Méthode d'analyse de la conformité des données et des équipements en accord avec les recommandations des autorités compétentes en termes de data integrity

Océanne Rumor

▶ **To cite this version:**

Océanne Rumor. Méthode d'analyse de la conformité des données et des équipements en accord avec les recommandations des autorités compétentes en termes de data integrity. Sciences pharmaceutiques. 2019. hal-03297923

HAL Id: hal-03297923
https://hal.univ-lorraine.fr/hal-03297923

Submitted on 23 Jul 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

UNIVERSITÉ DE LORRAINE

AVERTISSEMENT

Ce document est le fruit d'un long travail approuvé par le jury de soutenance et mis à disposition de l'ensemble de la communauté universitaire élargie.

Il est soumis à la propriété intellectuelle de l'auteur. Ceci implique une obligation de citation et de référencement lors de l'utilisation de ce document.

D'autre part, toute contrefaçon, plagiat, reproduction illicite encourt une poursuite pénale.

Contact : ddoc-thesesexercice-contact@univ-lorraine.fr

LIENS

Code de la Propriété Intellectuelle. articles L 122. 4
Code de la Propriété Intellectuelle. articles L 335.2- L 335.10
http://www.cfcopies.com/V2/leg/leg_droi.php
http://www.culture.gouv.fr/culture/infos-pratiques/droits/protection.htm

UNIVERSITE DE LORRAINE

2019

FACULTE DE PHARMACIE

THESE

Présentée et soutenue publiquement

Le 27 juin 2019, sur un sujet dédié à :

MÉTHODE D'ANALYSE DE LA CONFORMITÉ DES DONNÉES ET DES ÉQUIPEMENTS EN ACCORD AVEC LES RECOMMANDATIONS DES AUTORITÉS COMPÉTENTES EN TERMES DE DATA INTEGRITY

Pour obtenir

Le Diplôme d'Etat de Docteur en Pharmacie

Par Océanne Rumor

Née le 7 septembre 1992 à Champigny sur Marne (94)

Membres du Jury

Président : - Monsieur Igor Clarot – Professeur des Universités, Faculté de Pharmacie Nancy

Directeur : - Monsieur Pierre Noël Simon, Directeur Qualité / PRI, Société SPPH

Juges : - Madame Stéphanie Ribault, Responsable Qualité Opérationnelle, Société SPPH

- Madame Claudine Bonnetier, Pharmacien de production, Société SPPH

UNIVERSITÉ DE LORRAINE
FACULTÉ DE PHARMACIE
Année universitaire 2019-2020

DOYEN
Raphaël DUVAL
Vice-Doyen
Julien PERRIN
Directrice des études
Marie SOCHA
Conseil de la Pédagogie
Présidente, Brigitte LEININGER-MULLER
Vice-Présidente, Alexandrine LAMBERT
Collège d'Enseignement Pharmaceutique Hospitalier
Présidente, Béatrice DEMORE
Commission Prospective Facultaire
Président, Christophe GANTZER
Vice-Président, Jean-Louis MERLIN
Commission de la Recherche
Présidente, Caroline GAUCHER

Chargés de Mission

Communication	Marie-Paule SAUDER
Innovation pédagogique	Alexandrine LAMBERT
Référente ADE	Virginie PICHON
Référente dotation sur projet (DSP)	Marie-Paule SAUDER

Responsabilités

Filière Officine	Caroline PERRIN-SARRADO Julien GRAVOULET
Filière Industrie	Isabelle LARTAUD, Jean-Bernard REGNOUF de VAINS
Filière Hôpital	Béatrice DEMORE Marie SOCHA
Pharma Plus ENSIC	Jean-Bernard REGNOUF de VAINS
Pharma Plus ENSAIA	Xavier BELLANGER
Pharma Plus ENSGSI	Igor CLAROT
Cellule de Formation Continue et Individuelle	Luc FERRARI
Commission d'agrément des maîtres de stage	François DUPUIS
ERASMUS	Mihayl VARBANOV

DOYENS HONORAIRES

Chantal FINANCE
Francine PAULUS
Claude VIGNERON

PROFESSEURS EMERITES

Jeffrey ATKINSON
Max HENRY
Pierre LEROY
Claude VIGNERON

PROFESSEURS HONORAIRES

Jean-Claude BLOCK
Pierre DIXNEUF
Chantal FINANCE

MAITRES DE CONFERENCES HONORAIRES

Monique ALBERT
Mariette BEAUD
François BONNEAUX

Marie-Madeleine GALTEAU
Thérèse GIRARD
Pierre LABRUDE
Vincent LOPPINET
Philippe MAINCENT
Alain NICOLAS
Janine SCHWARTZBROD
Louis SCHWARTZBROD

Gérald CATAU
Jean-Claude CHEVIN
Jocelyne COLLOMB
Bernard DANGIEN
Marie-Claude FUZELLIER
Françoise HINZELIN
Marie-Hélène LIVERTOUX
Bernard MIGNOT
Blandine MOREAU
Dominique NOTTER
Francine PAULUS
Christine PERDICAKIS
Marie-France POCHON
Anne ROVEL
Gabriel TROCKLE
Maria WELLMAN-ROUSSEAU
Colette ZINUTTI

ASSISTANTS HONORAIRES

Marie-Catherine BERTHE
Annie PAVIS

ENSEIGNANTS	*Section CNU* *	*Discipline d'enseignement*

PROFESSEURS DES UNIVERSITES - PRATICIENS HOSPITALIERS

Danièle BENSOUSSAN-LEJZEROWICZ	*82*	*Thérapie cellulaire*
Béatrice DEMORE	*81*	*Pharmacie clinique*
Jean-Louis MERLIN	*82*	*Biologie cellulaire*
Jean-Michel SIMON	*81*	*Economie de la santé, Législation pharmaceutique*
Nathalie THILLY	*81*	*Santé publique et Epidémiologie*

PROFESSEURS DES UNIVERSITES

Ariane BOUDIER ¤	*85*	*Chimie Physique*
Christine CAPDEVILLE-ATKINSON	*86*	*Pharmacologie*
Igor CLAROT	*85*	*Chimie analytique*
Joël DUCOURNEAU	*85*	*Biophysique, Acoustique, Audioprothèse*
Raphaël DUVAL	*87*	*Microbiologie clinique*
Béatrice FAIVRE	*87*	*Hématologie, Biologie cellulaire*
Luc FERRARI	*86*	*Toxicologie*
Pascale FRIANT-MICHEL	*85*	*Mathématiques, Physique*
Christophe GANTZER	*87*	*Microbiologie*
Frédéric JORAND	*87*	*Eau, Santé, Environnement*
Isabelle LARTAUD	*86*	*Pharmacologie*
Dominique LAURAIN-MATTAR	*86*	*Pharmacognosie*
Brigitte LEININGER-MULLER	*87*	*Biochimie*
Patrick MENU	*86*	*Physiologie*
Jean-Bernard REGNOUF de VAINS	*86*	*Chimie thérapeutique*
Bertrand RIHN	*87*	*Biochimie, Biologie moléculaire*

MAITRES DE CONFÉRENCES DES UNIVERSITÉS - PRATICIENS HOSPITALIERS

Alexandre HARLE	*82*	*Biologie cellulaire oncologique*
Julien PERRIN	*82*	*Hématologie biologique*

Loïc REPPEL	*82*	*Biothérapie*
Marie SOCHA	*81*	*Pharmacie clinique, thérapeutique et biotechnique*

MAITRES DE CONFÉRENCES

Xavier BELLANGER ¤	*87*	*Parasitologie, Mycologie médicale*
Emmanuelle BENOIT ¤	*86*	*Communication et Santé*
Isabelle BERTRAND	*87*	*Microbiologie*
Michel BOISBRUN ¤	*86*	*Chimie thérapeutique*
Cédric BOURA ¤	*86*	*Physiologie*
Sandrine CAPIZZI BANAS	*87*	*Parasitologie*
Antoine CAROF ¤	*85*	*Informatique*
Sébastien DADE	*85*	*Bio-informatique*
Dominique DECOLIN	*85*	*Chimie analytique*
Natacha DREUMONT ¤	*87*	*Biochimie générale, Biochimie clinique*
Florence DUMARCAY ¤	*86*	*Chimie thérapeutique*
François DUPUIS ¤	*86*	*Pharmacologie*
Reine EL OMAR	*86*	*Physiologie*
Adil FAIZ	*85*	*Biophysique, Acoustique*
Anthony GANDIN	*87*	*Mycologie, Botanique*
Caroline GAUCHER ¤	*86*	*Chimie physique, Pharmacologie*
Stéphane GIBAUD ¤	*86*	*Pharmacie clinique*
Thierry HUMBERT	*86*	*Chimie organique*
Olivier JOUBERT ¤	*86*	*Toxicologie, Sécurité sanitaire*

ENSEIGNANTS (suite)	*Section CNU* *	*Discipline d'enseignement*
Alexandrine LAMBERT	*85*	*Informatique, Biostatistiques*
Julie LEONHARD	*86/01*	*Droit en Santé*
Christophe MERLIN ¤	*87*	*Microbiologie environnementale*
Maxime MOURER	*86*	*Chimie organique*
Coumba NDIAYE	*86*	*Epidémiologie et Santé publique*
Arnaud PALLOTTA	*86*	*Bioanalyse du médicament*
Marianne PARENT	*85*	*Pharmacie galénique*
Caroline PERRIN-SARRADO	*86*	*Pharmacologie*
Virginie PICHON	*85*	*Biophysique*
Sophie PINEL ¤	*85*	*Informatique en Santé (e-santé)*
Anne SAPIN-MINET ¤	*85*	*Pharmacie galénique*
Marie-Paule SAUDER	*87*	*Mycologie, Botanique*
Guillaume SAUTREY	*85*	*Chimie analytique*
Rosella SPINA	*86*	*Pharmacognosie*
Sabrina TOUCHET	*86*	*Pharmacochimie*
Mihayl VARBANOV	*87*	*Immuno-Virologie*
Marie-Noëlle VAULTIER	*87*	*Mycologie, Botanique*
Emilie VELOT ¤	*86*	*Physiologie-Physiopathologie humaines*
Mohamed ZAIOU ¤	*87*	*Biochimie et Biologie moléculaire*

PROFESSEUR ASSOCIE

Julien GRAVOULET	*86*	*Pharmacie clinique*

PROFESSEUR AGREGE

Christophe COCHAUD *11* *Anglais*

¤ *En attente de nomination*

ᴴ *Maître de conférences titulaire HDR*

***** *<u>Disciplines du Conseil National des Universités</u> :*
80 : Personnels enseignants et hospitaliers de pharmacie en sciences physico-chimiques et ingénierie appliquée à la santé
81 : Personnels enseignants et hospitaliers de pharmacie en sciences du médicament et des autres produits de santé
82 : Personnels enseignants et hospitaliers de pharmacie en sciences biologiques, fondamentales et cliniques
85 ; Personnels enseignants-chercheurs de pharmacie en sciences physico-chimiques et ingénierie appliquée à la santé
86 : Personnels enseignants-chercheurs de pharmacie en sciences du médicament et des autres produits de santé
87 : Personnels enseignants-chercheurs de pharmacie en sciences biologiques, fondamentales et cliniques

11 : Professeur agrégé de lettres et sciences humaines en langues et littératures anglaises et anglo-saxonnes

« LA FACULTE N'ENTEND DONNER AUCUNE APPROBATION, NI IMPROBATION AUX OPINIONS EMISES DANS LES THESES, CES OPINIONS DOIVENT ETRE CONSIDEREES COMME PROPRES A LEUR AUTEUR ».

SERMENT DES APOTHICAIRES

Je jure, en présence des maîtres de la Faculté, des conseillers de l'ordre des pharmaciens et de mes condisciples.

> **D'honorer ceux qui m'ont instruit dans les préceptes de mon art et de leur témoigner ma reconnaissance en restant fidèle à leur enseignement.**
>
> **D'exercer, dans l'intérêt de la santé publique, ma profession avec conscience et de respecter non seulement la législation en vigueur, mais aussi les règles de l'honneur, de la probité et du désintéressement.**
>
> **De ne jamais oublier ma responsabilité et mes devoirs envers le malade et sa dignité humaine ; en aucun cas, je ne consentirai à utiliser mes connaissances et mon état pour corrompre les mœurs et favoriser des actes criminels.**

Que les hommes m'accordent leur estime si je suis fidèle à mes promesses.

Que je sois couvert d'opprobre et méprisé de mes confrères si j'y manque.

Remerciements

Je souhaite remercier en premier lieu mon Directeur de thèse, M. Pierre-Noël Simon, Directeur Qualité et Pharmacien Responsable Intérimaire chez SPPH, de m'avoir accueillie en stage puis gardée dans son service durant mon M2. Je tiens à le remercier également pour la bienveillance dont il a fait preuve à mon égard, pour sa sympathie et sa bonne humeur.

Mes remerciements vont également à Monsieur Igor Clarot, Président de Jury et co-Directeur de thèse pour sa sympathie et sa patience durant ces années de préparation de thèse.

J'adresse de chaleureux remerciements à Stéphanie qui fût pour moi une profonde source d'inspiration humaine. Une personne qui retire le meilleur de chacun de nous, merci !

Merci également à Claudine qui m'a fait l'honneur de bien vouloir faire partie de mon jury, merci pour ta sympathie, ta douceur et ton sens de l'écoute.

Je n'oublie pas non plus toute l'équipe Qualité avec qui j'ai passé (et je passe toujours !) de très bons moments au quotidien. Merci à Kévin, la force tranquille de notre bureau, toujours prêt à me donner de bons conseils et m'aider dans mes recherches. Plus généralement merci à toutes les personnes que j'ai plaisir à côtoyer chaque jour au travail, les teams soirées, la team sport et la team pause de 10h.

Merci à la Direction SPPH, Eric Villette, Pierre Moissette, pour la confiance qu'ils m'accordent au quotidien.

Merci à la Dream Team, Camille, Caro et Kim d'avoir été présentes durant toutes ces années. Pour toutes ces crises de fou-rires et ces merveilleux moments… merci !

Je remercie également ma famille de m'avoir boostée durant toutes ces années d'études et plus spécifiquement pour passer ma thèse (« Quand est-ce que tu passes ta thèse ??! »), pour avoir cru en moi. A Maman, Papa, Romane, Mamie et Mémère, je vous aime !

Enfin, je remercie mon compagnon, Jonathan, de m'avoir apporté son soutien inconditionnel durant toutes ces années. Même en pyjama rose piloupilou de la PACES tu m'as aimé !

Je dédie cette thèse à mon Papi « chéri de mon cœur que j'aime passionnément par-dessus tout et à la folie... », à André

TABLE DES MATIERES

Table des illustrations **12**
Liste des tableaux **13**
Liste des abréviations **14**
PARTIE 1 : CONTEXTE ET EXPLICATION DE LA NOTION DE DATA INTEGRITY
1 Introduction **15**
1 Qu'est-ce qu'une donnée **18**
1.1 Une donnée dite « BPF » 19
1.2 Donnée brute et métadonnée 19
1.3 Enregistrement original 20
1.4 Vraie copie 21
2 Management de l'intégrité des données **21**
2.1 La liste ALCOA + ... 21
2.2 Connaissance et prise de décision 23
3 Contexte règlementaire **26**
3.1 Ecart relevés par les autorités de santé 26
3.2 Parallèle et différences entre les BPF et les notions ALCOA 31
4 Cycle de vie d'une donnée **36**
4.1 Enregistrement 36
4.1.1 Format des données 36
4.1.2 Inclusion / exclusion des données 37
4.1.3 Enregistrement manuel 37
4.1.4 Enregistrement électronique 37
4.1.5 Droits d'accès et administration 38
4.1.6 Signature électronique 41
4.2 Traitement 44
4.3 Contrôle 44
4.3.1 Audit trail 44
4.3.2 Contrôle des données 45
4.4 Stockage / Archivage / Destruction 46
5 Conclusion de la première partie **47**
PARTIE 2 : ANALYSES DE RISQUE DATA INTEGRITY ASSOCIEES AUX EQUIPEMENTS ET AUX DONNEES
6 Scope et définitions **49**
6.1 Analyses de risques 49

6.1.1 Risque 49
6.1.2 Management des risques 50
6.2 Système 51
6.3 Système informatique 52
6.4 Système informatisé 52
6.5 Validation 54
6.5.1 Validation prospective 55
6.5.2 Validation rétrospective 55
6.5.3 Validation concomitante 55
6.6 Qualification 55
6.6.1 QC : Qualification de conception 56
6.6.2 QI : Qualification d'installation 57
6.6.3 QO : Qualification opérationnelle 58
6.6.4 QP : Qualification des performances 58
6.7 Data management 58
7 Analyse de risque de l'équipement 59
7.1.1 Complexité logiciel 60
7.1.2 Complexité matériel 61
7.1.3 Indice de complexité 62
8 Analyse de risques système 63
8.1 Sensibilité 63
8.1.1 La subjectivité 63
8.1.2 Traçabilité 65
8.1.3 L'accessibilité 66
8.1.4 Indice de sensibilité 67
8.2 Criticité 67
8.2.1 Patient / Consommateur 67
8.2.2 Organisationnel / Financier 68
8.2.3 Responsabilité / Image client 70
8.2.4 Indice de criticité 71
8.3 Résultats de l'analyse de risque et degré de validation 71
8.4 Classement des données 72
9 Conclusion de la deuxième partie 74
10 Conclusion générale 75
11 Annexes 76

11.1 Annexe 1 76
12 Bibliographie 79
Résumé 81

TABLE DES ILLUSTRATIONS

Figure 1 - Illustration du rang d'une donnée à l'échelle de la connaissance 18
Figure 2 Schéma d'illustration Donnée brute / Métadonnée 20
Figure 3 - Intégrité des données et management de la qualité 24
Figure 4 - Nombre de warning letters impliquant une perte d'intégrité des données depuis 2008 jusqu'à 2017 29
Figure 5 - Répartition en Pourcentage des types d'Ecarts en référence au CFR part 21 30
Figure 6 - Cycle de vie d'une donnée 36
Figure 7 Schéma droits d'accès 39
Figure 8 Droits d'accès d'un système d'édition et d'impression d'étiquettes 40
Figure 9 Schéma du mécanisme de cryptage et de décryptage d'une signature électronique 42
Figure 10 Schéma illustrant le parallèle entre la signature électronique et la signature manuscrite 43
Figure 11 Exemple de signature manuscrite scannée 44
Figure 15 - Composantes du management des risques 51
Figure 12 Système informatisé et environnement opérationnel - PIC/S 53
Figure 13 Exemple d'une système informatisé - HPLC 54
Figure 14 - Etapes de qualification d'un equipement 56
Figure 16 Etude de complexité du système informatisé 60
Figure 17 - Classement des données en fonction de leur sensibilité et de leur criticité 73

LISTE DES TABLEAUX

Tableau I Exemples et contres-exemples d'illustration des notions ALCOP 23
Tableau II - Extraits d'écarts issus de Warning letters en lien avec l'intégrité des données de 2015 à 2017 28
Tableau III - Réparatitions des écarts en lien avec le CFR part 21 formulés à des entreprises de production de médicaments sur l'année 2017 29
Tableau IV Comparatif des notions ALCOA et du guide des BPF 32
Tableau V Echelle de complexité - Logiciel.....61
Tableau VI Echelle de complexité - Matériel.....61
Tableau VII - Qualification nécessaire en fonction de la complexité du système 62
Tableau VIII Représentativité des données en fonction de la complexité du système 64
Tableau IX Echelle de risque associé - Subjectivité.....65
Tableau X Echelle de risque associé - trçabilité.....66
Tableau XI Echelle de risque associé - Accessibilité 67
Tableau XII Echelle de criticité – Impact Patient / consommateur 68
Tableau XIII Echelle de criticité - Impact Organisationnel / Financier 69
Tableau XIV Echelle de criticité - Impact Responsabilité / Image client.....70
Tableau XV - Validation nécessaire en fonction de la sensibilité et de lacriticité du système informatisé.....71

LISTE DES ABRÉVIATIONS

FDA : Food and Drug Administration

cGMP : current Good Manufacturing Practices

CFDA: China Food and Drug administration

MHRA : UK's Medicine and Healthcare products Regulatory Agency

EMA: European Medicines Agency

PIC'S: Pharmaceutical Inspection Co-operation Scheme

OMS : Organisation Mondiale de la Santé

ANSM : Agence Nationale de Sécurité du médicament et des Produits de Santé

BPF: Bonnes Pratiques de Fabrication

PDF: Portable Document Format

ALCOA : Attributable Legible Contemporaneous Original Accurarte

ALCOP : Attribuable Lisible Contemporaine Originale Précise

BPR : Bonnes Pratiques de Rédaction

USA : United States of America

CFR : Code of Federal Regulations

ROM : Read Only Memory

OS : Operating System

VP: Validation d'un proceed

QC : Qualification de Conception

QI : Qualification d'Installation

QO : Qualification opérationnelle

QP : Qualification de Performance

DE : Données d'entrée

FAT: Factory Acceptance Test

SAT: Site Acceptance Test

ISO: International Organization for Standardization

IEC : International Electrotechnical Commission

IT : Informatique

1 INTRODUCTION

« Data Integrity », traduit littéralement en Français par « Intégrité des données » est un élément fondamental du système de management de la qualité. Il s'agit d'une méthode visant à garantir la fiabilité et la précision des données émanant des différentes opérations ayant conduit à l'obtention du produit fini (commandes, production, contrôle, approvisionnement...). Ces exigences s'appliquent tant aux données générées manuellement (format papier), qu'aux données informatiques.

Il s'agit à l'heure actuelle d'un des sujets majeurs pour les autorités pharmaceutiques.

Ces dernières années, la FDA (*Food and Drug Administration*) a constaté, lors des inspections CGMP (*Current Good Manufacturing Practices*), une augmentation significative des infractions impliquant la violation de l'intégrité des données au sein des différentes entreprises. En réponse à cela, la FDA a publié en avril 2016, une esquisse de guide intitulé *Data Integrity and Compliance with CGMP*.

En 2015 et 2016 six autorités majeures internationales ont publié des guides, de formes variables, à ce sujet. Deux documents publiés initialement respectivement par la *US Food and Drug Administration* (FDA) en avril 2016 et par l'Agence Européenne du médicament (EMA) en Août 2016 ont fait le choix d'un format questions /réponses. Les guides provenant de la *China Food and Drug Administration* (CFDA) ainsi que de la *UK's Medicines and Healthcare products Regulatory Agency* (MHRA), du *Pharmaceutical Inspection Co-operation Scheme* (PIC/S) et de l'Organisation Mondiale de la Santé (OMS) ont quant à eux fait le choix d'un format classique narratif. Ceci étant dit, tous ces guides sont sensiblement similaires à propos de ce qu'ils attendent des entreprises pharmaceutiques. (1)

Côté Français, depuis 2017, l'Agence Nationale de Sécurité du médicament et des Produits de Santé (ANSM) a constaté une hausse non négligeable du nombre et des types de problèmes liés à l'intégrité des données. Par ailleurs, les cas de fraudes ont été décrits par l'ANSM comme étant « de plus en plus fréquents et sophistiqués » même s'ils ne représentent actuellement que moins de 5% des cas de défaut d'intégrité des données.

Un document d'information, intitulé « Focus sur l'intégrité des données » a notamment été publié en novembre 2017. L'ANSM rappelle par ailleurs, dans cette présentation qu'aucun texte législatif supplémentaire n'a été publié à ce jour. Les notions fondamentales du *Data Integrity* sont retrouvent à l'heure actuelle dans le guide des Bonne Pratiques de Fabrication. (2)

Les entreprises doivent mettre en place des stratégies significatives et efficaces pour gérer leurs données et écarter les risques liés à la perte de leur intégrité, qu'elle soit volontaire ou non. Ces stratégies seront basées sur la compréhension des procédés et la gestion des connaissances technologiques.

L'intégrité des données est un élément fondamental du système Qualité car elle aide à garantir la sécurité du patient, à assurer la conformité réglementaire de l'entreprise et elle fournit également à cette dernière un avantage compétitif non négligeable qui se traduit suivant deux aspects : la confiance du consommateur et l'analyse fine et fiable des processus de production.

PARTIE 1 : CONTEXTE ET EXPLICATION DE LA NOTION DE DATA INTEGRITY

1 QU'EST-CE QU'UNE DONNEE

Le dictionnaire Larousse donne la définition suivante d'une donnée : « Ce qui est connu ou admis comme tel, sur lequel on peut fonder un raisonnement, qui sert de point de départ pour une recherche. ». (3)

Cette définition met en lumière une des caractéristiques premières que doit posséder une donnée, selon les recommandations en matière de *Data Integrity*, à savoir, la fiabilité ou vraisemblance. Une donnée est un élément qui sert de point d'appui à différents acteurs. L'entreprise elle-même, qui évalue la qualité des produits finis, les autorités amenées à contrôler ces données mais également et surtout, le consommateur final qui fonde sa confiance sur les éléments qui lui parviennent au sujet du produit consommé ou utilisé.

Cette seule définition ne suffit cependant pas à définir pleinement ce qu'est une donnée. En effet, une donnée ne peut se résumer comme un fait établi. Il s'agit plus précisément d'une information brute ou donnée brute accompagnée d'un contexte ou métadonnée.

La Figure 1 renseigne sur la place d'une donnée à l'échelle de la connaissance générale.

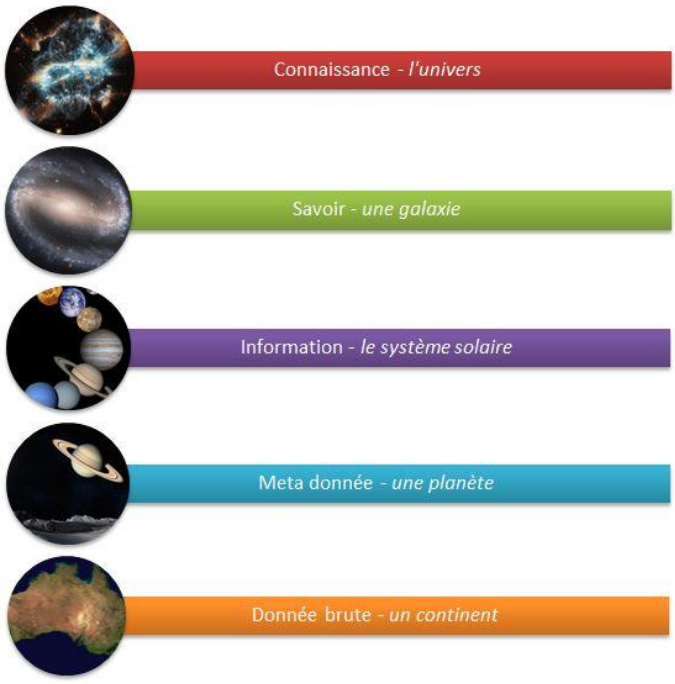

FIGURE 1 - ILLUSTRATION DU RANG D'UNE DONNEE A L'ECHELLE DE LA CONNAISSANCE

Une donnée est une information qui peut exister sous différentes formes, au format électronique ou papier. Les données peuvent se présenter sous forme de textes, de graphiques, de nombres, d'enregistrements audio, d'images mais également de résultats ou de rapports finaux.

1.1 UNE DONNEE DITE « BPF »

Les « BPF » sont les *Bonnes Pratiques de Fabrication* ou « cGMP » *current Good Manufacturing Practices* en anglais. Elles sont définies par l'Organisation Mondiale de la Santé OMS comme étant : « un des éléments de l'assurance de la qualité, garantissant que les produits sont fabriqués et contrôlés de façon uniforme et selon des normes de qualité adaptées à leur utilisation et spécifiées dans l'autorisation de mise sur le marché». (4)

On considère une donnée comme étant un enregistrement BPF, c'est-à-dire « la preuve des différentes actions entreprises pour démontrer la conformité aux instruction » (5), soit :

- Lorsque celle-ci est explicitement demandée par les instances réglementaires comme la FDA, l'ANSM, le MHRA, l'EMA ou dans des textes de loi.
- Lorsqu'il s'agit d'une donnée qui est générée pour démontrer la conformité avec de telles exigences même si elle n'est pas demandée explicitement (exemple : éléments de preuve en cas d'anomalie ou non-conformité sur un produit ou tout autre élément du processus de production)

Dès l'instant qu'une donnée est générée pour répondre à un requis BPF, elle devient automatiquement un enregistrement BPF et elle doit donc être conforme aux exigences de qualité et d'intégrité BPF.

1.2 DONNEE BRUTE ET METADONNEE

Une donnée brute est un enregistrement original obtenu dans le format dans lequel il a été initialement généré, papier ou électronique.

La qualité des données ne peut être assurée que si des métadonnées y sont associées. Une métadonnée a pour rôle de décrire les attributs des autres données (contexte, signification, unité, structure, interconnexions...). Les métadonnées font partie intégrante de l'enregistrement original, sans elles, la donnée n'a aucune signification.

Prenons l'exemple d'une cellule : sans contexte particulier cette information ne nous renseigne que très peu. Nous ne pouvons que supposer qu'elle forme avec d'autres cellules, un épithélium, un tissu organique de revêtement, sans aucune autre information sur sa fonction ou sa localisation. Cette cellule est notre donnée brute.

L'information complète, serait quant à elle : « cellule épithéliale pavimenteuse simple de l'endocarde ». Nous retrouvons la donnée brute à laquelle s'ajoutent les métadonnées qui renseignent sur la localisation et la fonction de cette cellule. La qualité des métadonnées associées permet de donner une vision claire et utilisable de l'information.

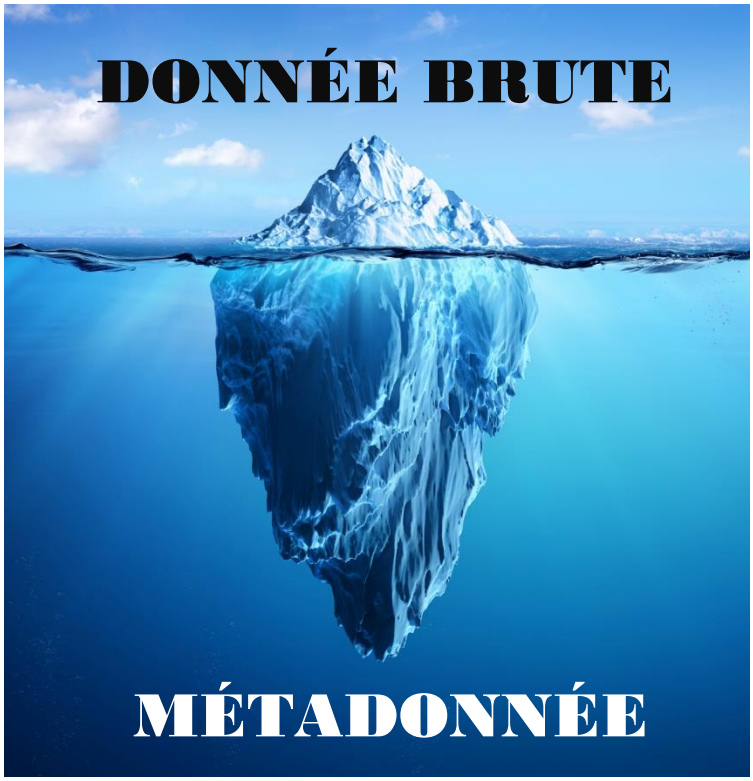

FIGURE 2 SCHEMA D'ILLUSTRATION DONNEE BRUTE / METADONNEE

Une métadonnée est donc une information nécessaire sur le contexte pour comprendre la donnée.

1.3 ENREGISTREMENT ORIGINAL

Un enregistrement original constitue un fichier ou une donnée dans le format dans lequel elle a été initialement générée et dont l'intégrité a été préservée.

Exemple : Enregistrement papier original complété par une responsable de ligne, donnée brute issue d'un système informatique.

Une donnée peut être statique, fixe à l'image d'un enregistrement papier ou *Portable Document Format* (bien que dans certains cas le format PDF ne soit pas totalement statique). Dans un enregistrement statique, les données sont fixes, elles sont figées, sans possibilité d'interaction. Des enregistrements papier, des images électroniques (dans une moindre mesure) sont des enregistrements statiques. Une donnée peut

également être dynamique, c'est-à-dire sous forme d'un enregistrement ou d'une donnée informatique avec lequel l'utilisateur peut interagir.

Pour illustrer cette notion, prenons l'exemple des mesures de chromatographie assistées par ordinateur. Les systèmes de chromatographie informatisés fournissent des données électroniques dynamiques qui donnent la possibilité à l'utilisateur d'interagir avec les données afin de visualiser l'intégration plus clairement, il s'agit de données dynamiques. Par exemple, il est possible, via le logiciel de modifier la ligne de base ou de cacher certains champs afin de permettre une meilleure vision du chromatogramme. Une fois le chromatogramme imprimé, la possibilité d'interaction est perdue, la donnée est devenue statique.

1.4 VRAIE COPIE

Une copie authentique est une copie de l'enregistrement original qui aura été contrôlée comme étant exacte et possédant les mêmes attributs et informations que la donnée originale. La copie peut être approuvée par une signature datée ou par signature électronique validée. Enfin, une copie authentique, peut avoir un format différent de la donnée originale mais elle doit cependant garder le même caractère statique ou dynamique que cette dernière.

2 MANAGEMENT DE L'INTEGRITE DES DONNEES

Le système de management de la qualité doit être appliqué à toutes les étapes de cycle de vie des données, et ce, afin d'assurer que les actions réalisées et les décisions prises en aval le soient de manière consciente et éclairée.

Les Bonnes Pratiques Documentaires font partie intégrante de la notion d'intégrité des données et sont le support d'une gestion efficace.

2.1 LA LISTE ALCOA +

L'acronyme ALCOA ou ALCOP traduit littéralement en français a été inventé par un inspecteur de la FDA pour traduire la notion de « Data Integrity ». En effet Stan Wooler, utilise ce terme pour la première fois dans les années 1990 pour l'aider à se souvenir des conditions de conformité pertinentes de l'intégrité des données. Il a choisi cet acronyme en référence au nom d'une société très connue née aux USA en 1886 : **Al**uminium **Co**mpany of **A**merica.

Il s'agit d'une liste d'attributs que doivent posséder les données de l'entreprise concernée. ALCOA se rapporte à la fois aux données papier, aux sources électroniques et aux enregistrements qui contiennent ces données.

Une version plus contemporaine de cette liste a vu le jour sous le nom de ALCOA Plus. Ces grandes notions sont également des concepts clefs des Bonnes Pratiques Documentaires. Selon cet acronyme la donnée doit être :

- **Attributable** : attribuable à la personne qui l'a générée. Il doit être possible d'identifier clairement la personne qui a réalisé la tâche enregistrée. Cette caractéristique a deux objectifs. Le premier est de démontrer et de vérifier, lors par exemple de la revue d'un dossier, que l'action a été réalisée par une personne qualifiée et compétente pour cette tâche. Le second est de pouvoir tracer tout changement, correction ou suppression appliqué à l'enregistrement.

- **Legible** : lisible et permanente. Les données doivent être facilement lisibles pour les personnes concernées. Elles doivent donc être accessibles et proprement reportées. Lors de corrections, les données manuscrites doivent être barrées de façon à laisser apparaitre l'information corrigée. Il en va de même lors de modifications informatiques : les nouvelles informations générées ne doivent pas se substituer aux précédentes. Il doit être possible d'en conserver la trace.

- **Contemporaneous** : contemporaine. L'enregistrement d'une donnée doit être simultané à l'action de façon à conserver sa représentativité et attester de ce qui a été réalisé en conditions réelles d'exécution.

- **Original** : originale ou une copie authentique. Une donnée originale peut se traduire comme une donnée primaire. Il s'agit de la première information générée et recueilli après l'action. Cette dernière, même lorsqu'elle est erronée, ne doit jamais être supprimée. Elle doit rester accessible et lisible à tout moment. Enfin, lorsqu'une donnée est générée dans un format dynamique, elle doit être autant que possible conservée dans ce format d'origine.

- **Accurate** : précise / exacte / correcte. Les prises de décision, tel qu'un retrait de lot, s'effectuent sur la base des données fournies. L'exactitude d'une donnée présentée constitue donc un des éléments essentiels de la qualité du produit final. Elle repose sur trois principes : la fiabilité du système qui la génère, la compétence et l'implication du personnel qui la recueille et l'absence de dissimulation en cas d'erreur.

Plus : Fiable, complète, cohérente, avérée, représentative de la situation.

ALCOA (+) implique des termes supplémentaires basés sur le concept de l'EMA et de l'OMS sur les données électroniques. Les termes complémentaires sont complète, cohérente (consistent), durable (enduring) et disponible (available). (6)

Le Tableau I ci-après illustre chaque notion de façon plus précise à l'aide d'un exemple ainsi qu'un contre-exemple :

TABLEAU I EXEMPLES ET CONTRES-EXEMPLES D'ILLUSTRATION DES NOTIONS ALCOP

Attribut	Exemples	Contre-exemples
Attribuable	Déconnexion systématique d'un système informatique lorsqu'il n'est pas utilisé par la personne. Présence de logins, identifiants, signatures électroniques.	Enregistrement complété manuellement par une autre personne que celle qui a réalisé l'action, en imitant sa signature.
Lisible	Enregistrement des contrôles de poids proprement au stylo bleu permanent (BPR - Bonnes pratiques de rédaction). Cahiers (de route ou de laboratoire) reliés et paginés.	Effacement du ticket de pesée imprimé après 2 ans de stockage dans le dossier de lot.
Contemporaine	Contrôles en cours de production réalisés toutes les 30 minutes reportés en temps réel.	Date et heures de pesée des matières premières complétées en avance afin de gagner du temps.
Originale	Ticket d'impression issu d'une erreur de pesée joint au dossier de lot et commenté.	Chromatogramme non conforme d'une matière première supprimé et remplacé par une analyse conforme après répétition des mesures.
Précise	Ticket de pesée issu d'une balance qualifiée et validée.	Heure de début et de fin de transfert de vrac relevées à l'aide de deux horloges différentes ayant 5 minutes de décalage entre elles.

2.2 CONNAISSANCE ET PRISE DE DECISION

L'intégrité des données permet de garantir la qualité du produit et d'apporter de la transparence aux autorités de santé et au consommateur final. Si l'intégrité des données générées n'a pas été maintenue, le produit peut être rappelé du marché créant ainsi de la méfiance et de la confusion chez le patient / consommateur final ainsi qu'au niveau des autorités de santé.

L'intégrité des données permet également un management efficace de la qualité des produits et éviter ainsi les retards ou arrêts de production qui peuvent conduire à des pénuries sur le marché. La figure ci-après décrit l'impact de la connaissance sur les prises de décisions :

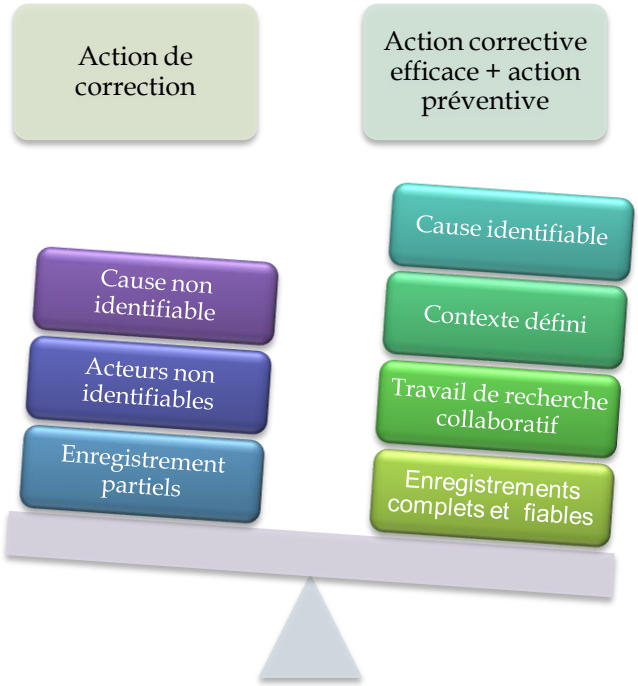

FIGURE 3 - INTEGRITE DES DONNEES ET MANAGEMENT DE LA QUALITE

Lors de l'apparition d'une non-conformité, dans le cas d'une faiblesse de l'intégrité des données, le manque d'informations ne pourra aboutir à la détection de la cause racine du problème, c'est-à-dire l'évènement ayant entraîné la conformité. Alors, seules des actions de correction, c'est-à-dire des actions ayant pour but d'éliminer la non-conformité elle-même et non sa cause, pourront être mises en place. La non-conformité pourra donc se reproduire car sa cause n'a pas été éliminée.

A l'inverse lorsque les acteurs disposent de tous les éléments et donc de toutes les données, la cause racine pourra être dévoilée et des actions correctives (et préventives) pourront être mises en place. Il s'agira là d'actions qui permettront, non plus seulement d'éliminer la non-conformité en elle-même mais également sa cause. Cette non-conformité ne se reproduira donc plus.

Outre le fait de permettre de mettre en place des actions efficaces, l'intégrité des données permet également dans certaines situations de limiter les conséquences du défaut. Prenons un exemple concret pour illustrer ce propos :

20 kg de matière première ont été incorporés deux fois dans le mélangeur au cours de la première étape de la fabrication d'un vrac de produit.

Cas 1 : Ce n'est pas la personne qui a incorporé les matières qui réalise les enregistrements de fabrication (donnée non attribuable) et les enregistrements d'incorporation ne sont pas réalisés à chaque étape mais en une fois à la fin de la fabrication afin de gagner du temps (donnée non contemporaine). La personne qui complète l'enregistrement a surveillé de loin la personne qui a réalisé la fabrication et sait qu'il est un bon élément donc complète le process de fabrication sans craintes d'erreur.

Le responsable de fabrication contrôle le dossier de fabrication, tout est conforme, le conditionnement du vrac peut débuter. Le vrac de matière est conditionné et analysé par le laboratoire de contrôle qui détecte une non-conformité dans les paramètres physico-chimiques du produit. L'équipe qualité étudie le dossier d'enregistrement et interview les équipes, rien d'anormal ne s'est produit, les produits finis sont détruits.

Perte cas 1 : un lot de produit fini + deux postes (7heures de travail) sur 5 personnes.

Cas 2 : La personne qui réalise la fabrication complète un enregistrement à chaque étape d'incorporation d'une matière première. Au moment de compléter la ligne qui correspond à la matière déjà incorporée, elle se rend compte qui celle-ci est déjà remplie et que la matière a été incorporée deux fois. Il prévient son responsable qui contacte l'équipe qualité.

L'équipe qualité donne son accord pour que par dérogation toutes les autres matières soient doublées, car le mélange a également été validé sur une taille de lot supérieure et qu'il s'agit de la première étape de fabrication. Sous la supervision d'un membre de l'équipe qualité et du responsable de fabrication toutes les matières sont doublées et les enregistrements complétés en conséquence. Un échantillon de vrac est envoyé au laboratoire de contrôle pour analyse, tout est conforme, le conditionnement peut débuter. Le vrac est conditionné et contrôlé conforme par le laboratoire.

Perte cas 2 : temps humain + analyses de laboratoire complémentaires.

La gestion de l'intégrité des données doit être comprise et mise en application par l'ensemble des acteurs de l'entreprise afin d'être efficace. Elle doit également être basée sur la transparence et la confiance et ne peut fonctionner dans un climat de sanctions.

3 CONTEXTE REGLEMENTAIRE

3.1 ECART RELEVES PAR LES AUTORITES DE SANTE

Comme évoqué en introduction, les différentes autorités de santé qu'elles soient outre-Atlantique (FDA) ou Européennes (EMA, MHRA, ANSM), ont constaté ces dernières années, une augmentation significative du nombre et des types de problèmes liés à l'intégrité des données.

Nous allons passer en revue les différents types d'écarts relevés lors des inspections de ces autorités afin de comprendre l'origine de la nécessité de publication de guides complémentaires et du renforcement des contrôles.

Ecarts fréquents relevés lors des inspection ANSM : (2)

Falsifications :

- Données analytiques, de production et règlementaires falsifiées : existantes et enregistrées comme étant nouvelles, données fabriquées, données manipulées (voir paragraphe 'analyses non officielles des échantillons de contrôle qualité')
- Origine de la substance active falsifiée

Manque de gestion :

- Gestion des formulaires vierges non maitrisée
- Enregistrements réécrits (avec ou sans modifications)
- Formulaires vierges partiellement remplis mis au rebut
- Données non enregistrées en temps réel
- Enregistrements antidatés
- Enregistrements non remplis par la personne ayant réalisé l'action
- Enregistrements de contrôle ou dossiers de lots de production non disponibles

Systèmes informatisés mal conçus et/ou mal contrôlés :

- Des systèmes informatisés mal conçus et/ou mal contrôlés :
- Absence de système de gestion des profils d'utilisateurs :
- Pas d'identifiant ni de mot de passe,
- Profil partagé ou profil administrateur en libre accès
- Absence d'« audit trail » ou « audit trail » inactivé
- Absence de protection contre la suppression des données
- Absence de sauvegarde des données

Analyses non officielles des échantillons de contrôle qualité :

- « Echantillon test » : un échantillon est sélectionné pour avoir un 'aperçu' du résultat et prendre des mesures pour que les analyses soient conformes = «analyse orientée vers un résultat cible»
- Ré-analyses jusqu'à l'obtention de résultats acceptables
- Données enregistrées incomplètes ou rapport sélectif
- Intégration manuelle erronée des pics chromatographiques

Ecarts identifiés dans les warning letters de la FDA :

Les warning letters, traduites en français par « lettre d'avertissement » sont l'équivalent des lettres d'injonction émises par l'ANSM. Elle est définie par la FDA comme suit : « La lettre d'avertissement identifie l'infraction, telle que de mauvaises pratiques de fabrication, des problèmes de réclamations pour ce que peut faire un produit ou des instructions d'utilisation incorrectes. La lettre précise également que la société doit corriger le problème et fournit des instructions et un délai à la société pour informer la FDA de ses plans en matière de correction. » (7)

Le tableau ci-après présente quelques exemples extraits d'écarts issus de warning letters en lien avec l'intégrités des données de 2015 à 2017 : (8)

TABLEAU II - EXTRAITS D'ECARTS ISSUS DE WARNING LETTERS EN LIEN AVEC L'INTEGRITE DES DONNEES DE 2015 A 2017

Date	Domaine	Pays	Ecart
11/08/17	Production de médicaments	USA	Système qualité n'assure pas l'intégrité des données de la qualité des médicaments
16/05/2016	Production de médicaments	Allemagne	Audit trail : pas suffisamment de contrôles sur l'accès ou les modifications des données
12/05/2016	Fabrication de principes actifs	Chine	Pas suffisamment de contrôle empêchant la manipulation et l'omission des données
03/03/2016	Production de médicaments	Inde	Données d'enregistrements de laboratoire incomplète, inexacte ou falsifiée
02/03/2016	Production de dispositifs médicaux stériles	USA	Validation non documentée
17/12/2015	Production de médicaments	Inde	Manque d'audit trail et pas suffisamment de contrôles sur le système
30/09/2015	Conception de logiciel dispositifs médicaux	USA	Manque de validation
28/09/2015	Fabrication de principes actifs	Inde	Manque de contrôle d'accès (identifiant et mot de passe unique) et données incomplètes
21/09/2015	Production de dispositifs médicaux	USA	Manque de validation

Au total en 2017, plus de 55 warning letters impliquant des manquements à l'intégrité des données ont été émises par la FDA. Il est à noter également que leur nombre n'a cessé d'augmenter depuis ces dernières années comme le présente le graphique ci-dessous :

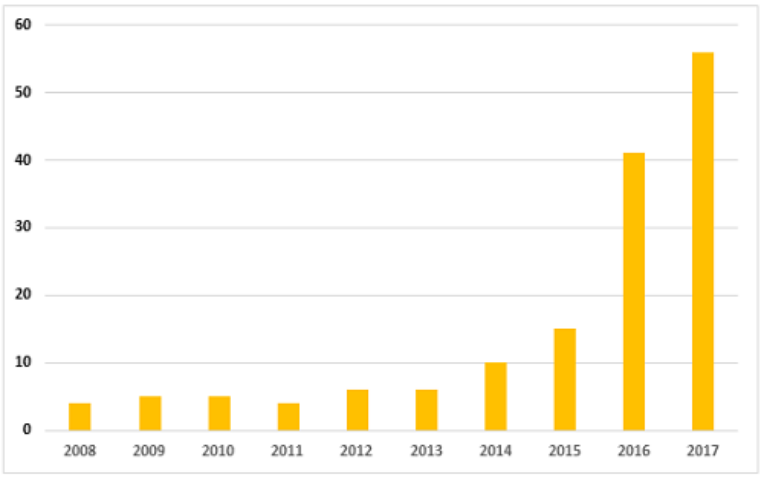

FIGURE 4 - NOMBRE DE WARNING LETTERS IMPLIQUANT UNE PERTE D'INTEGRITE DES DONNEES DEPUIS 2008 JUSQU'A 2017

Si on ne considère que le domaine de la production de médicaments, en 2017, le nombre d'écart en référence à des chapitres du *Code of Federal Régulation* (CFR) part 21 (9) s'est élevé à 34. Il est alors intéressant d'observer la répartition des types d'écarts, présentés dans le tableau ci-après :

TABLEAU III - REPARATITIONS DES ECARTS EN LIEN AVEC LE CFR PART 21 FORMULES A DES ENTREPRISES DE PRODUCTION DE MEDICAMENTS SUR L'ANNEE 2017

Section du CFR part 21 concernée	Titre de la section	Nombre de citations
221.188	Enregistrements de production et de contrôle des lots	9
211.194	Enregistrements de laboratoire	9
211.22	Responsabilités du contrôle qualité	8
211.192	Revue des enregistrements de production	5
211.68	Équipements automatiques, mécaniques et électroniques	3

Soit une répartition en pourcentage des écarts comme suit :

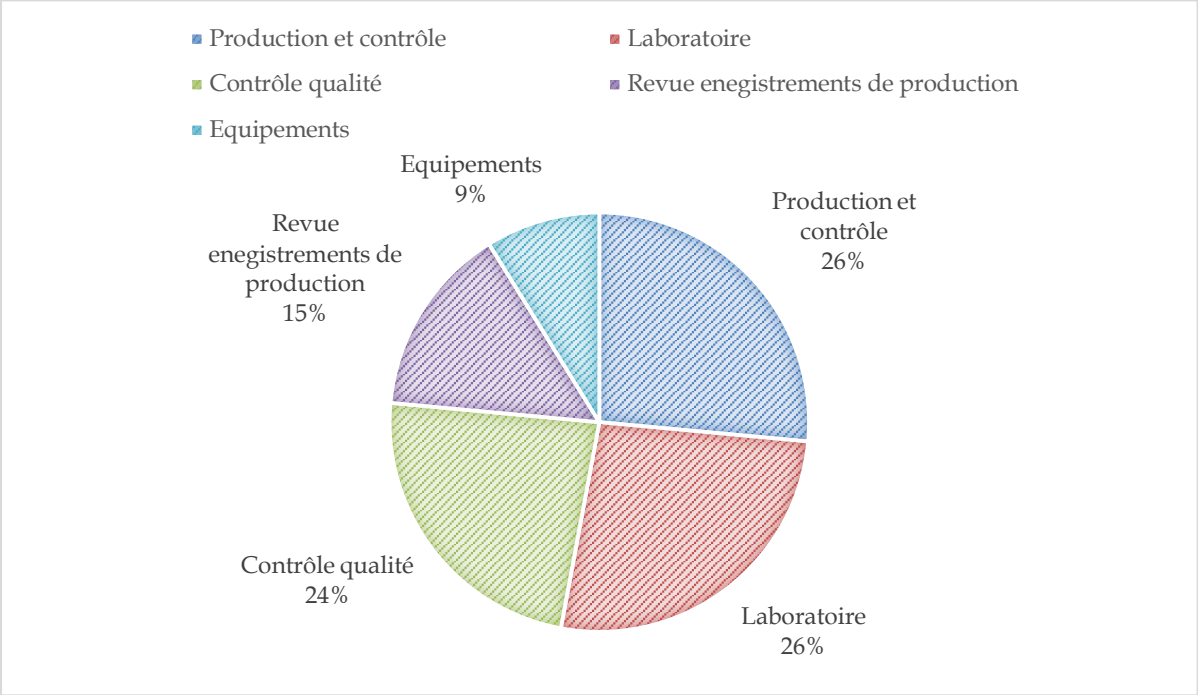

FIGURE 5 - REPARTITION EN POURCENTAGE DES TYPES D'ECARTS EN REFERENCE AU CFR PART 21

On constate dès lors que les écarts les plus nombreux sont ceux en lien avec les « Enregistrements de production et de contrôle des lots », les « Enregistrements de laboratoire » et les « Responsabilités du contrôle qualité ». Ils représentent au total plus de 75% des écarts en lien avec l'intégrité des données formulés en 2017 à des entreprises de production de médicaments.

La part « Revue des enregistrements de production » représente quant à elle 15% des écarts tandis que la part « Équipements automatiques, mécaniques et électroniques » ne représente que 9% des écarts.

Ces données permettent d'affirmer que l'augmentation des infractions liées à une perte d'intégrité des données n'est pas seulement en lien avec l'avènement des nouvelles technologies. De nombreuses exigences, applicables tant aux données au format électronique qu'aux données papier, ne sont pas encore pleinement respectées.

Il est cependant raisonnable de penser que la part associée aux équipements tende à augmenter durant ces prochaines années avec un renforcement des exigences des autorités quant à la maitrise des systèmes informatisés.

3.2 PARALLELE ET DIFFERENCES ENTRE LES BPF ET LES NOTIONS ALCOA

Aucun texte normatif supplémentaire n'a été publié à ce jour par l'Agence française du Médicament car les notions évoquées sont présentes dans le guide des Bonnes Pratiques de Fabrication, qui, rappelons-le, à valeur de loi dans l'industrie pharmaceutique. La notion d'intégrité des données n'est donc pas un élément nouveau tant au niveau français, qu'au niveau international.

Elle a été évoquée pour la première fois dans le guide des BPF de 1989 à travers les exigences suivantes :

- La modification ou la correction des données nécessite la signature, le motif et la possibilité de lire les données d'origine

- Les enregistrements doivent être complétés au moment où l'action est réalisée

- Enregistrement du nom (ou VISA) de la personne qui a effectué et vérifié l'action

Au niveau britannique, on la retrouve aussi dès 1971 dans le UK "Orange Guide" avec les notions suivantes :

- Copies des enregistrements pour éviter les erreurs de transcription

- Initiales des personnes qui effectuent chaque activité

- Enregistrement de l'historique de chaque lot, de l'approvisionnement jusqu'au conditionnement final.

Le Tableau IV ci-après est un comparatif entre les notions principales en matière d'Intégrité des données publiées dans les guides de la MHRA et la FDA et différentes sections des Bonne Pratiques de Fabrication.

TABLEAU IV COMPARATIF DES NOTIONS ALCOA ET DU GUIDE DES BPF

ALCOA	BPF Part I	BPF Part II	Annexe 11
Attribuable	**Documentation** (4.9 / 4.10)	**Equipements de fabrication** (5.43) **Documentation et enregistrements** (6.14 / 6.18 / 6.52)	**Personnel** (2.) **Traçabilité** (9.) **Sécurité** (12.1 / 12.4) **Signature électronique** (14.) **Libération** (15.)
Lisible	**Documentation** (4.7 / 4.9 / 4.10)	**Documentation et enregistrements** (6.11 / 6.14 / 6.15 / 6.50)	**Validation** (4.8) **Stockage** (7.1 / 7.2) **Sorties imprimées** (8.1) **Traçabilité** (9.) **Archivage** (17.)
Contemporaine	**Documentation** (4.8)	**Documentation et enregistrements** (6.14)	**Sécurité** (12.4) **Signature électronique** (14.)
Originale	**Documentation** (4.1 / 4.2)	**Documentation et enregistrements** (6.14)	**Validation** (4.8) **Sorties imprimées** (8.2) **Traçabilité** (9.)
Précise	**Documentation** (4.3) **Validation** (5.26) **Contrôle** (6.15 / 6.16)	**Equipements de fabrication** (5.40 / 5.42 / 5.45 / 5.46 / 5.47) **Documentation et enregistrements** (6.6)	**Validation** (4.8) **Données** (5. / 6.) **Stockage** (7.1 / 7.2) **Maitrise changement** (10.) **Evaluation** (11.) **Archivage** (17.)

Voici quelques extraits des références réglementaires ci-dessus :

- **Attribuable :** (5)

BPF Partie I : « 4.9. Toute correction apportée à un document doit être signée et datée; la correction devant permettre la lecture de la mention originale. »

BPF Partie 2 : « 6.14 Lorsque des données sont enregistrées sur la documentation, […] avec l'identification de la personne qui les a saisies. »

BPF - Annexe 11 : « 14. Signature électronique - Les enregistrements électroniques peuvent être signés électroniquement. Les signatures électroniques doivent :

a- avoir la même valeur, au sein de l'entreprise, qu'une signature manuscrite ;

b- être définitivement liées aux documents auxquels elles se rapportent ;

c- comprendre l'heure et la date de leur application. »

- **Lisible :** (5)

BPF Partie I : « 4.10. […] Des contrôles sécurisés doivent être mis en place – et validés s'il y a lieu – afin de s'assurer de l'intégrité des enregistrements pendant toute leur durée d'archivage. »

BPF Partie 2 : « 6.14 Lorsque des données sont enregistrées sur la documentation, elles doivent l'être de manière indélébile dans des zones prévues à cet effet […]. Les corrections apportées aux données doivent être datées et signées et laisser lisibles les données d'origine. »

BPF - Annexe 11 : « 17. Archivage - Les données peuvent être archivées. L'accessibilité, la lisibilité et l'intégrité de ces données doivent être vérifiées. Si des modifications significatives du système doivent être faites (par exemple, un changement d'équipement informatique ou de logiciel), alors la capacité à récupérer les données archivées doit être garantie et testée. »

- **Contemporaine :** (5)

BPF Partie I : « 4.8. Les enregistrements doivent être effectués ou finalisés au moment où chaque action est réalisée, de telle sorte que toutes les opérations significatives concernant la fabrication des médicaments puissent être tracées. »

BPF Partie 2 : « 6.14 Lorsque des données sont enregistrées sur la documentation, elles doivent l'être de manière indélébile dans des zones prévues à cet effet, immédiatement après avoir réalisé les activités correspondantes […] »

BPF - Annexe 11 : « 12.4. Les systèmes de gestion des données et des documents doivent être conçus pour enregistrer l'identité des utilisateurs impliqués dans la saisie, la modification, la confirmation ou la suppression de données, y compris la date et l'heure. »

- **Originale :** (5)

BPF Partie I : « 4.1. […] Les interactions et les mesures de contrôle doivent être définies pour les documents maîtres, les copies officielles, la manipulation des données et les enregistrements, que ce soit pour des systèmes hybrides ou homogènes. Des contrôles appropriés pour les documents électroniques, tels que des modèles, des formulaires, et les documents maîtres, doivent être mis en œuvre. »

BPF Partie 2 : « 6.14 […]. Les corrections apportées aux données doivent être datées et signées et laisser lisibles les données d'origine. »

BPF - Annexe 11 : « 8.2. Concernant les données nécessaires à la libération des lots, les impressions générées doivent pouvoir indiquer si l'une ou plusieurs d'entre elles ont été modifiées depuis leur saisie initiale. »

- **Précise :** (5)

BPF Partie I : « 4.3. Les documents contenant des instructions doivent être approuvés, signés et datés par les personnes appropriées et autorisées. Le contenu des documents ne doit pas être ambigu et doit être identifiable de façon unique. La date de prise d'effet doit être définie. »

BPF Partie 2 : « 6.60 Les enregistrements des contrôles de laboratoire doivent contenir toutes les données issues de tous les contrôles réalisés pour s'assurer de la conformité aux spécifications et aux normes, y compris les examens et les dosages »

BPF - Annexe 11 : « 5. Données - Les systèmes informatisés qui échangent des données électroniques avec d'autres systèmes doivent disposer de contrôles intégrés garantissant la sécurité et l'exactitude des entrées et des traitements des données et ce, afin de minimiser les risques. »

Les notions décrites par les différentes agences en matière d'intégrité de données sont sensiblement les mêmes.

Quelques différences sont à noter. La première est que du côté français, les informations sont disséminées au fil du guide des Bonnes Pratiques de Fabrication tandis que les guides spécifiques regroupent les notions essentielles en les illustrant de

différents exemples concrets qui aident les industriels à saisir toutes les facettes et l'intérêt du *Data Integrity* et à appliquer les mesures de gestions nécessaires.

La seconde différence réside en la spécificité imposée par les guides relatifs au *Data Integrity*. En effet, les guides fournis par la MHRA, la FDA et l'OMS considèrent cette notion comme un élément à part entière. Par exemple, il est indiqué qu'une formation sur l'intégrité des données doit être promulguée aux employés tandis que selon le guide des BPF « le fabricant doit assurer la formation de tout le personnel » sans établir de formation spécifique sur l'intégrité des données.

Enfin, les guides publiés au sujet du Data Integrity favorisent et préconisent l'utilisation de systèmes entièrement informatisés ainsi que le recours aux signatures électroniques. Il est à maintes reprises mentionné que l'utilisation de système hybrides comme l'impression et la signature manuelle de documents informatiques est tolérée mais non idéale. Le recours aux systèmes entièrement informatisés n'est ni préconisé, ni dénoncé par l'ANSM.

La notion d'intégrité des données n'est donc pas un concept nouveau mais elle a connu, conjointement avec l'avènement des nouvelles technologies, un essor qui, selon les pays, a pris différentes formes dans la présentation et l'explication qui en a été donnée.

4 CYCLE DE VIE D'UNE DONNEE

Le cycle de vie d'une donnée représente toutes les phases de la vie d'une donnée, depuis sa création et sa collecte jusqu'à son archivage en vue d'une éventuelle réutilisation comme le présente la Figure 6. (10)

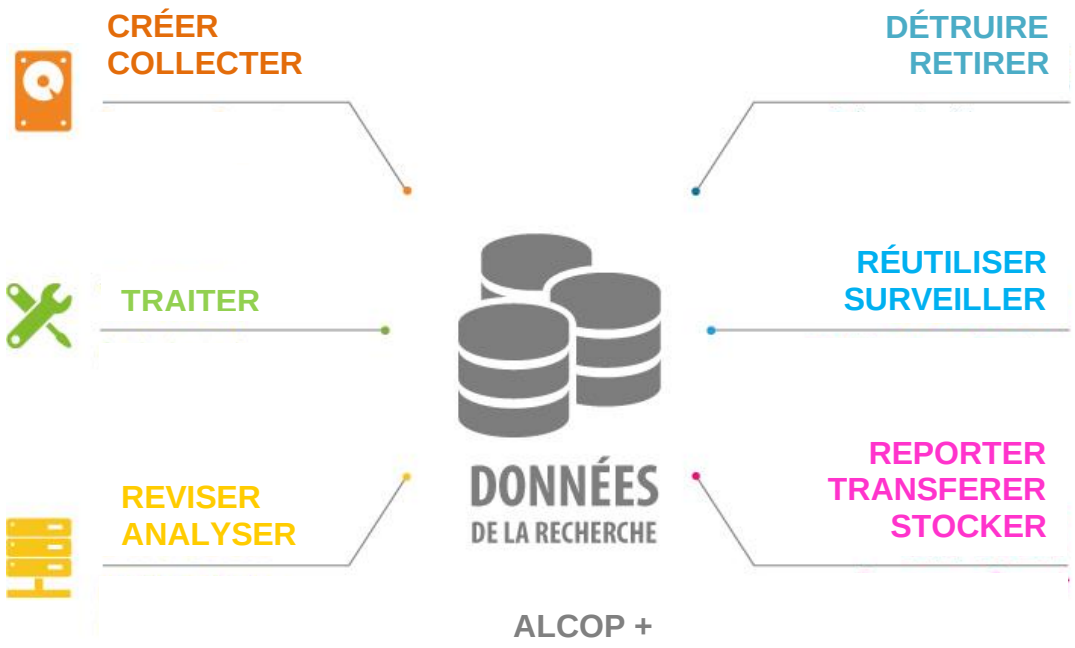

FIGURE 6 - CYCLE DE VIE D'UNE DONNEE

Durant la période où une donnée doit être conservée, il est à noter que sa réutilisation équivaut à une nouvelle collecte. En ce sens, aucune perte d'information ne doit survenir lors de l'archivage de cette dernière et le format originel doit être conservé afin de préserver le caractère dynamique et l'exploitabilité de la donnée.

4.1 ENREGISTREMENT

4.1.1 FORMAT DES DONNEES

Il est tout d'abord primordial de rappeler, que les exigences en matière d'intégrité des données, s'appliquent aux données générées manuellement (format papier), mais aussi aux données informatiques.

La méthode d'enregistrement sélectionnée (manuelle ou non) devra garantir l'exactitude, la complétude et la représentativité des données.

Il est concevable que certaines données générées par informatique soient enregistrées sous format papier ou PDF, sous réserve de justifier que l'aspect statique de celles-ci ne remette pas en cause l'intégrité de la donnée originale. Cependant, lorsque les systèmes informatiques permettent un enregistrement dynamique des données, il n'est pas permis de préférer un enregistrement statique.

4.1.2 INCLUSION / EXCLUSION DES DONNEES

Certaines données peuvent être exclues lorsqu'il peut être démontré de façon scientifique qu'il s'agit d'une donnée anormale ou non représentative. Dans tous les cas, une justification documentée sera exigée et cette exclusion sera prise en compte lors de l'étude des données. Toutes les données (même celles exclues) doivent être gardées avec l'ensemble des données collectées.

4.1.3 ENREGISTREMENT MANUEL

C'est la personne qui a réalisé l'action qui doit l'enregistrer, l'utilisation d'un scribe pour une autre personne ne peut être qu'exceptionnelle et ne peut avoir lieu que dans deux cas :

- Si le fait d'enregistrer la donnée au moment de l'action peut compromettre le produit fini ou l'action en cours

Exemple : tâche effectuée en zone stérile et enregistrée en zone non stérile.

- Pour concilier une limitation liée à la langue

Exemple : activité effectuée par un opérateur mais vérifiée et enregistrée par son supérieur.

Dans les deux cas, l'enregistrement doit être fait au moment de l'action et doit identifier tous les acteurs : la personne effectuant la tâche et celle qui l'enregistre. Lors d'une saisie manuelle des données, ce lien se fera au moyen d'un visa ou tout autre élément pouvant identifier la personne.

4.1.4 ENREGISTREMENT ELECTRONIQUE

Les contrôles d'accès doivent être pleinement utilisés. Ils se présentent sous la forme de sessions (logins) individuelles et de mots de passe personnels.

Ils permettent de s'assurer que les employés n'ont accès qu'aux fonctionnalités des systèmes informatiques propres à leur rôle et que les données saisies ou les actions réalisées sont reliées à un individu spécifique. L'entreprise doit être en mesure de montrer le niveau d'accès (fonctionnalités accessibles) accordé à chaque employé et d'assurer la disponibilité d'un historique des niveaux d'accès utilisateurs.

Le partage d'identifiants ou les identifiants dits « génériques », c'est-à-dire connus et utilisés par tous les employés ne doivent pas être utilisés. Lorsque les systèmes informatiques supportent les accès individuels, ils doivent être utilisés.

Certains systèmes peuvent nécessiter l'achat d'une licence supplémentaire. D'autres systèmes en revanche, ne peuvent supporter aucun accès utilisateur ou un nombre réduit de sessions. Dans ce cas, des contrôles alternatifs peuvent être fournis par des logiciels tiers ou par traçabilité papier. La pertinence de systèmes alternatifs doit être justifiée et documentée.

Le cas d'une traçabilité papier, c'est-à-dire le recours à un système hybride est actuellement permis lorsque l'équivalence à un système informatisé est démontrée. Cependant, si une telle équivalence ne peut être démontrée, il est attendu que l'entreprise ait fait évoluer cette méthode vers un système informatisé depuis fin 2017.

4.1.5 DROITS D'ACCES ET ADMINISTRATION

A chaque personne ou groupe de personnes seront attribuées certaines possibilités d'interaction avec le système et les données qui s'y rapportent, on parle alors de droit ou de privilèges utilisateurs. L'attribution de ces droits d'accès est réalisée par un ou plusieurs administrateurs. (11)

Un administrateur est garant de l'accès au système d'information et de sa sécurité, il prévient les anomalies éventuelles, participe au développement et à la maintenance des applications informatiques. Il intervient également pour rétablir le service en cas de problème. Les tâches d'administration sont une composante indissociable du cycle de vie du système d'information. Elles se traduisent par un ensemble de processus et de mesures techniques et non techniques visant à assurer le maintien en condition opérationnelle et de sécurité du système.

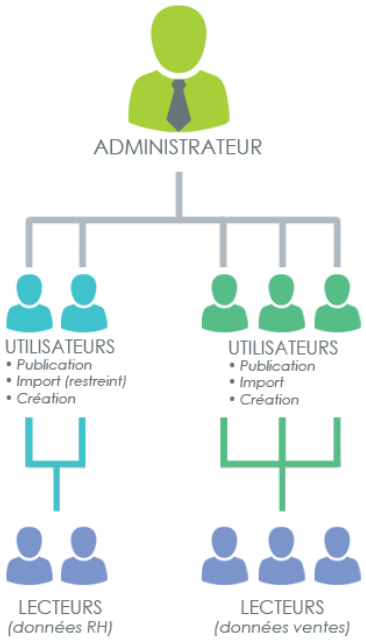

FIGURE 7 SCHEMA DROITS D'ACCES

Les utilisateurs ayant des droits administrateurs doivent s'enregistrer avec un identifiant unique, qui permettra d'attribuer des fonctions (suppression, modifications de données) à des groupes d'utilisateurs comme le schématise la figure ci-dessus. Les utilisateurs qui ne possèdent pas de droit permettant une interaction avec le système sont appelé lecteurs.

Exemple : Droits d'accès sur un système d'édition et d'impression d'étiquettes de caisses américaines en zone de conditionnement.

FIGURE 8 DROITS D'ACCES D'UN SYSTEME D'EDITION ET D'IMPRESSION D'ETIQUETTES

Dans cet exemple, l'administrateur établit des profils d'utilisateurs ayant des droits d'accès et d'interaction avec le système. Les Chefs d'équipes, habilités et formés à la gestion du système auront la possibilité notamment, via des sessions individuelles, de créer des masques et d'imprimer les étiquettes pour les équipes de production. Un autre groupe d'utilisateurs est celui des conducteurs de lignes qui, eux, ne pourront pas influencer les données mais n'auront qu'un droit de lecture, c'est-à-dire de consultation des étiquettes créées.

Les accès administrateurs systèmes doivent êtres restreints à un nombre minimum de personnes possible, en prenant en compte la taille et la nature de l'entreprise. Les droits administrateurs génériques, c'est-à-dire les droits non rattachés à une personne, ne doivent pas être utilisés.

Par ailleurs, ces accès ne doivent pas être attribués à des personnes ayant un lien direct avec les données, ceci afin d'éviter tout risque de correction dissimulée :

- Personnes générant les données
- Personnes effectuant un suivi des données
- Personnes en charge de l'approbation des données

Un processus organisationnel et technique de gestion des comptes d'administration et des privilèges associés doit être mis en œuvre tout au long du cycle de vie des données.

Ce processus de gestion doit intégrer une procédure de contrôle et de révision régulière de ces comptes et des autorisations d'accès aux ressources d'administration. Les droits d'administration des postes doivent être strictement réservés aux personnes en charge de leur configuration et uniquement utilisés pour des tâches qui s'y rapportent.

Enfin, toutes les modifications effectuées sous un statut d'administrateur système doivent être enregistrées, visibles et approuvées par le système qualité de l'entreprise.

4.1.6 SIGNATURE ELECTRONIQUE

Selon cette directive, on entend par signature électronique, « une donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification ».

La signature électronique doit donc être unique et remplir les critères suivants :

- Prouver irrévocablement l'identité de l'auteur du document
- Contrer la falsification et figer le document dans le temps

La cryptographie n'est cependant pas née avec l'avènement du numérique. Le cryptage ou chiffrement relève de la cryptographie, terme dérivé du grec *kryptos*, signifiant caché ou secret. En 700 avant Jésus-Christ., les Spartiates écrivaient des messages secrets sur des bandes de cuir enroulées autour de bâtons de bois. La suite de caractères sur la bandelette déroulée n'avait aucun sens, mais lorsqu'elle était enroulée autour d'un bâton de même diamètre, le destinataire pouvait déchiffrer le message.

Le principe des signatures électroniques est celui de la cryptographie asymétrique aussi appelée cryptographie à clef publique, c'est-à-dire que la clef qui sert au cryptage n'est pas la même que celle utilisée pour le décryptage mais elles sont reliées entre elles par une logique mathématique. Nous allons nous intéresser à cette méthode de cryptographie asymétrique, schématisée sur la Figure 9, afin de comprendre son fonctionnement et la sécurisation qu'elle apporte aux données.

En premier lieu, le document est crypté selon un algorithme particulier : la *hash function* (fonction de hachage). Ce processus génère un texte chiffré, ou cryptogramme, qui ne peut être affiché dans sa forme d'origine que s'il est déchiffré à l'aide de la bonne clé.

Ce même document est ensuite crypté selon une clef unique privée qui ne peut appartenir qu'à une seule personne (ou organisme). Un certificat numérique est alors associé : il s'agit d'un document numérique permettant de valider le lien entre une signature électronique et son signataire.

Lors de la vérification, le document est décrypté en utilisant, d'une part l'algorithme particulier, la *hash function* et d'autre part la clef publique liée à la clef privée utilisée pour chiffrer le document.

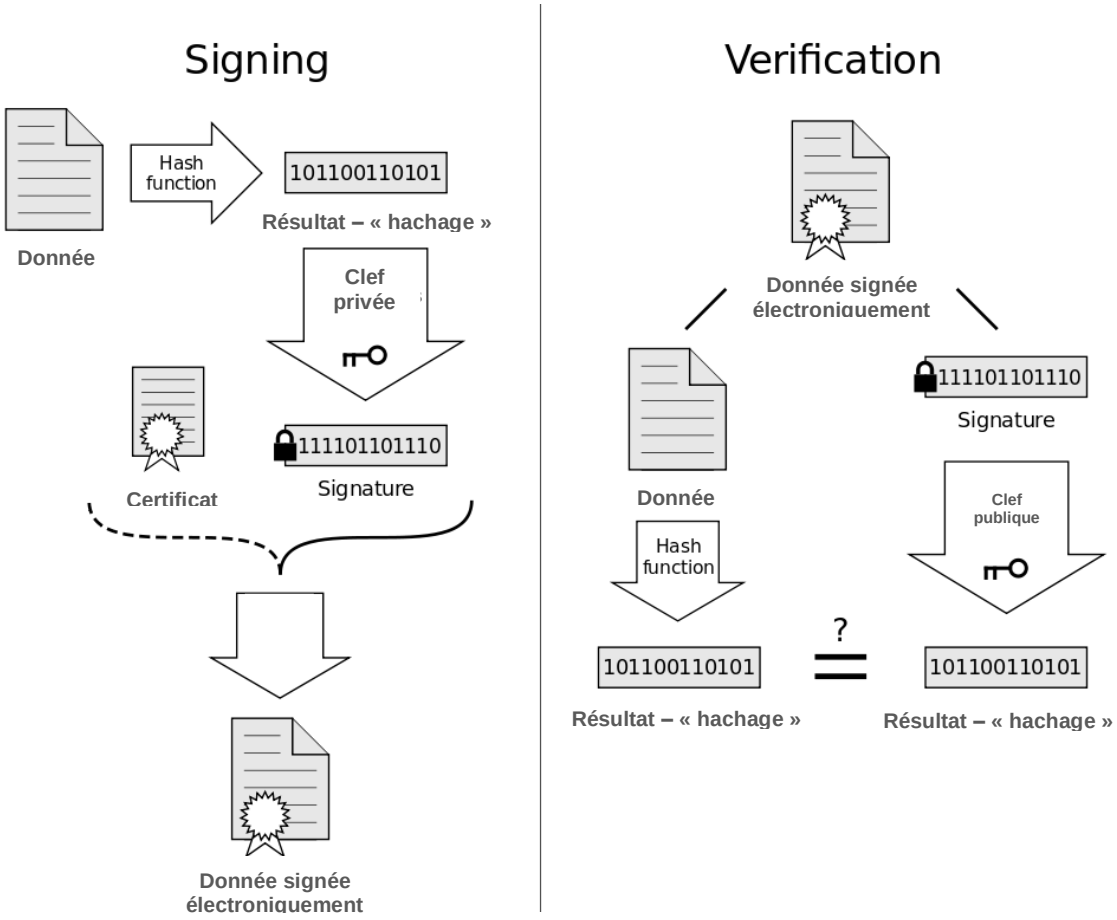

FIGURE 9 SCHEMA DU MECANISME DE CRYPTAGE ET DE DECRYPTAGE D'UNE SIGNATURE ELECTRONIQUE

On obtient pour chaque méthode de décryptage, *hash function* et clef publique, une série numérique de 0 et 1 et que l'on nomme *Hash* ou hachage. Si les deux séries numériques issues du décryptage sont identiques, nous sommes en présence d'un document valide.

La méthode de cryptage décrite précédemment est permise au moyen de logiciels ou matériels configurés utilisant des fonctions et clefs cryptographiques propres spécifiques. Le signataire, détenteur du dispositif de création, utilise ces codes ou clefs pour créer la signature électronique.

La signature ainsi générée et liée à des données est vérifiée au moyen de dispositifs de vérification de signature. Tout comme les dispositifs de création, il s'agit de logiciels ou matériels configurés qui utilisent des fonctions et des clefs de décryptage pour authentifier la signature. Si la signature est vérifiée, un certificat, sous forme d'attestation électronique, est délivré et confirme l'identité de la personne.

Lorsqu'un document papier ou une copie pdf d'un document comportant une signature électronique est créé, la métadonnée associée à la signature doit être maintenue dans le document.

Comme l'explicite la Figure 10, la signature électronique accomplit de façon plus sécurisée ce que la signature manuscrite exécute depuis longtemps. Un document physique papier devient électronique et immatériel, le stylo est remplacé par un logiciel de cryptage et l'équivalence de spécificité du geste de la signature est assurée par un code secret inclus dans le logiciel et personnel à chaque utilisateur.

FIGURE 10 SCHEMA ILLUSTRANT LE PARALLELE ENTRE LA SIGNATURE ELECTRONIQUE ET LA SIGNATURE MANUSCRITE

L'insertion d'une image d'une signature scannée comme présenté sur la Figure 11 ou une note en bas de page ne constitue pas une signature électronique.

FIGURE 11 EXEMPLE DE SIGNATURE MANUSCRITE SCANNEE

L'utilisation de signatures électroniques doit être conforme aux exigences de standards internationaux tels que la directive 1999/93/EC. Ces exigences sont détaillées dans l'extrait de la directive 1999/93/CE en Annexe I. Il y est décrit point par point toutes les caractéristiques et informations que doivent posséder :

- Les certificats qualifiés
- Les prestataires de services fournissant les certificats dont une liste doit être définie et tenue à jour par chaque état membre de l'Union Européenne (12)
- Les outils et supports de créations de signatures électroniques sécurisées
- Les méthodes de vérification des signatures

4.2 TRAITEMENT

Les transferts et migrations de données doivent être conçus et validés pour assurer que les principes d'intégrité de données soient respectés. Il doit y avoir une traçabilité de toutes les sessions utilisateurs utilisées dans les différentes activités de traitement de données.

Les systèmes informatiques doivent êtres configurés de manière à ce que les paramètres critiques soient enregistrés en temps réel par l'utilisateur. Une étape critique peut être par exemple un paramètre qui doit se situer en dessous d'une certaine limite ou dans une certaine gamme pour assurer la qualité du produit fini.

Enfin, une donnée peut être enregistrée en tant que « vraie copie », c'est-à-dire une copie de l'information originale. L'exactitude (représentative et complète) de cette copie devra être vérifiée.

Une copie vraie peut être générée dans un format différent de celui d'origine mais il faudra, autant que possible, garder l'équivalence de la nature dynamique ou statique de la donnée.

4.3 CONTROLE

4.3.1 AUDIT TRAIL

Un « audit trail », traduit littéralement par piste d'audit, est un enregistrement des informations critiques, comme par exemple la modification ou la suppression d'une donnée, qui permet la reconstruction des activités.

Lorsque des systèmes informatiques sont employés pour enregistrer, traiter et archiver les données, ils doivent êtres configurés pour pouvoir fournir une trace de toutes les actions effectuées sur ces données. Il doit également être possible d'associer toutes ces actions aux personnes qui les ont réalisées. Tout changement doit être horodaté et justifié. Les éléments inclus dans l'*audit trail* sont ceux qui permettent la reconstruction chronologique du procédé ou des activités. (13)

L'*audit trail* doit être en permanence activé. Les utilisateurs, à l'exception des administrateurs systèmes, ne doivent pas être en mesure d'inactiver l'audit trail.

La pertinence des données incluses dans un audit trail est fonction de sa capacité à fournir un contrôle robuste des données. Il n'est pas nécessaire d'intégrer toutes les activités système. Les frappes clavier et ouverture/fermeture session pourront en être exclues.

Lorsqu'il n'est pas possible d'obtenir de telles fonctionnalités, il est permis d'utiliser un *audit trail* sous format papier pour tracer les changements effectués sur les données. Ces systèmes hybrides sont actuellement autorisés lorsque l'équivalence à un *audit trail* intégré informatisé est démontrée. Cependant, si une telle équivalence ne peut être démontrée, il est attendu que l'entreprise ait fait évoluer ce système vers un système informatisé depuis fin 2017. (14)

4.3.2 CONTROLE DES DONNEES

L'entreprise doit posséder une procédure qui décrit le procédé de contrôle et de validation des données. Le contrôle des données doit également inclure les métadonnées pertinentes et les *audits trail*.

Ces contrôles doivent être réalisés sur les données originales ou sur de vraies copies. Lorsque le contrôle n'est pas mené par l'entreprise qui a généré la donnée, les responsabilités respectives doivent être documentées et approuvées par les deux parties.

Enfin, la procédure de contrôle doit décrire les mesures à prendre en cas de détection d'une erreur ou d'une omission. Elle doit notamment permettre d'effectuer des corrections ou clarifications de données en accord avec les Bonnes Pratiques, utilisant le principe ALCOA+.

4.4 STOCKAGE / ARCHIVAGE / DESTRUCTION

La sauvegarde des données peut se faire soit à l'aide de sauvegardes soit sous forme d'archives.

L'objectif de la sauvegarde ou *backup* est la récupération des données en cas d'événement rendant celles-ci inaccessibles : perte ou endommagement. La sauvegarde s'applique aussi bien aux données dynamiques qu'aux données statiques. Elle est une copie de l'information en cours d'utilisation. En d'autres termes, si la sauvegarde est perdue, l'entreprise n'est pas impactée car elle conserve ses données actives.

L'archivage, quant à lui, a pour finalité de préserver les données anciennes ou dormantes sur une longue durée. L'archivage a pour but de stocker sur le long terme un volume important d'informations.

Les modalités de sauvegarde des données ou des documents devront garantir la protection des enregistrements contre d'éventuelles altérations ou pertes, qu'elles soient intentionnelles ou non. Des contrôles de sécurité doivent êtres en place pour assurer l'intégrité des données tout au long de la période de sauvegarde.

Exemple : des données générées sous format papier peuvent être sauvegardées par scan.

Les archives peuvent être constituées des données originales ou de vraies copies et doivent être protégées de façon à ce qu'elles ne puissent pas être altérées ou supprimées sans détection.

Par ailleurs, les données (et métadonnées) archivées doivent demeurer lisibles durant toute la période de stockage. Dans le cas d'archivage de données électroniques, ce procédé devra être validé et vérifié périodiquement pour les données légales.

Les données doivent être accessibles à tout moment sur demande des autorités compétentes.

Enfin, les procédures de destruction doivent tenir compte de la criticité des données et des exigences législatives en vigueur. Il est donc primordial de définir le temps de rétention nécessaire pour chaque donnée, qu'il s'agisse d'une période légale ou nécessaire au bon fonctionnement de l'entreprise.

5 CONCLUSION DE LA PREMIERE PARTIE

Pour qu'une décision soit robuste, l'intégrité des données qui la supportent doit être garantie. Quelle confiance peut-on accorder à une décision Qualité prise sur la base de données erronées ?

Il est alors fondamental que le système Qualité d'une entreprise puisse permettre l'identification et la mise sous contrôle des points de vulnérabilité des données critiques, que ces données soient électroniques ou enregistrées sur un support papier.

La gestion de l'intégrité des données correspond à l'ensemble des dispositions qui visent à garantir que les données, quel que soit le format dans lequel elles sont générées, sont enregistrées, traitées, conservées et exploitées de façon à garantir un enregistrement complet, cohérent et exact tout au long de leur cycle de vie. Elle fait partie intégrante du système qualité pharmaceutique.

PARTIE 2 : ANALYSES DE RISQUE DATA INTEGRITY ASSOCIEES AUX EQUIPEMENTS ET AUX DONNEES

6 SCOPE ET DEFINITIONS

Le degré de vulnérabilité d'une donnée, en regard d'une modification non contrôlée (volontaire ou non), est évalué au travers d'une analyse de risques. Afin de pouvoir gérer ses données et assurer leur intégrité, l'entreprise doit procéder à une évaluation de celles-ci en effectuant une analyse des risques qui doit tenir compte de la vulnérabilité des données, des systèmes informatisés mais également des processus.

A l'issue de cette analyse, l'entreprise sera en capacité de mettre en place des mesures afin d'assurer l'intégrité des données qu'elle génère ou exploite. Parmi ces mesures, on trouve la qualification des équipements et la validation des systèmes. La réalisation d'une analyse de risques permettra donc à l'entreprise de cibler ses faiblesses en termes de Data Management mais également d'évaluer si oui ou non certains équipements ou systèmes nécessitent d'être qualifiés ou validés.

Les facteurs à prendre en compte pour cette analyse peuvent être la complexité du processus analysé, son degré d'automatisation ou la subjectivité de l'interprétation des résultats. L'évaluation est réalisée en regard de tout le processus (ou système) exploitant cette donnée, et non pas seulement sur des fonctionnalités ou technologies informatiques. Il convient donc d'analyser, d'une part, l'équipement mais également le système dans son ensemble.

La validation des systèmes informatisés, si elle est toujours nécessaire, n'est plus suffisante aujourd'hui pour garantir une maitrise des risques sur l'intégrité des données. L'évaluation doit être réalisée en prenant en considération l'aspect matériel et technologique mais également le système qui entoure la donnée : documentation, procédures, utilisateurs, contexte... C'est ici que réside la principale évolution de l'approche Data Integrity, l'avènement du Data Management (Gestion des données).

6.1 ANALYSES DE RISQUES

6.1.1 RISQUE

Il convient dans un premier temps de définir la notion de risque. Le risque est défini dans le dictionnaire Larousse comme étant « la possibilité, probabilité d'un fait, d'un événement considéré comme un mal ou un dommage ».

Cette seule définition ne suffit néanmoins pas à définir le risque dans un contexte industriel. Le terme « risque » apparait 590 fois dans les BPF et est défini en ces termes : « combinaison de la probabilité d'apparition d'un dommage et de sa gravité » (définition elle-même issue du Guide ISO - International Organization for Standardization /IEC – International Electrotechnical Commission 51).

La norme ISO 9001 version 2015 quant à elle, donne une définition plus générale du risque, il s'agit de « l'effet de l'incertitude sur un résultat escompté ».

6.1.2 MANAGEMENT DES RISQUES

Le management des risques consiste à évaluer le risque en entreprise et à développer diverses stratégies afin de le garder sous contrôle (transfert du risque, évitement, réduction des effets, acceptation des conséquences, etc.). Apparu aux États-Unis dans les années 1960, ce concept a évolué à la fin du XXe siècle avec différentes périodes dans son approche stratégique : de la simple gestion des sinistres marquant la fin des années 1980, en passant par une gestion globale des assurances, avec mise en place de mesures de prévention et développement des plans de gestion de crise industrielle.

La fin des années 1990 voit ainsi l'apparition des notions de gestion des risques associées au développement d'outils comme la cartographie des risques. Cette dernière a pour objectif d'identifier, d'évaluer, de quantifier les risques, mais aussi de définir les mesures, comme les plans de contrôle qui permettront de les réduire voire de les éliminer. Le management des risques favorise la sécurité, établit des plans de gestion de crise en renforçant l'efficacité des organisations et des systèmes de gestion, y compris celle des nouvelles technologies. (15)

Les principes de gestion des risques sont utilisés efficacement dans de nombreux domaines d'activité : gouvernement, y compris les finances, les assurances, la sécurité au travail, la santé publique, pharmacovigilance, et par les agences réglementant ces industries.

L'approche basée sur les risques est en outre au cœur de la dernière version de la norme ISO 13485-2016 « Dispositifs médicaux -- Systèmes de management de la qualité -- Exigences à des fins réglementaires ». Il s'agit non plus là d'un outil de mesure mais d'une opportunité d'identifier les risques pesant sur les activités de l'entreprise et d'y répondre de façon proportionnée et efficace. Cette approche est plus générale que la gestion des risques au sens ISO 14971, l'objectif n'est pas uniquement la sécurité du patient mais aussi la conformité du système de management de la qualité, le respect des exigences règlementaires et de toute autre source pertinente, par exemple le risque financier de l'entreprise ou le risque vis-à-vis de l'image client.

Enfin, selon le chapitre 5 des BFP « Les systèmes informatisés concernés par les BPF doivent être validés. L'importance et l'étendue de la validation dépendent de la diversité, de la complexité et de la criticité de l'application informatique. » (5). Une approche basée sur les risques associés au système doit donc être mise en place.

En fonction des résultats de l'analyse de risque, seront appliquées aux systèmes les différentes phases de qualification afin d'apporter la preuve que les matériels et les logiciels sont adaptés à la réalisation des travaux qui leurs sont demandés.

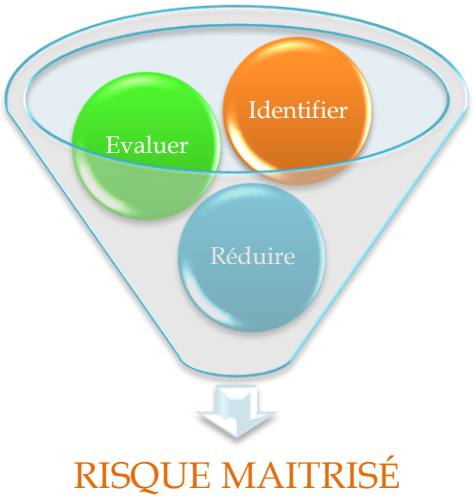

FIGURE 12 - COMPOSANTES DU MANAGEMENT DES RISQUES

En résumé, le management des risques se compose en trois phases :

- L'identification des risques : quels équipements / procédés feront partie de mon analyse et quels risques vais-je identifier ?
- L'évaluation des risques : quelle est la probabilité de survenue et l'impact de tels risques ?
- La réduction : que dois-je mettre en place pour réduire les risques identifiés ? Qualification du système informatique / validation du système informatisé ?

La méthodologie proposée consiste dans un premier temps à réaliser l'analyse des risques associés aux équipements informatiques et de déterminer la nécessité d'une qualification de ces équipements. Dans un second temps, c'est le système informatisé incluant le système informatique et son environnement qui seront analysés afin de déterminer la nécessité de mise en place d'une validation du système.

6.2 SYSTEME

Un système est défini selon les BPF comme étant « un ensemble structuré d'opérations et de techniques interactives qui sont réunies pour former un tout organisé ». Dans la littérature conventionnelle il est défini comme un « ensemble d'éléments considérés dans leurs relations à l'intérieur d'un tout fonctionnant de manière unitaire ». Le point commun entre ces deux définitions réside dans la notion d'interconnexion d'éléments individuels formant ainsi une unité à part entière.

Prenons l'exemple du système circulatoire sanguin. Il s'agit là d'un ensemble de vaisseaux et organes tels que le cœur, l'aorte, les différentes veines et artères, interconnectés formant un système organisé.

6.3 SYSTEME INFORMATIQUE

Depuis la fin des années 50, plusieurs scientifiques tentaient d'imaginer un mot pour désigner les activités liées aux ordinateurs : *Computronik*, *Informatik*, sans succès. Ce n'est qu'en 1962 que le mot « Informatique » a vu le jour, créé par Philippe Dreyfus. Il s'agit d'un néologisme de la langue française issu de la contraction des mots « automatique » et « information ». (16)

Le terme informatique peut être défini comme étant la « science du traitement rationnel, notamment par machines automatiques, de l'information ». (16) Un système informatique peut donc être défini comme un ensemble d'éléments interconnectés dont la fonction finale serait le traitement des informations.

Un système informatique peut se décomposer en deux sous-ensembles :

La partie « logiciel »

- *Software* : il s'agit de la partie invisible et « intelligente » du système. Il s'agit d'un ensemble de programmes qui sont exécutables, c'est-à-dire compris par la machine et qui servent à la faire fonctionner.

ET/OU

- *Firmware* : appelé couramment micrologiciel, est un programme logiciel ou un ensemble d'instructions programmées directement sur un périphérique matériel. Le micrologiciel est généralement stocké dans la ROM (Read Only Memory, mémoire qui ne permet que la lecture des informations qu'elle contient) d'un périphérique matériel.

La partie « matériel », le *hardware* : il s'agit des éléments matériels qui composent une machine informatique. Il peut s'agir de matériel interne comme des pièces détachées montées sur des circuits imprimés (processeur, carte son, disque dur...) ou de matériel externe (imprimante, écran d'affichage,...)

6.4 SYSTEME INFORMATISE

Selon les BPF, un système informatisé correspond à un « système comprenant la saisie de données, le traitement électronique et la sortie d'informations destinées à être utilisées à des fins soit de rapport, soit de contrôle automatique » mais cette seule définition ne suffit pas à comprendre ce qu'est un système informatisé car elle le considère comme un système informatique. (17)

Un système informatisé peut être décrit comme étant l'association d'un système informatique ou automatisé et du processus contrôlé par ce dernier.

Le processus quant à lui est composé des équipements de support qui n'entrent pas dans la catégorie *hardware* du système informatique ainsi que des procédures opérationnelles et du personnel qui utilise le système.

La Figure 13 ci-après identifie les différents composants d'un système informatique.

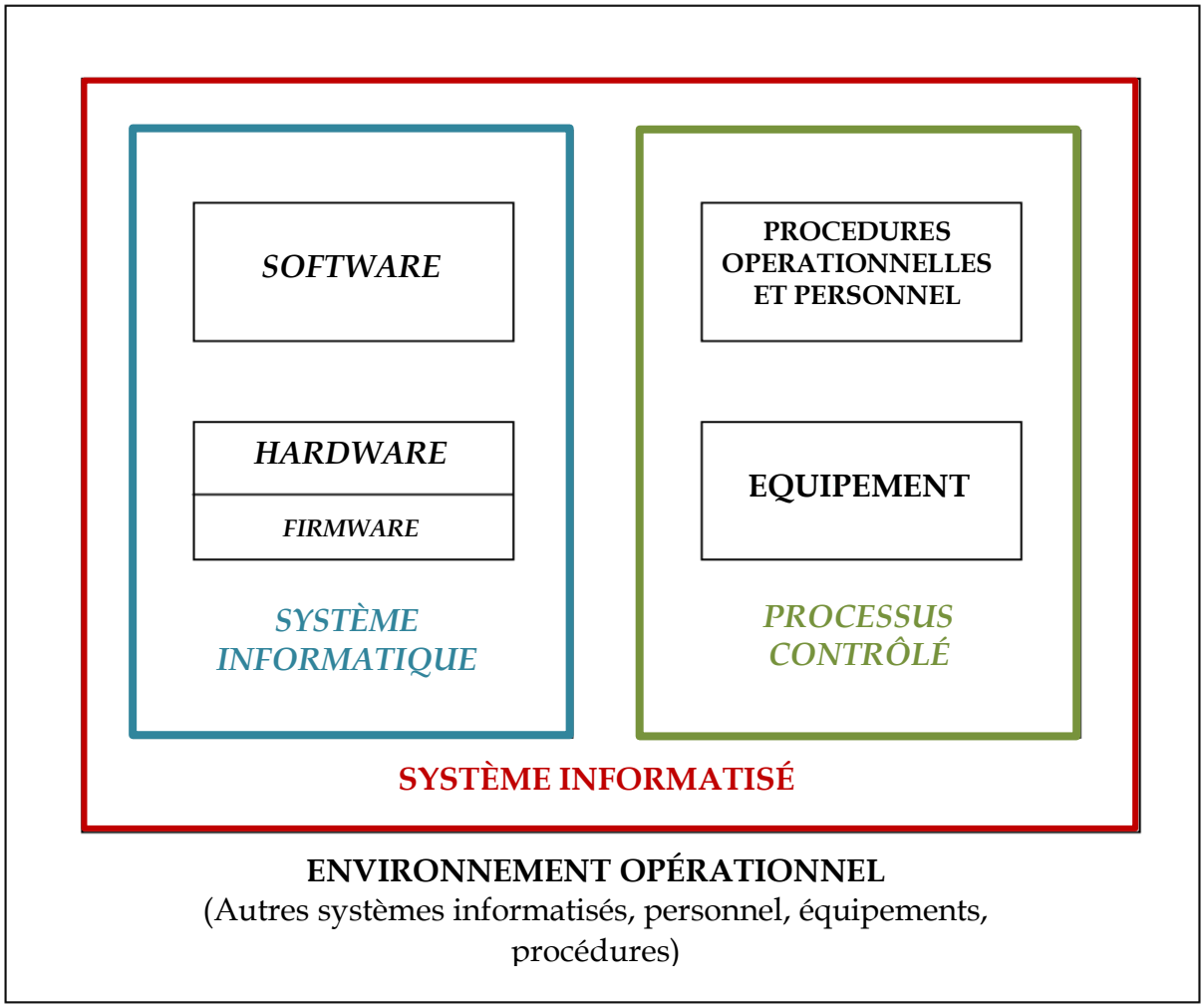

FIGURE 13 SYSTEME INFORMATISE ET ENVIRONNEMENT OPERATIONNEL - PIC/S

Exemple : Cas d'un système de Chromatographie Liquide Haute Performance présenté sur la Figure 14.

Le système informatique sera représenté par l'ordinateur servant à l'acquisition des données. Il est composé d'un *software*. On y trouve notamment un système d'exploitation, c'est-à-dire un logiciel qui « discute » directement avec les composants et sert à faire fonctionner le système. Parmi les plus connus on trouve GNU/Linux, Microsoft Windows, MacOS (Operating System). Dans la sous-unité software on trouve également des logiciels annexes exerçant chacun une fonction spécifique, notamment un logiciel d'acquisition et de gestion des données chromatographiques type Empower, Azur, Clarity, etc.

Il est intéressant d'observer le côté *hardware* de ce système : doit-on considérer le détecteur un matériel externe faisant partie intégrante du système informatique ? Dans cet exemple non ; ne seront considérés comme *hardware* que les composants matériels servant à faire fonctionner le système informatique.

Enfin, le processus contrôlé se compose de procédures d'utilisation du chromatographe ainsi que de méthodes utilisateurs et du personnel habilité à réaliser

les mesures. L'équipement sera représenté par le chromatographe, il s'agit de la partie du système informatisé qui réalise la tâche ou l'action, ici l'analyse de l'échantillon.

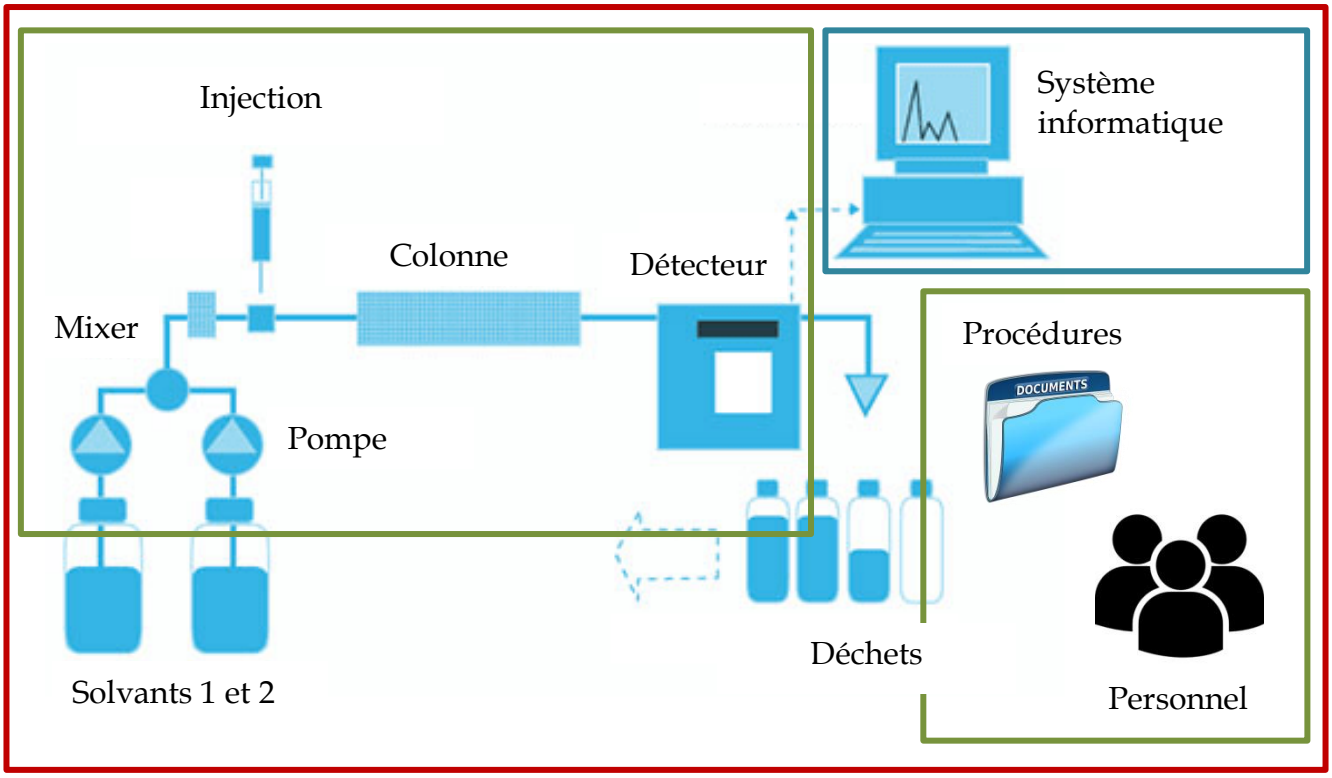

FIGURE 14 EXEMPLE D'UNE SYSTEME INFORMATISE - HPLC

Le système informatisé doit donc s'entendre comme l'environnement de la donnée. Ce n'est plus uniquement le système informatique (qui génère directement des données) qu'il faut analyser mais tout l'écosystème qu'il y a autour afin d'avoir une vision élargie et juste des risques de perte d'intégrité qui peuvent survenir.

6.5 VALIDATION

Bien que ne pouvant être considéré seule, la validation constitue un des outils, qui permet d'assurer l'intégrité des données générées et traitées par un système. Lorsque ce système fonctionne de manière reproductible et efficace et que les biais ont été maitrisés et contrôlés, la confiance à l'intégrité des données gérée augmente sensiblement.

La validation est définie dans les BPF comme suit : « La validation d'un procédé (VP) est la preuve documentée que le procédé mis en œuvre à l'intérieur des paramètres établis peut fonctionner de manière efficace et reproductible pour produire un intermédiaire ou une substance active conforme à ses spécifications et à ses caractéristiques de qualité préétablies ».(5) Il convient également en cas de changement ayant un impact sur la qualité du produit de maintenir cet état validé.

La validation s'applique donc à un système entier (voir Figure 13), dans lequel se trouve des équipements qui seront, eux qualifiés. On parlera donc de validation d'un système informatisé et de qualification d'un système informatique.

Il existe trois types de validations :

- La validation prospective
- La validation rétrospective
- La validation concomitante

6.5.1 VALIDATION PROSPECTIVE

C'est une validation effectuée avant la production de routine de produits destinés à la vente ou sur un produit fabriqué selon un procédé, comportant des modifications importantes pouvant se répercuter sur les caractéristiques du produit.

6.5.2 VALIDATION RETROSPECTIVE

Pour des produits plus anciens, la validation prospective n'était pas encore applicable. Par conséquent, ces produits doivent être à présent soumis à une validation. La validation rétrospective est réalisée pour un produit déjà commercialisé et est définie comme l'établissement de la preuve documentée qu'un système fait ce qu'il prétend faire, « sur la base des données relatives à la fabrication, aux essais et au contrôle du lot ». (5) Cette revue de toute la fabrication antérieure évalue les données dans le but de prouver que le processus est toujours sous contrôle. Elle peut être utilisée pour les procédés bien établis qui ont été utilisés sans aucun changement majeur qui affecte les attributs qualité critiques du produit. Elle peut être utilisée par exemple pour d'anciens produits non validés lors de leur mise sur le marché mais devant l'être à présent pour être conformes aux exigences réglementaires.

6.5.3 VALIDATION CONCOMITANTE

C'est une validation réalisée durant la production de routine de produits destinés à la vente qui n'est utilisée qu'à titre exceptionnel et qui, dans tous les cas, doit être justifiée.

6.6 QUALIFICATION

La qualification, au même titre que la validation, mais ici à l'échelle d'un équipement (système informatique), aide à supporter l'intégrité des données. Tout comme la validation, la qualification d'un équipement ne peut garantir à elle seule l'intégrité des données, elle doit être couplée à un système efficace de Data Management. Cependant, la confiance en une donnée débute lorsqu'on peut avoir confiance en l'équipement qui la génère, c'est pourquoi la qualification demeure un outil indispensable pour la mise en conformité et le maintien de l'intégrité des données produites.

La qualification selon les BPF, est définie comme une « opération destinée à démontrer que tout matériel ou équipement utilisé pour la fabrication, le conditionnement ou le contrôle fonctionne correctement et donne des résultats attendus pour l'usage auquel il est destiné ». (5) Elle fait partie à part entière du processus de validation.

Il existe différentes qualifications suivant l'étape de développement de l'équipement, depuis la conception jusqu'à l'utilisation en routine :

- Qualification de conception (QC)
- Qualification d'installation (QI)
- Qualification opérationnelle (QO)
- Qualification de performance (QP)

La figure ci-après présente ces différentes étapes et les spécifications clefs associées :

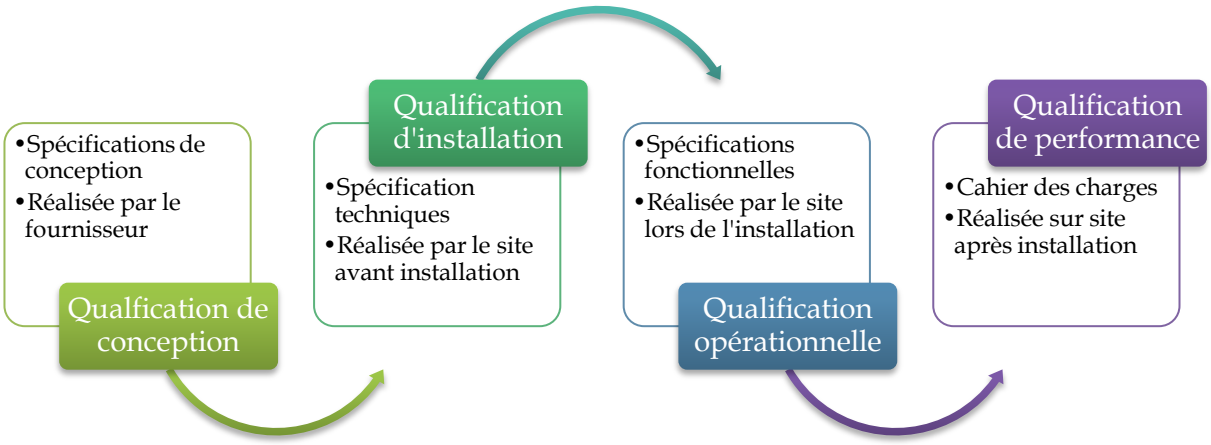

FIGURE 15 - ETAPES DE QUALIFICATION D'UN EQUIPEMENT

6.6.1 QC : QUALIFICATION DE CONCEPTION

La qualification de conception a pour but de vérifier la conformité qualitative et quantitative des spécifications documentées depuis l'expression des besoins jusqu'aux ordres de mise en œuvre, incluant les données d'entrée (DE), revue de conception, cahier des charges et ordre de mission.

Les documents de sortie seront constitués de cahier des charges, analyse de risque et de criticité et les spécifications de mises en œuvre.

A la suite de cette première qualification, réalisée par le concepteur / fournisseur de l'équipement, l'entreprise doit réaliser deux types des tests :

Tests d'acceptation d'usine ou Factory Acceptance Test (FAT)

Cette phase de qualification a pour objectif de vérifier les tests fournisseurs (partiellement ou totalement) avant livraison sur site et la conformité des systèmes à qualifier par rapport :

- aux spécifications des besoins utilisateur ou cahier des charges,
- aux spécifications fonctionnelles approuvées,
- à la conception approuvée,
- aux exigences réglementaires,
- aux besoins de qualification du projet,

Il s'agit schématiquement de vérifier sur base documentaire la qualification de conception.

Test d'acceptation du site ou Site Acceptance Test (SAT)

Cette phase de qualification, réception, liée au processus d'ingénierie a pour objectif de vérifier les tests fournisseurs sur le site avec toutes les utilités connectées et permet également de finaliser les derniers réglages par rapport à l'environnement du système. (18)

Il s'agit là de vérifier la qualification de conception dans l'environnement réel de l'équipement.

A l'issue de cette première phase, l'équipement contrôlé par le fournisseur et approuvé par le site receveur peut être mis en exploitation dans l'entreprise. La phase de Qualification d'Installation peut alors débuter.

6.6.2 QI : QUALIFICATION D'INSTALLATION

La qualification d'installation est la vérification documentée qu'au moment de leur mise en place, chacun des systèmes, leur environnement et leur configuration, sont en conformité avec :

- les paramètres critiques (hors fonctionnement),
- les recommandations des fournisseurs,
- la réglementation.

Le protocole et les fiches de tests sont rédigés à partir des spécifications des besoins utilisateur, des spécifications d'ingénierie, des critères d'acceptation et suivant les conclusions de l'analyse de criticité composants.

L'acceptation de la qualification d'installation sert à prouver que le système a été vérifié et que toute la documentation fournisseur nécessaire est complète.

L'acceptation de cette phase est formalisée par un rapport de qualification d'installation qui autorise le passage à la phase de qualification opérationnelle en l'absence de réserves critiques sur le système.

Le rapport de qualification d'installation est approuvé lorsque tous les écarts ont été statués et toutes les réserves critiques de qualification levées et soldées.

6.6.3 QO : QUALIFICATION OPERATIONNELLE

La qualification opérationnelle permet de s'assurer et de vérifier, de façon documentée, que le système fonctionne dans les plages spécifiées et que le personnel de production a été formé.

La qualification opérationnelle fait appel à la réalisation de tests appelés « tests fonctionnels » permettant de simuler le fonctionnement de l'équipement, de l'installation ou du système dans son intégralité, et notamment avec le ou les sous-systèmes de contrôle commande.

Ces tests permettent de s'assurer que le matériel installé répond aux spécifications et à la conception approuvée, fonctionne et s'intègre correctement par rapport aux autres matériels des systèmes informatiques ou système existants.

Les tests opérationnels de l'équipement et la validation des systèmes informatisés associés peuvent être effectués simultanément.

L'acceptation de cette phase est formalisée par un rapport de qualification opérationnelle qui autorise le passage à la phase de qualification de performance en l'absence de réserve critique sur le système.

Le rapport de qualification opérationnelle est approuvé lorsque tous les écarts critiques ont été levés et statués et toutes les réserves critiques de qualification soldées.

6.6.4 QP : QUALIFICATION DES PERFORMANCES

La dernière étape de cette série de qualifications est la qualification de performance. Elle consiste à démontrer que le procédé unitaire atteint ses performances de manière reproductible et conforme tout en respectant les spécifications et les attributs qualité.

Les documents de sortie seront constitués des fiches de tests avec relevé des paramètres, enregistrements et la synthèse incluant d'éventuelles réserves et leur traitement autorisant l'exploitation en routine.

6.7 DATA MANAGEMENT

La notion de Data Mangement est née de la compréhension des exigences en matière de Data Integrity. Il ne s'agit plus uniquement de disposer de systèmes validés et

d'équipement qualifiés mais de mettre en place une stratégie globale de gestion des données.

Plus qu'un outil de gestion, il s'agit d'un secteur à part entière du système de management de la Qualité en entreprise. Le Data management est guidé par l'analyse de risques sur l'intégrité des données qui est réalisée. Seront alors considérées les données électroniques, les données papier, mais également les données hybrides et « les interfaces entre les deux au cours de leur cycle de vie, et non plus seulement sur les systèmes critiques ». (19)

La Data Mangement est le versant qualité qui fait appliquer les principes de gestion de l'intégrité des données tout au long du cycle de vie des données. Il suit les principes de l'ALCOA + et des bonnes pratiques documentaires et informatiques. Ses outils peuvent être les mêmes que pour une gestion de la qualité produit mais en ciblant non plus le cycle de vie d'un produit mais celui d'une donnée.

Exemple : *Le Data Management peut passer par une formation des équipes aux risques liés à une perte d'intégrité des données.*

Il peut également se traduire par la mise en place au sein d'une entreprise d'un système de signatures électroniques des documents déterminés, via une analyse de risques, comme étant prioritaires.

7 ANALYSE DE RISQUE DE L'EQUIPEMENT

Afin de déterminer et de classer les systèmes informatiques selon leur besoin en termes de qualification, il va être nécessaire dans un premier temps d'effectuer une évaluation risque. Cette évaluation va reposer sur la probabilité d'occurrence d'un dommage ou dysfonctionnement.

La probabilité d'apparition d'un dommage sera fonction de la complexité du système selon deux modalités :

- **Complexité Logiciel**
- **Complexité Matériel**

Cette classification de complexité permet de couvrir les différents aspects d'un système informatique comme l'illustre la Figure 13. L'étude de la complexité logicielle permettra d'évaluer le *software*. L'étude de la complexité du matériel permettra quant à elle d'apprécier l'équipement, le *hardware* et le cas échéant le *firmware* du système.

Le potentiel comportement humain vis-à-vis du système informatisé ainsi que les procédures associées seront eux-mêmes fonction de la complexité globale du système.

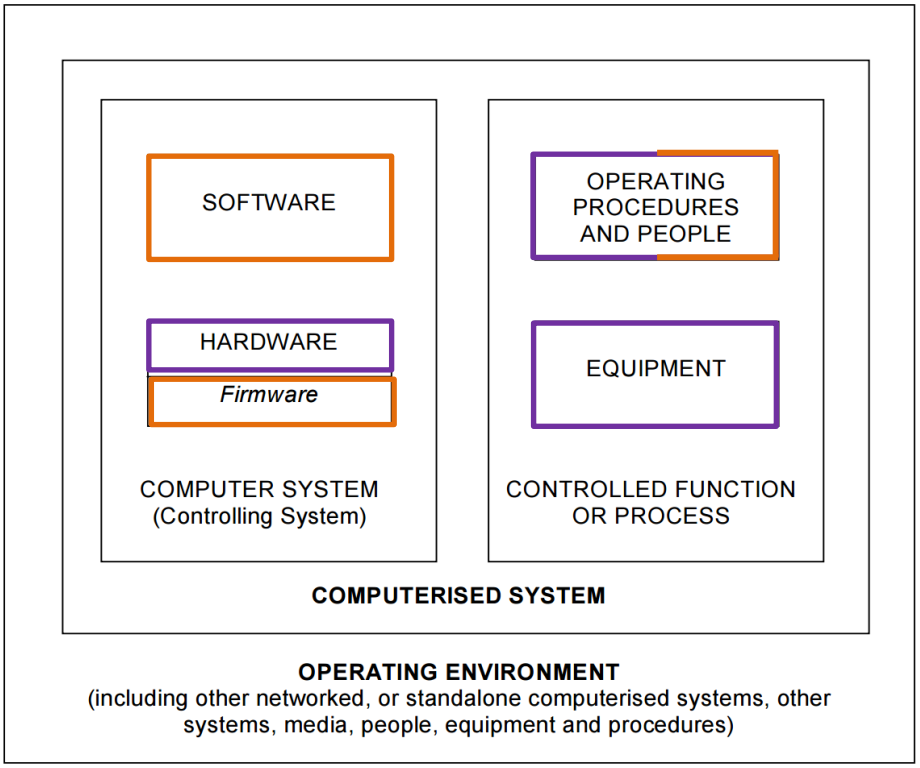

FIGURE 16 ETUDE DE COMPLEXITE DU SYSTEME INFORMATISE

7.1.1 COMPLEXITE LOGICIEL

La complexité logicielle est fonction du type de logiciel intégré au système. On distingue donc différents cas :

- Firmware : programme intégré directement dans le matériel. *Exemple : clef usb*
- Logiciel non configurable : logiciel ne pouvant être paramétré par l'utilisateur. *Exemple : pHmètre*
- Logiciel configurable : logiciel pouvant être configuré par l'utilisateur. *Exemple : logiciel de chromatographie liquide haute performance*
- Logiciel personnalisé : Logiciel conçu spécifiquement pour répondre aux besoins d'une entreprise. *Exemple : logiciel d'une machine de production spécifique*

TABLEAU V ECHELLE DE COMPLEXITE - LOGICIEL

Cotation	Niveau
1	Firmware
3	Logiciels non configurables
5	Logiciels configurables
10	Logiciel personnalisés

7.1.2 COMPLEXITE MATERIEL

Dans cette analyse, le terme matériel désigne à la fois les notions d'équipement, c'est-à-dire l'appareillage servant à effectuer la tâche considérée ainsi que la partie *hardware* du système informatique.

La complexité matérielle est fonction du d'équipement considéré. On distingue donc différents cas :

- Matériel standard non configurable sans capacité de mesure *Exemple : Compresseur pour recyclage des déchets*
- Matériel standard non configurable avec capacité de mesure. *Exemple : Thermomètre électronique*
- Matériel configurable avec ou sans capacité de mesure. *Exemple : Ordinateur de bureau*
- Matériel personnalisé avec ou sans capacité de mesure. *Exemple : Mélangeur réalisé sur mesure*

TABLEAU VI ECHELLE DE COMPLEXITE - MATERIEL

Cotation	Niveau
1	Matériel standard non configurable sans capacité de mesure
3	Matériel standard non configurable avec capacité de mesure
5	Matériel configurable avec ou sans capacité de mesure
10	Matériel personnalisé avec ou sans capacité de mesure

7.1.3 INDICE DE COMPLEXITE

L'indice de complexité correspondra au produit des cotations respectives de complexité logiciel et complexité matériel.

Complexité = Complexité logiciel x complexité matériel

1 ≤ Indice Equipement ≤ 9 : équipement simple

9 < Indice Equipement ≤ 25 : équipement de complexité intermédiaire

25 < Indice Equipement ≤ 100 : équipement complexe

Cet indice de complexité permet de déterminer la nécessité et le degré d'effort qui devront être mis en place pour la qualification de l'équipement.

Le tableau ci-après présente les efforts de qualification nécessaires en fonction de la criticité du logiciel et du matériel :

TABLEAU VII - QUALIFICATION NECESSAIRE EN FONCTION DE LA COMPLEXITE DU SYSTEME

		Complexité matériel			
		Simple 1	**Faible 3**	**Intermédiaire 5**	**Elevée 10**
Complexité logiciel	**Simple 1**	Qualification d'installation (QI)	Qualification d'installation (QI)	QI + Qualification opérationnelle (QO)	QI + Qualification opérationnelle (QO)
	Faible 3	Qualification d'installation (QI)	Qualification d'installation (QI)	QI + Qualification opérationnelle (QO)	QI + QO + Qualification de performance (QP)
	Intermédiaire 5	QI + Qualification opérationnelle (QO)	QI + Qualification opérationnelle (QO)	QI + Qualification opérationnelle (QO)	QI + QO + Qualification de performance (QP)
	Elevée 10	QI + Qualification opérationnelle (QO)	QI + QO + Qualification de performance (QP)	QI + QO + Qualification de performance (QP)	QI + QO + Qualification de performance (QP)

Le système informatique, ayant été analysé, il convient à présent de s'intéresser au système informatisé c'est-à-dire au système informatique et son environnement.

8 ANALYSE DE RISQUES SYSTEME

La mise en place du « Data Integrity » s'effectue en deux temps. Il s'agit dans un premier temps de mesurer la sensibilité associée aux données (qui inclue la complexité du système informatique) puis dans un second temps, d'évaluer l'impact que pourrait avoir une donnée erronée ou manquante à l'échelle de l'entreprise : la criticité.

Le degré d'effort et les ressources allouées à l'organisation et aux techniques de contrôle du cycle de vie des données seront déterminés en fonction de la sensibilité et de la criticité de ces données comparées aux autres besoins qualité. L'entreprise doit créer un système capable de fournir un niveau de contrôle acceptable des données basé sur une analyse de risque documentée.

L'avantage de ce type d'analyse est qu'il devient possible d'analyser soit uniquement les données au cas par cas afin de mettre en place un système de Data Management seul ; soit de faire les moyennes des résultats obtenus pour chaque donnée afin d'analyser le système dans son intégralité pour par exemple, statuer sur une éventuelle validation de ce dernier couplée à des actions de Data Management.

8.1 SENSIBILITE

Trois critères seront étudiés afin d'évaluer la sensibilité à la donnée :

- La subjectivité
- La traçabilité
- L'accessibilité

8.1.1 LA SUBJECTIVITE

Ce critère est dépendant de la complexité du système informatique qui produit la donnée. En effet, un système complexe implique souvent une interprétation des données et donc une éventuelle perte de représentativité. De façon générale, plus le système est complexe et plus la donnée sera soumise à interprétation car elle ne pourra pas être exploitée directement.

Le Tableau VIII Représentativité des données en fonction de la complexité du système donne quelques exemples d'appareils fréquemment utilisés en industrie pharmaceutique.

TABLEAU VIII REPRESENTATIVITE DES DONNEES EN FONCTION DE LA COMPLEXITE DU SYSTEME

Complexité du système	**Système simple**	→				**Système complexe**
↓	pH-mètre	Test d'intégrité du filtre			Serveur de réponse interactive	ERP / Progiciel
		Spectrophotomètre UV	Système HPLC	Chromatographie en phase liquide couplée à spectrométrie de masse	Système de gestion de l'information en laboratoire	Logiciels personnalisés
	Balance	Spectroscopie IR		Base de données de pharmacovigilance		
		Machines ECG	Dossier permanent de l'essai		Base de données clinique	
		Tableur			Outils d'analyse statistique	
	Thermomètres	Enregistreurs de données	Domotique			
Logiciel	Pas de logiciel	Logiciel simple				Logiciel complexe
Impressions / sorties	Peuvent représenter les données originales	Ne sont pas représentatives des données originales				

MANIPULATION INTERPRETATION

<u>Exemple :</u> le traitement des données par un logiciel d'analyse statistique puis une interprétation humaine sont deux facteurs de risque concernant la représentativité de la donnée.

Les systèmes complexes donneront la plupart du temps lieu à une interprétation des données qu'elle soit humaine ou informatique, le risque associé sera donc élevé. Cependant, les systèmes dits de faible complexité tels que les pH-mètres ou les balances présentent également un risque élevé et ne doivent pas être ignorés car les données générées peuvent être aisément manipulées ou répétées et perdre leur fiabilité et leur représentativité. (Voir critère vulnérabilité)

Quelques exemples pour illustrer chaque cotation :

- Donnée issue d'un système « simple », non soumise à interprétation. *Exemple : Balance*
- Donnée directement interprétée par le système qui la génère. Cas d'un système qualifié. *Exemple : Logiciel d'édition / impression d'étiquettes*
- Donnée soumise à interprétation humaine. *Exemple : Graphiques issus d'une sonde de température*
- Donnée soumise à interprétation humaine collégiale ou interprétée par un système non qualifié. *Exemple : Chromatographe liquide haute performance non qualifié*

TABLEAU IX ECHELLE DE RISQUE ASSOCIE - SUBJECTIVITE

Cotation	Niveau
1	Donnée issue d'un système « simple », non soumise à interprétation
3	Donnée directement interprétée par le système qui la génère. Cas d'un système qualifié.
5	Donnée soumise à interprétation humaine
10	Donnée soumise à interprétation humaine collégiale ou interprétée par un système non qualifié.

Jugée comme la moins impactante, la subjectivité possède une échelle de risque avec des cotation plus faibles que la traçabilité et l'accessibilité afin de pondérer ces différents critères d'analyse.

8.1.2 TRAÇABILITE

Ce paramètre est relatif à l'équipement ou au système informatisé qui génère la donnée. Ce risque varie d'abord, suivant le degré avec lequel la donnée (ou le système qui la génère) peut être configuré, et donc potentiellement manipulé. Par exemple la possibilité de répéter des mesures afin d'obtenir une valeur conforme sur un pH-mètre traduit un fort risque associé.

Nous nous intéressons donc dans cette section à la possibilité ou non pour chaque donnée d'obtenir un historique des modifications /créations / suppression effectuées ou de contrôle via un système de double VISA.

Ce paramètre ayant un fort impact sur l'intégrité des données, une échelle de risque différente de celle de la subjectivité a été établie. Les cotations sont plus élevées afin de pondérer de façon plus marquée l'indice final.

TABLEAU X ECHELLE DE RISQUE ASSOCIE - TRAÇABILITE

Cotation	Niveau
1	IT (Informatique) : Audit trail complet des paramètres critiques Papier : VISA + double contrôle systématique par un tiers habilité
5	IT : Signature électronique de l'élément Papier : VISA + vérification finale par un responsable
10	IT : Identification des personnes ayant édité et/ou modifié le document sans signature électronique Papier : VISA sans vérification ultérieure
100	IT / Papier : aucune identification

8.1.3 L'ACCESSIBILITE

Ce dernier paramètre est en lien avec la traçabilité. Cependant, il inclut une notion supplémentaire, celle de la sécurisation de la donnée. Une sécurité doit être apportée afin de ne pas avoir de perte ou de modification non autorisée volontaire ou non mais également de ne pas avoir de consultation et/ou de diffusion des données aux personnes non autorisées. Ce paramètre est d'autant plus important lorsque des données sensibles ou confidentielles sont traitées.

Tout comme pour le paramètre « traçabilité », une échelle de risque différente de celle de la subjectivité a été établie. Les cotations sont plus élevées afin de pondérer de façon plus marquée l'indice final.

Quelques exemples pour illustrer chaque cotation :

- Accès restreint à l'aide d'identifiants uniques (logins) aux seules personnes concernées. *Exemple : sessions individuelles avec mot de passe sur un automate de fabrication*
- Accès restreint sans identifiants uniques (logins) aux seules personnes concernées. *Exemple : données protégées par un mot de passe connu uniquement par les personnes concernées*
- Accès restreint aux groupes de personnes potentiellement concernées sans distinction individuelle. Exemple : données accessibles dans un dossier informatique par un seul service de l'entreprise type « Dossier Qualité »
- Pas de restriction d'accès au sein de l'entreprise *Exemple : Equipement de production accessible à tout moment par une personne non concernée*

TABLEAU XI ECHELLE DE RISQUE ASSOCIE - ACCESSIBILITE

Cotation	Niveau
1	Accès restreint à l'aide d'identifiants uniques (logins) aux seules personnes concernées
5	Accès restreint sans identifiants uniques (logins) aux seules personnes concernées
10	Accès restreint aux groupes de personnes potentiellement concernées sans distinction individuelle.
100	Pas de restriction d'accès au sein de l'entreprise

8.1.4 INDICE DE SENSIBILITE

L'indice de sensibilité correspondra au produit des cotations respectives de Subjectivité / Traçabilité / Accessibilité :

Sensibilité = Subjectivité x Traçabilité x Accessibilité

1 ≤ Indice de sensibilité ≤ 75: faible sensibilité

75 < Indice de sensibilité ≤ 500: sensibilité moyenne

500 < Indice de sensibilité ≤ 100 000: forte sensibilité

Cet indice traduit la sensibilité de la ou des données dans le contexte du système informatisé. Elle prend en compte le système informatique ainsi que l'aspect organisationnel et humain du système.

8.2 CRITICITE

La criticité représente l'impact d'un défaut processus, d'une perte d'information ou de l'exploitation d'une donnée erronée vis-à-vis de trois acteurs clefs :

- Le patient ou consommateur du produit final
- L'entreprise elle-même
- Les autorités compétentes ou le client de l'entreprise (dans le cas d'un façonnier)

8.2.1 PATIENT / CONSOMMATEUR

Cette composante de l'analyse s'intéresse à l'acteur en bout de chaîne qui va acheter et/ou consommer le produit fabriqué. Nous nous intéresserons à l'impact d'un défaut sur la santé du patient mais également sa satisfaction à l'égard du produit. Elle-même en lien avec la confiance que le consommateur aura vis-à-vis de l'entreprise.

Quelques exemples pour illustrer chaque cotation :

- N'entraine ni risque pour le patient, ni gêne lors de l'utilisation *Exemple : témoin de l'étiquette produit absente du dossier de fabrication*
- Sans conséquence pour la santé du consommateur mais insatisfaction. *Exemple : Légère rayure sur le décor d'un produit n'entrainant pas de difficultés de lecture.*
- Gêne lors de l'utilisation par le consommateur. *Exemple : Défauts d'impression sur le décor du produit entrainant des difficultés de lecture des instructions d'utilisation.*
- Défaut pouvant générer un risque pour la sécurité du patient. *Exemple : Mauvais dosage du principe actif lors de la fabrication.*

TABLEAU XII ECHELLE DE CRITICITE – IMPACT PATIENT / CONSOMMATEUR

Cotation	Dénomination	Impact
1	Sans impact	N'entraine ni risque pour le patient, ni gêne lors de l'utilisation
5	Impact mineur	Sans conséquence pour la santé du consommateur mais insatisfaction
10	Impact majeur	Gêne lors de l'utilisation par le consommateur
100	Impact critique	Défaut pouvant générer un risque pour la sécurité du patient

8.2.2 ORGANISATIONNEL / FINANCIER

Dans cette partie, il s'agira d'évaluer l'impact que pourrait avoir une donnée manquante ou erronée sur la santé de l'entreprise. Seront considérées des perte financières et/ou organisationnelles.

Quelques exemples pour illustrer chaque cotation :

- N'entraine ni perte de temps, ni désorganisation du travail, ni perte financière. *Exemple : Fichier de suivi des congés d'un service rendu accessible accidentellement à un autre service.*
- Perte de temps modérée, n'entrainant pas de désorganisation. Ou perte financière sans impact significatif. *Exemple : VISA préparateur manquant dans un dossier de fabrication.*
- Surcharge de travail et/ou désorganisation modérée mais temporaire. Ou interruption ou ralentissement temporaire de certaines activités. Ou perte financière modérée. *Exemple : erreur dans le planning d'assignation des équipes aux lignes de production.*

- Désorganisation importante et durable de l'activité avec perte significative d'activité et/ou replanification et/ou recours à un tiers. Ou perte financière importante. *Exemple : Erreur de conditionnement d'un vrac (formule adulte dans flacon enfant), rejet et destruction du lot.*

TABLEAU XIII ECHELLE DE CRITICITE - IMPACT ORGANISATIONNEL / FINANCIER

Cotation	Dénomination	Impact
1	Sans impact	N'entraine ni perte de temps, ni désorganisation du travail, ni perte financière.
3	Impact mineur	Perte de temps modérée, n'entrainant pas de désorganisation. Perte financière sans impact significatif.
5	Impact majeur	Surcharge de travail et/ou désorganisation modérée mais temporaire. Interruption ou ralentissement temporaire de certaines activités. Perte financière modérée
10	Impact critique	Désorganisation importante et durable de l'activité avec perte significative d'activité et/ou replanification et/ou recours à un tiers Perte financière importante

Tout comme pour la subjectivité, une pondération des différents critères a été appliquée. L'impact organisationnel et financier a été jugé moins critique que les impacts « Responsabilité / Image client » et « Patient / consommateur », il possède donc des cotations plus faibles.

8.2.3 RESPONSABILITE / IMAGE CLIENT

Enfin, ce dernier item de la criticité s'intéresse à l'impact d'un défaut d'intégrité des données sur la responsabilité de l'entreprise vis-à-vis des autorités compétentes ainsi que de sa capacité à satisfaire et à garder la confiance de son client (cas d'un façonnier ou d'une relation avec un distributeur).

Quelques exemples pour illustrer chaque cotation :

- Sans impact, absence de plainte. *Exemple : Suppression accidentelle du fichier Excel de réservation des salles de réunion.*
- Evènement indésirable sans lien avec le cahier des charges Ou insatisfaction client modérée sans impact sur sa confiance. *Exemple : destruction accidentelle des fiches de spécifications des articles de conditionnement signées par le client.*
- Non-respect du cahier des charges. Ou insatisfaction client avec perte de confiance passagère. *Exemple : Fiche de prix produit ayant fuité de l'entreprise car manque de sécurisation des échanges mail et du travail à domicile d'un employé.*
- Non-respect des lois en vigueur et/ou condamnation pénale Ou perte définitive du client. *Exemple : Certificat d'analyses produit falsifié.*

TABLEAU XIV ECHELLE DE CRITICITE - IMPACT RESPONSABILITE / IMAGE CLIENT

Cotation	Dénomination	Impact
1	Sans impact	Sans impact, absence de plainte
5	Impact mineur	Evènement indésirable sans lien avec le cahier des charges Insatisfaction client modérée sans impact sur sa confiance
10	Impact majeur	Non-respect du cahier des charges Insatisfaction client avec perte de confiance passagère
100	Impact critique	Non-respect des lois en vigueur et/ou condamnation pénale Perte définitive du client

8.2.4 INDICE DE CRITICITE

Afin de permettre une analyse plus fine et un recoupement avec l'indice de sensibilité, il convient de calculer l'indice de criticité. Cet indice correspondra au produit des cotations respectives de l'Impact patient ou consommateur/ Impact organisationnel et financier / Financier et Responsabilité / Image client :

Criticité = Sécurité x Organisationnel x Responsabilité

1 ≤ Indice Equipement ≤ 75: Impact mineur

75 < Indice Equipement ≤ 500: Impact majeur

500 < Indice Equipement ≤ 100 000: Impact critique

Cet indice de criticité est à coupler avec les résultats de sensibilité précédents.

8.3 RESULTATS DE L'ANALYSE DE RISQUE ET DEGRE DE VALIDATION

L'indice de sensibilité calculé couplé à l'indice de criticité vont permettre à l'entreprise de déterminer les efforts de validation qui seront appliqués au système informatisé. Pour chaque système informatisé, il convient de faire respectivement les moyennes des indices de sensibilité et de criticité des données analysées dont le cycle de vie est lié à ce système, puis de comparer ces deux valeurs au tableau ci-après :

TABLEAU XV - VALIDATION NECESSAIRE EN FONCTION DE LA SENSIBILITE ET DE LACRITICITE DU SYSTEME INFORMATISE

		Sensibilité		
		Faible	**Moyenne**	**Forte**
Criticité	**Mineur**	Risque négligeable	Risque négligeable	Qualification équipement
	Majeur	Qualification équipement	Qualification équipement	Validation du système
	Critique	Validation du système	Validation du système	Validation du système

Exemple :

Donnée 1 : Sensibilité = 250 (Moyenne) / Criticité = 300 (Majeur)

Donnée 2 : Sensibilité = 500 (Moyenne) / Criticité = 100 (Majeur)

Donnée 3 : Sensibilité = 50 (Faible) / Criticité = 250 (Majeur)

Moyenne : Sensibilité = 267 (Moyenne) / Criticité = 217 (Majeur)

D'après le tableau ci-dessus, le risque associé à ce système étant globalement « moyen », une qualification de l'équipement serait suffisante.

Dès lors qu'il s'agit de moyennes, certains choix peuvent demeurer difficiles lorsqu'interviennent des extrêmes. Doit-on considérer un risque global comme négligeable alors qu'une donnée a été analysée comme étant critique et à forte sensibilité ?

L'entreprise est donc libre d'appliquer des règles supplémentaires. Par exemple, il serait envisageable d'ajouter la règle suivante : lorsqu'une donnée est évaluée comme « critique », même si la moyenne ne l'est pas, il convient d'effectuer une validation du système. Les analyses de risques étant des outils, il convient de les adapter au mieux aux besoins de l'entreprise.

Enfin, la validation ou la qualification n'étant pas, à elles seules, suffisantes pour garantir l'intégrité des données, il convient de les coupler, à un Data Management efficace.

8.4 CLASSEMENT DES DONNEES

Le degré d'implication du système de Data Management, au même titre que le degré d'effort de validation du système, est dépendant de la combinaison de l'indice de criticité et de l'indice de sensibilité associé à la donnée.

On peut dès lors classer les données à intégrer à un système de Data Management en quatre groupes :

- Les données non sensibles non critiques. Il s'agit de données dont une perte ou modification n'aurait pas ou peu d'impact mais qui demeurent correctement maitrisées par l'entreprise.

Exemple : Fichier Excel de suivi des congés d'un service, accessible par ce service uniquement et protégé par un mot de passe

- Les données sensibles non critiques. Il s'agit de données dont une perte ou modification n'aurait pas ou peu d'impact mais qui ne sont pas maitrisées par l'entreprise. Ces données sont à étudier au cas par cas afin de déterminer si des actions sont nécessaires ou non.

Exemple : *tableau de suivi de l'entretien des espaces verts accessible par toute l'entreprise*

- Les données non sensibles critiques. Il s'agit là de données qui ont un fort impact sur les décisions finales. Le risque de modification ou suppression est en général faible et maitrisé mais compte tenu de l'impact que peuvent avoir ces données il est nécessaire d'en assurer un suivi.

Exemple : *équipement de production avec sessions individuelles et mot de passe*

- Les données sensibles critiques. Bien que rares, elles constituent une faille majeure dans un système de management de l'intégrité des données. Il s'agit de données ayant un fort impact sur la qualité du produit fini mais qui ne sont pas maitrisées et donc soumises au risque de biais ou de perte de l'information. Ce dernier groupe traduit une faiblesse du système et doit être traité en priorité.

Exemple : *Chromatographe liquide haute performance non qualifié, en libre accès pour tout le personnel de l'entreprise*

Le schéma ci-après présente ces différentes grandes catégories de données :

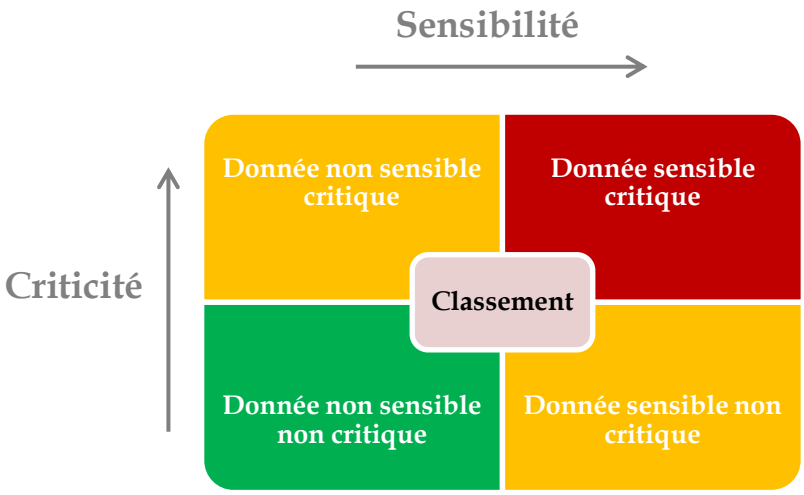

FIGURE 17 - CLASSEMENT DES DONNEES EN FONCTION DE LEUR SENSIBILITE ET DE LEUR CRITICITE

La priorisation des actions à mener est donc fonction de la sensibilité des données concernées et de leur criticité, c'est-à-dire l'impact potentiel d'une perte d'intégrité. Cette évaluation doit être réalisée selon des critères de notation définis au préalable. Il incombe à l'entreprise de définir une grille standardisée de cotation du risque selon ses propres critères ou d'adapter de façon collégiale une méthode d'analyse de risque à cette étude.

Il faut également inclure à cette étude l'acceptation d'un niveau approprié de risque résiduel, qui devra être correctement documenté et réévalué régulièrement. Ce risque

résiduel est, par définition, le risque qui subsiste après réponse ou après l'application de mesures d'atténuation de ce dernier.

Un des indicateurs de la maturité d'un système de management de la qualité est l'acceptation et l'évaluation de ce risque car elle implique nécessairement la priorisation des actions. A contrario, il semble peu probable qu'une entreprise qui ne considère ou ne détecte pas ce risque résiduel ait réalisé une étude de risque performante et adéquate.

9 CONCLUSION DE LA DEUXIEME PARTIE

Le sujet Data Integrity ayant été assimilé pendant longtemps à une problématique informatique, les dispositifs techniques sont bien souvent en place, qu'il s'agisse de fonctionnalités informatiques de sécurisation et de contrôle, ou d'automatisation de processus, destinée à limiter les erreurs liées aux interventions humaines.

La mise en place de solutions techniques n'est cependant pas suffisante si elles ne sont pas exploitées de manière appropriée et efficiente.

Le niveau d'effort à apporter pour maîtriser les données est fixé en fonction de la criticité de celles-ci et de leur impact sur l'entreprise, qu'il s'agisse de risque patient, d'impact financier ou de responsabilité réglementaire. La maitrise de l'intégrité des données suit donc une approche basée sur le risque, pour identifier les données critiques et les risques d'altération qui leur sont associés, afin d'ajuster les efforts de contrôle au juste nécessaire, et de manière proportionnelle avec les autres activités qualité.

Cette maitrise de l'intégrité des données passe en premier lieu par une maitrise technique des équipements et des systèmes via des qualifications et validations mais également par un Data Mangement efficace et robuste.

10 CONCLUSION GENERALE

L'intégrité des données est un processus important et qui demande une réadaptation de son système documentaire et de son système qualité en profondeur.

Les vingt dernières années ont très largement débattu des sujets relatifs à la validation des systèmes informatisés. Il est vrai que dans l'expression système d'information, la balance penchait beaucoup plus en faveur du système que de l'information. C'est la première grande vertu de cette démarche que d'avoir repositionné la donnée au centre du débat, en soulignant son importance mais aussi sa fragilité et ses menaces.

Les bonnes pratiques de gestion des données et de leur intégrité donnent confiance dans la robustesse des décisions pharmaceutiques et font partie intégrante du système Qualité. Les risques d'altération des données doivent être pilotés au même titre que les risques sur les produits, car la qualité d'un produit pharmaceutique est étroitement liée à la qualité de ses enregistrements de traçabilité.

L'aspect organisationnel de l'intégrité des données suppose une certaine maturité sur le sujet, avec une bonne implication des métiers et du management, et une prise de conscience des risques au niveau de l'entreprise, ce qui nécessite parfois une évolution de la culture.

La clé de la maîtrise du Data Integrity repose sur trois éléments fondamentaux :

- La compréhension de ses données au travers des analyses de risques en intégrant une vision « système » et « environnement » de la donnée
- Le développement et le maintien de la confiance en ses équipements et ses systèmes au moyen de qualification et de validation appropriées.
- Une mise en place efficace du Data Management avec un engagement fort de la Direction : une cause d'entreprise à tous les niveaux.

Les bonnes pratiques de Data Management et de Data Integrity font partie intégrante du système Qualité et permettent à l'entreprise d'avoir confiance en ses décisions grâce à une analyse fine et éclairée des évènements. C'est pourquoi, les risques de perte d'intégrité des données doivent être analysés et traités au même titre que les risques inhérents à la qualité des produits finis, car la qualité d'un produit pharmaceutique est très souvent liée à la qualité de ses données de traçabilité.

11 ANNEXES

11.1 ANNEXE 1

ANNEX I

Requirements for qualified certificates

Qualified certificates must contain:

(a) an indication that the certificate is issued as a qualified certificate;

(b) the identification of the certification-service-provider and the State in which it is established;

(c) the name of the signatory or a pseudonym, which shall be identified as such;

(d) provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended;

(e) signature-verification data which correspond to signature-creation data under the control of the signatory;

(f) an indication of the beginning and end of the period of validity of the certificate;

(g) the identity code of the certificate;

(h) the advanced electronic signature of the certification-service-provider issuing it;

(i) limitations on the scope of use of the certificate, if applicable; and

(j) limits on the value of transactions for which the certificate can be used, if applicable.

ANNEX II

Requirements for certification-service-providers issuing qualified certificates

Certification-service-providers must:

(a) demonstrate the reliability necessary for providing certification services;

(b) ensure the operation of a prompt and secure directory and a secure and immediate revocation service;

(c) ensure that the date and time when a certificate is issued or revoked can be determined precisely;

(d) verify, by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued;

(e) employ personnel who possess the expert knowledge, experience, and qualifications necessary for the services provided, in particular competence at managerial level, expertise in electronic signature technology and familiarity

with proper security procedures; they must also apply administrative and management procedures which are adequate and correspond to recognised standards;

(f) use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the processes supported by them;

(g) take measures against forgery of certificates, and, in cases where the certification-service-provider generates signature-creation data, guarantee confidentiality during the process of generating such data;

(h) maintain sufficient financial resources to operate in conformity with the requirements laid down in the Directive, in particular to bear the risk of liability for damages, for example, by obtaining appropriate insurance;

(i) record all relevant information concerning a qualified certificate for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings. Such recording may be done electronically;

(j) not store or copy signature-creation data of the person to whom the certification-service-provider provided key management services;

(k) before entering into a contractual relationship with a person seeking a certificate to support his electronic signature, inform that person by a durable means of communication of the precise terms and conditions regarding the use of the certificate, including any limitations on its use, the existence of a voluntary accreditation scheme and procedures for complaints and dispute settlement. Such information, which may be transmitted electronically, must be in writing and in readily understandable language. Relevant parts of this information must also be made available on request to third-parties relying on the certificate;
(l) use trustworthy systems to store certificates in a verifiable form so that:

- only authorised persons can make entries and changes,
- information can be checked for authenticity,
- certificates are publicly available for retrieval in only those cases for which the certificate-holder's consent has been obtained, and
- any technical changes compromising these security requirements are apparent to the operator.

ANNEX III

Requirements for secure signature-creation devices

1. Secure-signature-creation devices must, by appropriate technical and procedural means, ensure at the least that:

   (a) the signature-creation-data used for signature generation can practically occur only once, and that their secrecy is reasonably assured;

(b) the signature creation data used for signature generation cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology;

(c) the signature-creation-data used for signature generation can be reliably protected by the legitimate signatory against the use of others.

2. Secure signature creation devices must not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process.

ANNEX IV

Recommendations for secure signature verification

During the signature-verification process it should be ensured with reasonable certainty that:

(a) the data used for verifying the signature correspond to the data displayed to the verifier;

(b) the signature is reliably verified and the result of that verification is correctly displayed;

(c) the verifier can, as necessary, reliably establish the contents of the signed data;

(d) the authenticity and validity of the certificate required at the time of signature verification are reliably verified;

(e) the result of verification and the signatory's identity are correctly displayed;

(f) the use of a pseudonym is clearly indicated; and

(g) any security-relevant changes can be detected.

12 BIBLIOGRAPHIE

1. Comparing Recent Data ManagementIntegrity Guidances FDA EMA China FDA [Internet]. [cité 23 mai 2019]. Disponible sur: https://www.pharmaceuticalonline.com/doc/comparing-recent-data-management-integrity-guidances-fda-ema-china-fda-0001

2. Bezzenine N-I-P inspection des matières premières D de l'inspection. Focus sur l'intégrité des données - Réunion d'information à destination des opérateurs « matières premières à usage pharmaceutique ». :28.

3. Larousse É. Définitions : donnée - Dictionnaire de français Larousse [Internet]. [cité 8 oct 2017]. Disponible sur: http://www.larousse.fr/dictionnaires/francais/donn%C3%A9e/26436

4. Guide OMS des normes relatives aux bonnes pratiques de fabrication (BPF) [Internet]. [cité 23 mai 2019]. Disponible sur: https://apps.who.int/iris/bitstream/handle/10665/68527/WHO_VSQ_97.01_fre.pdf;jsessionid=AC1D738F60D091F8456C674BBD9A4E61?sequence=1

5. GUIDE DES BONNES PRATIQUES DE FABRICATION.

6. Guidance on good data and record management practices - WHO [Internet]. [cité 23 mai 2019]. Disponible sur: https://www.who.int/medicines/publications/pharmprep/WHO_TRS_996_annex05.pdf

7. Commissioner O of the. Warning Letters [Internet]. FDA. 2019 [cité 24 mai 2019]. Disponible sur: http://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/compliance-actions-and-activities/warning-letters

8. FDA Warning Letters Archives [Internet]. Ofni Systems. [cité 23 mai 2019]. Disponible sur: http://www.ofnisystems.com/fda-warning-letters/

9. CFR - Code of Federal Regulations Title 21 [Internet]. [cité 23 mai 2019]. Disponible sur: https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?fr=210.3

10. UK Data Archive - RESEARCH DATA LIFECYCLE [Internet]. [cité 12 juill 2017]. Disponible sur: http://www.data-archive.ac.uk/create-manage/life-cycle

11. Note technique Recommandations relatives à l'administration sécurisée des systèmes d'information - Secrétariat général de la défense et de la sécurité nationale [Internet]. [cité 24 mai 2019]. Disponible sur: https://www.ssi.gouv.fr/uploads/2015/02/NP_SDE_DAT_NT_Archi_Admin.pdf

12. alampel. EU Trusted Lists [Internet]. Digital Single Market - European Commission. 2013 [cité 24 mai 2019]. Disponible sur: https://ec.europa.eu/digital-single-market/en/eu-trusted-lists-trust-service-providers

13. MHRA_GxP_data_integrity_guide_March_edited_Final.pdf [Internet]. [cité 23 mai 2019]. 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

14. U.S. Department of Health and Human Services Food and Drug Administration Center for Drug Evaluation and Research (CDER) Center for Biologics Evaluation and Research (CBER) Center for Veterinary Medicine (CVM. Data Integrity and Compliance With Drug CGMP Questions and Answers Guidance for Industry. Quest Answ. 2018;17.

15. BERNARD M, YAYE HS, HOURI J-J, DO B. Management des risques appliqué à la production pharmaceutique - Concepts et réglementation [Internet]. Ref : TIP598WEB - « Médicaments et produits pharmaceutiques ». 2015 [cité 24 mai 2019]. Disponible sur: https://www.techniques-ingenieur.fr/base-documentaire/biomedical-pharma-th15/qualite-et-controle-des-medicaments-42642210/management-des-risques-applique-a-la-production-pharmaceutique-pha3050/

16. Démythifier l'Ordinateur en Biologie - Histoire de l'informatique [Internet]. [cité 24 mai 2019]. Disponible sur: http://www.snv.jussieu.fr/enseignement/DOB/Histoire.html

17. Pouvreau T. Les systèmes informatisés dans l'industrie pharmaceutique: approche de la conformité basée sur les risques et gestion agile des projets de validation. :90.

18. Rousseaux J-F. La validation des systèmes informatisés dans l'industrie pharmaceutique. réglementation, méthodologie et application au laboratoire de contrôle. :114.

19. Data Integrity : vers la mise en place d'un Data Management. [Internet]. A3P - Industrie Pharmaceutique & Biotechnologie. 2018 [cité 24 mai 2019]. Disponible sur: https://a3p.org/data-integrity-vers-la-mise-en-place-dun-data-management/

RESUME

La Data Integrity est au cœur des dernières évolutions réglementaires que ce soit aux Etats-Unis ou encore en Europe. Pourquoi un tel engouement pour l'intégrité des données ?

L'intégrité des données constitue une exigence fondamentale du système qualité pharmaceutique décrit au Chapitre 1 des GMP et une exigence générale du système Qualité des dispositifs médicaux décrits dans le paragraphe 4 de l'ISO 13485 :2016. Les données se réfèrent au système ALCOA et doivent donc être attribuables (auteur et source identifiées), lisibles (interprétables et à long terme), contemporaines (enregistrées au moment où elles sont collectées), originales (ou de copie certifiée) et fiables.

En outre, un système de gestion des risques doit être en place tout au long du cycle de vie des données jusqu'aux étapes de prise de décision garantissant l'intégrité des données. Ce système de management du risque devrait inclure un volet sur les process métier (production, contrôle qualité …) dont les facteurs à considérer sont :

- La complexité du process générant les données (mesure de pH sur un pHmètre contre des outils statistiques ou les logiciels complexes pour le traitement de la donnée…),
- Le niveau de protection de la donnée : degré de protection des données des sources d'altération : omission, destruction, manipulation…
- La cohérence des processus, le degré d'automatisation et d'intervention humaine,
- La subjectivité des résultats (interprétation ou non).

Considérant la mouvance actuelle de la réglementation et la nécessité de disposer d'une analyse toujours plus poussée de la maitrise des risques, il semble cohérent d'initier une réflexion en interne sur la gestion concrète de cette Data Integrity qui pourra notamment être portée par la validation des infrastructures et systèmes informatisés manipulant ces données.

FACULTE DE PHARMACIE UNIVERSITE DE LORRAINE

DEMANDE D'IMPRIMATUR

Date de soutenance : 27/06/2019

DIPLOME D'ETAT DE DOCTEUR EN PHARMACIE

présenté par : RUMOR OCEANNE

Sujet : **METHODE D'ANALYSE DE LA CONFORMITE DES DONNEES ET DES EQUIPEMENTS EN ACCORD AVEC LES RECOMMANDATIONS DES AUTORITES INTERNATIONNALES EN TERMES DE DATA INTEGRITY**

Jury :

Président : M. Igor CLAROT, Professeur
Directeur : M. Pierre Noël SIMON, Pharmacien – Directeur qualité
Juges : Mme Stéphanie RIBAULT, Responsable qualité opérationnelle
Mme Claudine BONNETIER, Pharmacien de production

Vu,

Nancy, le 16 · 05 · 2019

Le Président du Jury Et Co-Directeur — M. Igor CLAROT

Directeur de Thèse — M. Pierre Noël SIMON

Vu et approuvé,

Nancy, le 4 · 06 · 2019

Doyen de la Faculté de Pharmacie de l'Université de Lorraine,

Pr. Raphaël DUVAL

Vu,

Nancy, le

Le Président de l'Université de Lorraine,

Pierre MUTZENHARDT

N° d'enregistrement : 10748