 2023]. Migration dans le Cloud computing & Data Integrity. Disponible sur: <https://www.a3p.org/migration-dans-le-cloud-data-integrity/>
46. HOLM PEDERSEN C. NNE. [cité 12 févr 2023]. How data integrity brings you closer to digital transformation. Disponible sur: <https://www.nne.com/techtalk/how-data-integrity-brings-you-closer-to-digital-transformation/>
47. A comparison between CSV Guideline / regulations in Japan, India and China [Internet]. [cité 21 mars 2023]. Disponible sur: <https://blog.pqegroup.com/csv-data-integrity/csv-guideline-regulations-japan-india-china>
48. EBAN K, SALZMAN S. In generic drug plants in China and India, data falsification is still a problem [Internet]. STAT. 2019 [cité 23 mars 2023]. Disponible sur: <https://www.statnews.com/2019/10/29/data-falsification-still-problematic-china-india-generic-drug-plants/>
49. UNGER B. Pharmaceutical Online. 2016 [cité 25 mars 2023]. Comparing Recent Data Management/Integrity Guidances: FDA, EMA, & China FDA. Disponible sur: <https://www.pharmaceuticalonline.com/doc/comparing-recent-data-management-integrity-guidances-fda-ema-china-fda-0001>
50. JPMA [Internet]. 2019 [cité 31 mars 2023]. Data Integrity (For Working-Level Personnel). Disponible sur:

[https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.jpma.or.jp%2Fenglish%2Freports%2Fquality\\_technology\\_committee%2Feki4g6000004ae7-att%2Fpractitioner\\_e.pptx&wdOrigin=BROWSELINK](https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.jpma.or.jp%2Fenglish%2Freports%2Fquality_technology_committee%2Feki4g6000004ae7-att%2Fpractitioner_e.pptx&wdOrigin=BROWSELINK)

51. PharmTech [Internet]. 2018 [cité 1 avr 2023]. Data Integrity Issues Found at China Facility. Disponible sur: <https://www.pharmtech.com/view/data-integrity-issues-found-china-facility>

52. PharmTech [Internet]. 2019 [cité 2 avr 2023]. Data Integrity Violations Found at China Facility. Disponible sur: <https://www.pharmtech.com/view/data-integrity-violations-found-china-facility-0>

53. Beckman Coulter Life Sciences [Internet]. [cité 7 avr 2023]. 21 CFR Partie 11, règlements mondiaux connexes. Disponible sur: <https://www.beckman.fr/resources/industry-standards/21-cfr-part-11/global-equivalents-and-related-regulations>

54. Pharmaceuticals and Medical Devices Agency [Internet]. [cité 10 avr 2023]. Joint Statement on transparency and data integrity International Coalition of Medicines Regulatory Authorities (ICMRA) and the World Health Organization (WHO) | Pharmaceuticals and Medical Devices Agency. Disponible sur: <https://www.pmda.go.jp/english/int-activities/int-harmony/icmra/0021.html>

55. Japan Pharmaceutical Manufacturers Association(JPMA) [Internet]. [cité 10 avr 2023]. DI (Data Integrity) related Publications | Quality & Technology Committee. Disponible sur: [https://www.jpma.or.jp/english/reports/quality\\_technology\\_committee/di.html](https://www.jpma.or.jp/english/reports/quality_technology_committee/di.html)

56. BioPharm International [Internet]. 2017 [cité 11 avr 2023]. Data Integrity Problems Found at Japan Facility. Disponible sur: <https://www.biopharminternational.com/view/data-integrity-problems-found-japan-facility>

57. MANGEL A. GMP Compliance. 2012 [cité 12 avr 2023]. Japanese Requirements on Computerised Systems - ECA Academy. Disponible sur: <https://www.gmp-compliance.org/gmp-news/japanese-requirements-on-computerised-systems>

58. GMP Compliance [Internet]. 2018 [cité 12 avr 2023]. Data integrity still in the focus of FDA: new warning letter to Japanese API manufacturer - ECA Academy. Disponible sur: <https://www.gmp-compliance.org/gmp-news/data-integrity-still-in-the-focus-of-fda-new-warning-letter-to-japanese-api-manufacturer>

59. JPMA [Internet]. 2019 [cité 12 avr 2023]. Data Integrity (For Management Personnel). Disponible sur: <https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.jpma.or.jp>



%2Fenglish%2Freports%2Fquality\_technology\_committee%2Feki4g6000004ae7-att%2Fmanagement\_e.pptx&wdOrigin=BROWSELINK

60. PharmTech [Internet]. 2018 [cité 16 avr 2023]. Data Integrity Violations Found at Japanese Facility. Disponible sur: <https://www.pharmtech.com/view/data-integrity-violations-found-japanese-facility>
61. Singh A, Joshi R, Hussain A. Analyzing the state of Data Integrity Compliance in the Indian pharmaceutical industry [Internet]. Fraud Investigation & Dispute Services; 2015 [cité 4 août 2023] p. 20. Disponible sur: <https://rx-360.org/wp-content/uploads/2018/08/ey-data-integrity-compliance-in-the-pharma-industry.pdf>
62. CHOUDHARY A. pharmaceutical guidelines. [cité 22 avr 2023]. FDA's Data Integrity Issues in Indian Facilities: Pharmaguideline. Disponible sur: <https://www.pharmaguideline.com/2015/02/FDA-data-integrity-issues-during-inspection.html>
63. PharmTech [Internet]. 2019 [cité 23 avr 2023]. Data Integrity Violations Found at India Facility. Disponible sur: <https://www.pharmtech.com/view/data-integrity-violations-found-india-facility>
64. FSID & GP. GUIDELINES Data Integrity & Computer System Validation [Internet]. Disponible sur: [https://gilsinp.ru/download/Validatsiya/SIDGP\\_en\\_2019-02.pdf](https://gilsinp.ru/download/Validatsiya/SIDGP_en_2019-02.pdf)
65. STONES M. Russian Institute for Drugs and Good Practices unveils new data guide - European Pharmaceutical Review Russia drugs Institute unveils data guide [Internet]. European Pharmaceutical Review. 2018 [cité 23 avr 2023]. Disponible sur: <https://www.europeanpharmaceuticalreview.com/news/78899/russian-institute-for-drugs-and-good-practices-unveils-data-guide/>
66. Branch LS. Consolidated federal laws of Canada, Food and Drug Regulations [Internet]. 2023 [cité 25 avr 2023]. Disponible sur: [https://laws-lois.justice.gc.ca/eng/regulations/C.R.C.,\\_c.\\_870/](https://laws-lois.justice.gc.ca/eng/regulations/C.R.C.,_c._870/)
67. COFEPRIS: the Mexican health authority [Internet]. Regulatory Affairs in Latin America. 2012 [cité 29 avr 2023]. Disponible sur: <https://latampharmara.com/mexico/cofepris-the-mexican-health-authority/>
68. Sanitarios CF para la P contra R. gob.mx. [cité 30 avr 2023]. Anexos a la Norma Oficial Mexicana NOM-SSA1-059-2015. Disponible sur: <http://www.gob.mx/cofepris/documentos/anexos-a-la-norma-oficial-mexicana-nom-ssa1-059-2015>

## TITRE ET RÉSUMÉ EN ANGLAIS

### DATA INTEGRITY IN THE PHARMACEUTICAL INDUSTRIES: EVOLUTION OVER TIME AND AROUND THE WORLD

Data integrity consists of keeping data complete, reliable and credible throughout its lifecycle. To do this, it is necessary to respect each item of the ALCOA + principle: Attributable, Legible, Contemporaneous, Original and Accurate. These criteria can be achieved according to three levels of rigor, keeping in mind risk management.

Data Integrity can be applied in all companies, from those with old equipment to Industry 4.0. This is possible through IT and management. Data Integrity is then considered in several areas such as access management, types of backups and even Audit Trails.

In addition, to meet regulatory requirements, Data Integrity is starting to be deployed worldwide. Some Asian countries are tending to tighten their legislation by resorting to new guidelines. Other nations prefer to work with consulting firms in order to set up an appropriate system.

**AUTEUR :** GIL SARAH

**TITRE :** L'INTÉGRITÉ DES DONNÉES DANS LES INDUSTRIES PHARMACEUTIQUES : ÉVOLUTION AU COURS DU TEMPS ET DANS LE MONDE

**DIRECTRICE DE THÈSE :** ARELLANO CÉCILE

**LIEU ET DATE DE SOUTENANCE :** FACULTÉ DES SCIENCES PHARMACEUTIQUES DE TOULOUSE, LE 02/02/2024

---

### **RÉSUMÉ en français**

L'Intégrité des Données consiste à maintenir ces dernières entières, fiables et crédibles tout au long de leur cycle de vie. Il faut pour cela respecter chaque item du principe ALCOA + : Attribuable, Lisible, Contemporain, Original et Exact (Accurate). Ces critères peuvent être atteints selon trois niveaux de rigueur, en gardant à l'esprit le management des risques.

L'Intégrité des Données peut être appliquée dans toutes les entreprises, allant de celles pourvues d'anciens équipements aux industries 4.0. Cela est ainsi possible au travers de l'informatique et du management. L'Intégrité des Données est alors considérée dans plusieurs domaines tels que la gestion des accès, les types de sauvegardes ou encore les Audit Trails.

De plus, pour répondre aux exigences réglementaires, l'Intégrité des Données commence à être déployée dans le monde entier. Certains pays d'Asie tendent à durcir leurs législations en ayant recours à de nouvelles guidelines. D'autres nations préfèrent collaborer avec des sociétés de conseil afin de mettre en place un système approprié.

---

**Titre et résumé en anglais :** voir au recto de la dernière page de la thèse

---

**DISCIPLINE administrative :** PHARMACIE

---

### **MOTS-CLÉS :**

INTÉGRITÉ DES DONNÉES ; CYCLE DE VIE ; SÉCURITÉ ; MANAGEMENT DES RISQUES ; ALCOA + ; ÉQUIPEMENTS ; INFORMATIQUE ; INDUSTRIES 4.0 ; ASIE ; AMÉRIQUE DU NORD

---

### **INTITULÉ ET ADRESSE DE L'U.F.R. OU DU LABORATOIRE :**

Université Toulouse III Paul Sabatier, Faculté de Santé – Département des Sciences Pharmaceutiques  
35 Chemin des Maraîchers, 31062 TOULOUSE Cedex 9