Thèse d'exercice

Université de Limoges

Faculté de Pharmacie

Année 2023 Thèse N°

Thèse pour le diplôme d'État de docteur en Pharmacie

Présentée et soutenue publiquement

le 24 avril 2023

Par Arnaud AUGROS

Né le 14 février 1994 à Périgueux

Maitrise de l'intégrité des données sur un site de production pharmaceutique et stratégie d'implémentation sur les systèmes informatisés

Thèse dirigée par Marylène VIANA et Marc NOISETTE

Examinateurs :

Mme. le Professeur Marylène VIANA, Pharmacie Galénique, Président de thèse

M. le Docteur Marc NOISETTE, Pharmacien, Juge

Mme. le Docteur Betty LAVERDET POUCH, Pharmacie Galénique, Juge

Thèse d'exercice

Université de Limoges

Faculté de Pharmacie

Année 2023 Thèse N°

Thèse pour le diplôme d'État de docteur en Pharmacie

Présentée et soutenue publiquement

le 24 avril 2023

Par Arnaud AUGROS

Né le 14 février 1994 à Périgueux

Maitrise de l'intégrité des données sur un site de production pharmaceutique et stratégie d'implémentation sur les systèmes informatisés

Thèse dirigée par Marylène VIANA et Marc NOISETTE

Examinateurs :

Mme. le Professeur Marylène VIANA, Pharmacie Galénique, Président de thèse

M. le Docteur Marc NOISETTE, Pharmacien, Juge

Mme. le Docteur Betty LAVERDET POUCH, Pharmacie Galénique, Juge

Personnel enseignant de la Faculté de Pharmacie de Limoges

Le 1er septembre 2022

Doyen de la Faculté

Monsieur le Professeur COURTIOUX Bertrand

Vice-doyen de la Faculté

Monsieur LÉGER David, Maître de conférences

Assesseurs de la Faculté

Monsieur le Professeur BATTU Serge

Monsieur le Professeur PICARD Nicolas

Professeurs des Universités – Hospitalo-Universitaires

M. PICARD Nicolas	Pharmacologie
Mme ROGEZ Sylvie	Microbiologie, parasitologie, immunologie et hématologie
M. SAINT-MARCOUX Franck	Toxicologie

Professeurs des Universités – Universitaires

M. BATTU Serge	Chimie analytique et bromatologie
M. CARDOT Philippe	Chimie analytique et bromatologie
M. COURTIOUX Bertrand	Microbiologie, parasitologie, immunologie et hématologie
M. DESMOULIERE Alexis	Physiologie
M. DUROUX Jean-Luc	Biophysique et mathématiques
Mme FAGNÈRE Catherine	Chimie organique, thérapeutique et pharmacie clinique
M. LIAGRE Bertrand	Biochimie et biologie moléculaire
Mme MAMBU Lengo	Pharmacognosie
M. TROUILLAS Patrick	Biophysique et mathématiques
Mme VIANA Marylène	Pharmacie galénique

Maitres de Conférences des Universités – Hospitalo-Universitaires

M. BARRAUD Olivier (*)	Microbiologie, parasitologie, immunologie et hématologie
Mme. CHAUZEIX Jasmine	Microbiologie, parasitologie, immunologie et hématologie
M. JOST Jérémy	Chimie organique, thérapeutique et pharmacie clinique

Maitres de Conférences des Universités – Universitaires

M. BASLY Jean-Philippe (*)	Chimie analytique et bromatologie
Mme BEAUBRUN-GIRY Karine	Pharmacie galénique
Mme BÉGAUD Gaëlle	Chimie analytique et bromatologie
M. BILLET Fabrice	Physiologie
Mme BONAUD Amélie	Microbiologie, parasitologie, immunologie et hématologie
M. CALLISTE Claude	Biophysique et mathématiques
M. CHEMIN Guillaume	Biochimie et biologie moléculaire
Mme CLÉDAT Dominique	Chimie analytique et bromatologie
M. COMBY Francis	Chimie organique, thérapeutique et pharmacie clinique
Mme DELEBASSÉE Sylvie	Microbiologie, parasitologie, immunologie et hématologie
Mme DEMIOT Claire-Elise (*)	Pharmacologie
M. FABRE Gabin	Biophysique et mathématiques
M. LABROUSSE Pascal (*)	Botanique et cryptogamie
Mme LAVERDET Betty	Pharmacie galénique
M. LAWSON Roland	Pharmacologie
M. LÉGER David	Biochimie et biologie moléculaire
Mme MARRE-FOURNIER Françoise	Biochimie et biologie moléculaire
M. MERCIER Aurélien	Microbiologie, parasitologie, immunologie et hématologie

Mme MILLOT Marion (*)	Pharmacognosie
Mme PASCAUD-MATHIEU Patricia	Pharmacie galénique
Mme POUGET Christelle (*)	Chimie organique, thérapeutique et pharmacie clinique
M. TOUBLET François-Xavier	Chimie organique, thérapeutique et pharmacie clinique
M. VIGNOLES Philippe (*)	Biophysique et mathématiques

(*) Titulaire de l'Habilitation à Diriger des Recherches (HDR)

Assistant Hospitalo-Universitaire

Mme MARCELLAUD Elodie	Chimie organique, thérapeutique et pharmacie clinique

Attachés Temporaires d'Enseignement et de Recherche

M. DELMON Cédric	Pharmacognosie, botanique et mycologie
Mme KENE MALAHA Angéladine	Épidémiologie, statistique, santé publique

Enseignants d'anglais

M. HEGARTY Andrew	Chargé de cours
Mme VERCELLIN Karen	Professeur certifié

Remerciements

À Mme. VIANA,

Je tiens à vous remercier pour votre soutien et vos conseils dans la rédaction de cette thèse et de l'honneur que vous me faites de présider ce Jury. Je vous remercie également pour les enseignements pratiques et théoriques que vous nous avez transmis tout au long du cursus universitaire. Ces enseignements me guident dans mes prises de décision aujourd'hui.

A M. NOISETTE,

Je tiens à te remercier tout particulièrement car sans toi ce projet n'aurait pas été possible. Ton soutien et tes conseils tout au long de l'année d'alternance et durant la rédaction de cette thèse m'ont permis de finaliser tous mes projets professionnels. Je te serai toujours reconnaissant pour tout ce que tu as fait durant ces 3 dernières années.

A Mme. LAVERDET,

Je vous remercie pour la participation à ce jury ainsi que pour vos enseignements durant ces années de formation à l'université de Limoges.

A mes collègues,

Je tiens à remercier le groupe Data Integrity Management et tout particulièrement Antoine, sans qui je n'aurais pas pu réaliser ce projet et qui m'a été d'une très grande aide pour la rédaction de cette thèse.

Je tiens à remercier toute l'équipe de BioS dans le cadre de ce projet et de la confiance qu'ils ont su m'accorder et de l'accueil qu'ils m'ont fait : Maxime, Isabelle, Benjamin, Steven, Béatrice et tant d'autres.

Je tiens également à remercier toute l'équipe de l'assurance qualité externe et opérationnelle qui m'ont soutenu au cours de cette dernière année : Rebecca, Maryline, Julie, Vesna, Isabelle, Arnaud, Laure, Sonia, Nathalie, Loetitia, Fiona et tant d'autres

Je tiens à remercier plus généralement toute l'équipe des Laboratoires Servier Industrie pour la confiance qu'ils m'ont accordée.

À ma famille,

Je remercie mes parents sans qui ces études n'auraient jamais pu être réalisables et qui ont toujours su me guider et m'accompagner tout au long de mes projets.

Je remercie également ma grand-mère qui m'a transmis les valeurs indispensables à la réalisation de notre profession et qui a su me guider dans mes choix.

Je remercie plus généralement toute ma famille pour tout le soutien que vous m'avez apporté tout au long de ces études, point culminant de 6 années d'apprentissage.

À mes amis,

Benjamin, Grégoire, que dire de notre trio qui a survécu à toutes ces années qui ont parfois été rudes mais durant lesquelles nous avons toujours su nous serrer les coudes les uns les autres et avancer ensemble. Votre amitié m'est précieuse et j'espère que nous resterons amis encore longtemps.

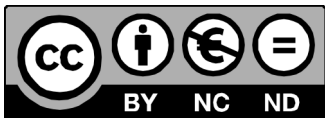
Je remercie tout le master RMQIS de Bordeaux, pour les moments passés. J'ai énormément appris à vos côtés.

Je remercie également toute la promotion de l'université de Limoges pour les projets réalisés durant toutes ces années. Le monde de la pharmacie est un petit monde. Nous nous reverrons sans aucun doute.

Merci à toi Floriane, qui a supporté que je reste assis au bureau pendant des heures et des heures, et qui m'a guidé et donné ton avis lorsque c'était nécessaire. Tu as été formidable, et je vais maintenant débarrasser le bureau de tous mes papiers, comme je te l'avais promis !

Enfin, je tiens à remercier toute l'équipe de la faculté de pharmacie de Limoges pour leurs enseignements qui m'ont permis de me réaliser pleinement dans mon métier de pharmacien.

Droits d’auteurs



Liste des abréviations

ALCOA : Attributable, Legible, Contemporaneous, Original, Accurate

ALCOA+ : Attributable, Legible, Contemporaneous, Original, Accurate, Available, Consistent, Enduring, Complete

AMM : Autorisation de Mise sur le Marché

ANSM : Agence Nationale de Sécurité du Médicament et des produits de santé

AQ : Assurance qualité

DI : Data integrity

DIM: Data Integrity Management

EBR: Electronic Batch Record

EMA : European Medicines Agency

EMS: Environmental Monitoring System

ERP: Enterprise Resource Planning

FDA : Food and Drug Administration

GMP: Good Manufacturing Practices

GDP : Good Distribution Practices

GxP : abréviation générale pour les recommandations et les réglementations de « bonnes pratiques ».

ICH : International Conference on Harmonisation

LIMS : Laboratory Information Management System

OMS : Organisation mondiale de la santé, agence spécialisée de l'Organisation des Nations unies pour la santé publique

PIC/S : Pharmaceutical Inspection Convention and Pharmaceutical Inspection Co-operation Scheme

QI : Qualification d'installation

QO : Qualification opérationnelle

QP : Qualification de performance

RACI : Responsible, Accountable, Consulted, Informed.

URS : User Requirement Specification

UTC : Coordinated Universal Time

ID : Identification

Table des matières

Table des illustrations

Table des tableaux

Introduction

La maitrise de la qualité est l'un des principes de gestion les plus importants pour toute organisation, quel que soit son secteur d'activité et particulièrement pour le secteur pharmaceutique. Le maintien de normes de qualité suffisantes sur les sites de production pharmaceutique permet de s'assurer que les médicaments produits répondent aux grands principes de qualité, de sécurité et d'efficacité du médicament. L'intégrité des données ou « *data integrity* » est une des exigences fondamentales car elle garantit que les décision prises par les industriels et les autorités réglementaires sont issues de données fiables. [1]

Les sites de fabrication pharmaceutique sont confrontés à de nombreux défis à l'ère du numérique. En effet, l'industrie 4.0 révolutionne la façon dont elle fabrique, améliore et distribue ses produits par la multiplication des systèmes informatisés, l'augmentation de nouvelles architectures des bases de données et par l'émergence du cloud. Cependant l'émergence de nouveaux textes sur l'intégrité des données ces 20 dernières années et l'augmentation des écarts constatés par les autorités réglementaires indiquent que la data integrity est l'une des principales problématiques auxquelles l'industrie pharmaceutique est actuellement confrontée. La Food And Drug Administration (FDA) a publié la première directive en 1963, et depuis lors, la FDA, l'Union européenne (UE), l'Organisation Mondiale de la santé (OMS) et la Medicines and Healthcare products Regulatory Agency (MHRA) ont publié de nombreuses autres directives. [2]

Le non-respect de ces exigences peut entraîner un nombre élevé de résultats non valides, et causer ainsi des prises de décisions inadaptées ayant un impact potentiel sur les patients, et entrainer des problématiques de post-commercialisation et de rappels de lots. Pour traiter les causes racines de ces non-conformités, une approche globale est nécessaire. Elle doit être intégrée de manière efficace dans le système de gestion de la qualité, et elle doit s'appliquer aux documents papiers et électroniques. [3]

Ainsi en quoi la maitrise de l'intégrité des données est-elle un pilier majeur pour la maitrise de la qualité sur un site de fabrication pharmaceutique ? Quelles stratégies adopter et comment implémenter un outil de maitrise des systèmes informatisés ? Afin de répondre à cette problématique, nous nous attacherons dans une première partie à définir ce qu'est l'intégrité des données et pourquoi elle est importante sur un site de production pharmaceutique en

introduisant ses grands principes. Puis dans une seconde partie nous nous intéresserons aux différents leviers qui existent afin de garantir l'intégrité de la donnée tout au long de son cycle de vie, avec une approche par gestion du risque. Enfin nous nous concentrerons sur un cas illustrant la mise en place d'une stratégie d'évaluation et de maitrise des systèmes informatisés sur un site de production pharmaceutique.

La maitrise des données sur un site de production pharmaceutique

1.1. Qu'est-ce que la data integrity ?

1.1.1. Glossaire

Certains termes inhérents à l'intégrité des données sont importants pour comprendre les stratégies exposées dans cette thèse d'exercice. Parmi les plus importants voici une liste des termes et leur explication associée ci-dessous tel que décrit dans le « *Guideline on data integrity* » de l'Organisation mondiale de la santé (OMS).

Données

> *« Le terme « données » couvre tous les enregistrements originaux et les copies conformes des enregistrements originaux, incluant les données source et les métadonnées ainsi que toutes les transformations et rapports ultérieurs de ces données, qui sont générées ou enregistrées au moment de l'activité BPx et qui permettent la reconstruction et l'évaluation entière et complète de l'activité BPx. Les données doivent être enregistrées de manière exacte au moment de l'activité par des moyens pérennes. Les données peuvent être contenues dans des enregistrements papier (comme les feuilles de travail et les cahiers de route (logbooks)), des enregistrements électroniques et des audit-trails, des photographies, des microfilms ou des microfiches, des fichiers audio ou vidéo ou tout autre support d'enregistrement de l'information relative aux activités BPx . » [4]*

Métadonnées

> *« Les métadonnées sont des données relatives aux données qui fournissent les informations contextuelles requises pour comprendre ces données. Ces métadonnées incluent les métadonnées structurelles et descriptives. De telles données décrivent la structure, les éléments de données, les interactions et les autres caractéristiques des données. Elles permettent également aux données d'être attribuables à un individu. Les métadonnées nécessaires pour évaluer la signification des données doivent être liées de manière sûre aux données et faire l'objet d'une revue adéquate. Par exemple, dans la pesée, le chiffre 8 n'a pas de sens sans les métadonnées, c'est-à-dire l'unité, mg. D'autres exemples de métadonnées incluent l'horodatage de l'activité, l'identifiant opérateur (ID) de la personne qui a effectué une activité, l'identifiant (ID) de l'instrument utilisé, les paramètres de processus, les fichiers de séquence, les audit-trails et les autres données nécessaires à la compréhension des données et à la reconstruction des activités. » [4]*

Copie :

« Une copie conforme (également appelée « vraie copie ») est une copie d'un enregistrement original de données qui a été vérifiée et certifiée pour attester qu'il s'agit d'une copie exacte et complète préservant l'intégralité du contenu et de la signification de l'enregistrement original, avec, dans le cas de données électroniques, toutes les métadonnées essentielles et le format d'enregistrement original. » [4]

Audit trail

« L'audit-trail (parfois appelé « piste d'audit ») est une forme de métadonnées qui contient une information associée aux actions concernant la création, la modification ou la suppression d'enregistrements BPx. L'audit-trail fournit un enregistrement sécurisé des détails du cycle de vie tels que la création, les ajouts, les suppressions ou les altérations d'information dans un enregistrement, soit papier soit électronique, sans masquer ou écraser l'enregistrement original. L'audit-trail facilite la reconstruction de l'historique de tels évènements relatifs à l'enregistrement, indépendamment de son support, incluant le « qui, quoi, quand et pourquoi » de l'action. Par exemple, dans un enregistrement papier, l'audit-trail d'une modification serait documenté par le fait de barrer d'une simple ligne la saisie originale tout en lui permettant de rester lisible et documenter par les initiales de la personne ayant effectué la modification, avec la date de la modification et la raison de la modification, comme requis pour étayer et justifier le changement. Pour des enregistrements électroniques, des audit-trails sécurisés, générés par l'ordinateur et horodatés doivent permettre la reconstruction du fil des évènements relatifs à la création, la modification et la suppression des données électroniques. Les audit-trails générés par ordinateur doivent conserver la saisie originale et documenter l'identification de l'utilisateur, l'horodatage de l'action, ainsi que la raison du changement, comme requis pour étayer et justifier l'action. Les audit-trails générés par ordinateur peuvent inclure des journaux d'évènements discrets, des fichiers d'historique, des requêtes ou des rapports de base de données ou d'autres mécanismes qui affichent des évènements relatifs au système informatisé, aux enregistrements électroniques spécifiques ou aux données spécifiques contenues dans l'enregistrement. » [4]

Système informatisé :

> *« Un système informatisé contrôle la performance d'un ou plusieurs processus automatisés et/ou fonctions automatisées. Cela inclut le matériel informatique, les logiciels, les dispositifs périphériques, les réseaux et la documentation, par exemple les manuels et les procédures opérationnelles (SOP), ainsi que le personnel interagissant avec le matériel et le logiciel, par exemple les utilisateurs et le personnel de support informatique. » [4]*

1.1.2. Définition

L'intégrité des données d'un site de production pharmaceutique est définie comme le degré auquel les données sont attribuables, lisibles, contemporaines, originales, précises, complètes, cohérentes, durables et disponibles tout au long du cycle de vie de la donnée. [5]

Elle permet aux sites de production et aux autorités réglementaires de prendre des décisions éclairées pour la certification d'un lot, l'autorisation de mise sur le marché d'une nouvelle spécialité pharmaceutique ou encore la mise en place d'actions correctives sur la base de données fiables. Il s'agit donc d'une exigence fondamentale du système de management de la qualité pharmaceutique qui s'applique aussi bien aux systèmes manuels (papier) qu'électroniques. L'intégrité des données ne peut être assurée qu'en l'absence de biais et se retrouve dans tous les aspects de la fabrication pharmaceutique. La violation de cette intégrité signifie l'introduction d'un biais délibéré ou accidentel, mais qui dans tous les cas est préjudiciable à la qualité, la sécurité et l'efficacité du médicament.[6]

1.1.3. Le cycle de vie de la donnée

1.1.3.1. Définition

Le "cycle de vie des données" fait référence à la manière dont les données sont générées, traitées, enregistrées, vérifiées, utilisées pour la prise de décision, archivées et finalement détruites à la fin de la période de conservation. Également appelé cycle de vie de l'information, il désigne l'ensemble de la période pendant laquelle les données existent dans le système. Ce cycle de vie englobe toutes les étapes par lesquelles passe une donnée pharmaceutique. La Figure 1 ci-dessous illustre les grandes étapes du cycle de vie des données tel que décrit dans le *Guidance on good manufacturing practice and good distribution practice: Questions and answers* de l'European Medical Agency (EMA) paru en 2018 sur la maitrise de l'intégrité des données. [4]

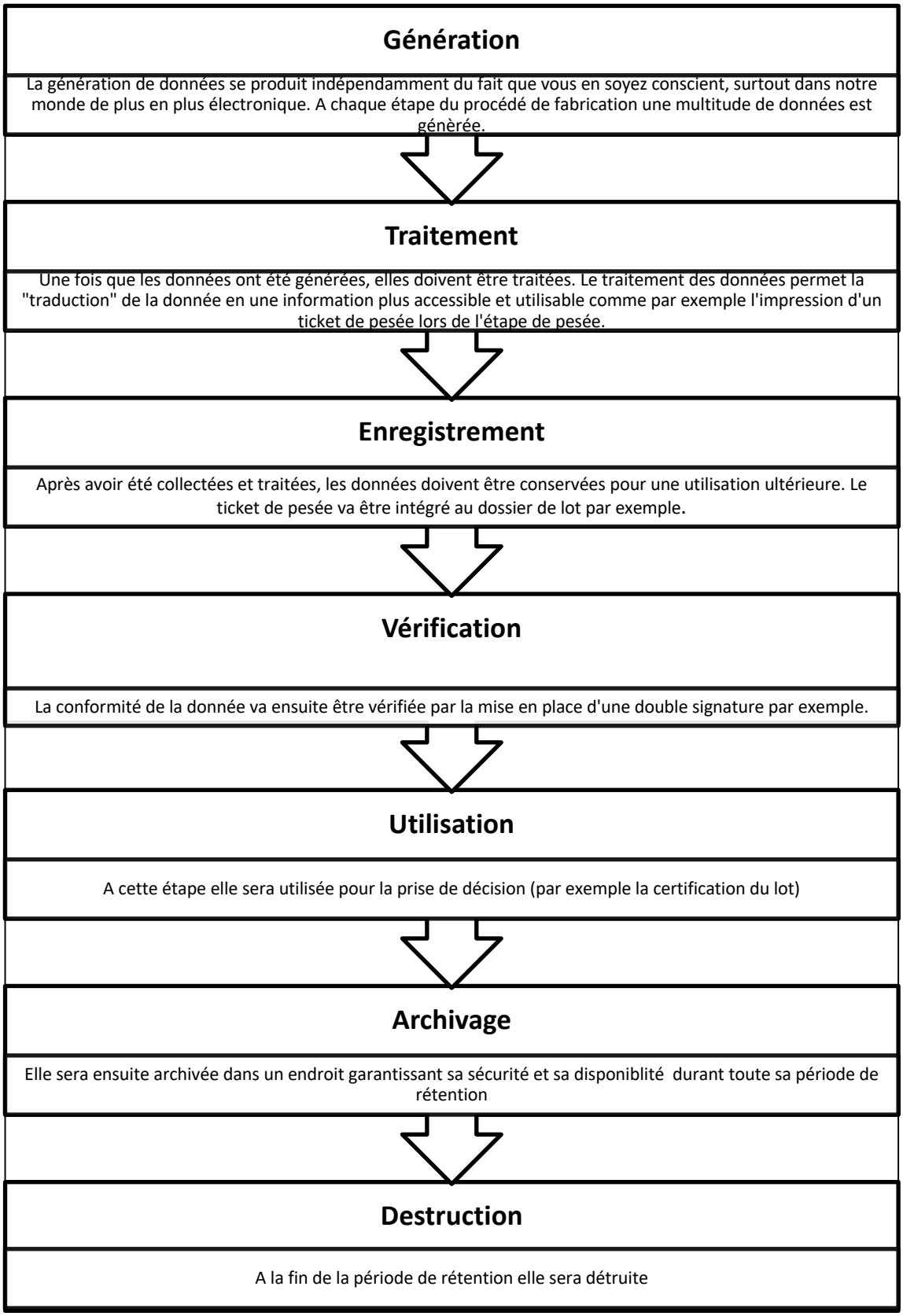


Figure 1 : le cycle de vie de la donnée selon l'EMA [4]

1.1.3.2. Une multitude de frontières entre la génération et la destruction de la donnée

Les données pharmaceutiques relatives à un produit ou à un processus peuvent également traverser plusieurs frontières au cours de leurs cycles de vie. Il peut s'agir du transfert de données entre des systèmes papiers et des systèmes informatiques (par exemple entre les systèmes informatisés et les dossiers de lots papiers), ou entre différentes frontières organisationnelles, tant internes (par exemple entre la production, le service contrôle qualité et l'assurance qualité), qu'externes (par exemple les valeurs des quantités expédiées et réceptionnées entre le site de production et le site de distribution). [1]

La Figure 2 ci-dessous illustre la multitude de frontières qu'une donnée peut traverser au sein d'un site de production pharamceutique.

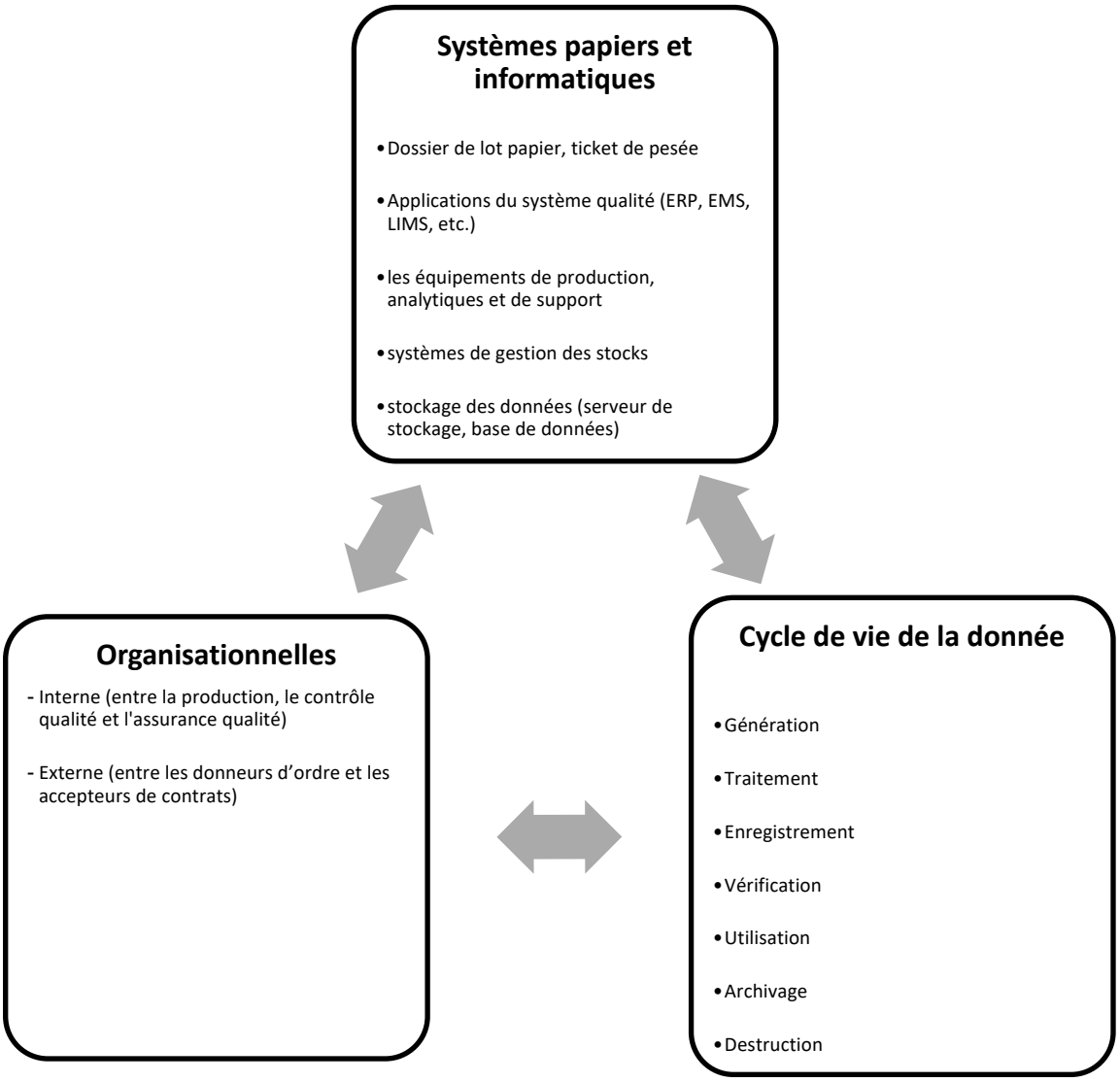


Figure 2 : les différentes frontières traversées par les données d'un site de production pharmaceutique

Une bonne connaissance du cycle de vie de ses données et des différentes interfaces possibles est un prérequis à la mise en place d'un système de maitrise des données. Par conséquent, il est primordial de déterminer le qui, le quoi, le où et le comment de la donnée à chaque étape du cycle de vie des données. Ces contrôles doivent être définis, communiqués et compris dans l'ensemble de l'organisation pour garantir le respect des exigences de conformité en matière d'intégrité des données.

1.1.4. Les 9 principes ALCOA+

ALCOA est un acronyme utilisé pour attribuable, lisible, contemporain, original et exact. Il a été introduit par la Food and Drug Administration dans les années 1990 et est toujours utilisé par la FDA. Aujourd'hui, il est utilisé par les autorités réglementaires comme cadre pour assurer l'intégrité des données et est essentiel pour garantir les bonnes pratiques documentaires y compris les Bonnes Pratiques de Fabrication au travers du « Q&A data integrity » de l'European Medicines Agency (EMA) publié en 2016. Il s'applique aux données papiers et électroniques. Les principes illustrés par le « + » ont été introduits plus tardivement à l'ALCOA en 2010 et font référence à complète, cohérente, durable et disponible. [7]

La Figure 3 ci-dessous représente ces 9 principes :

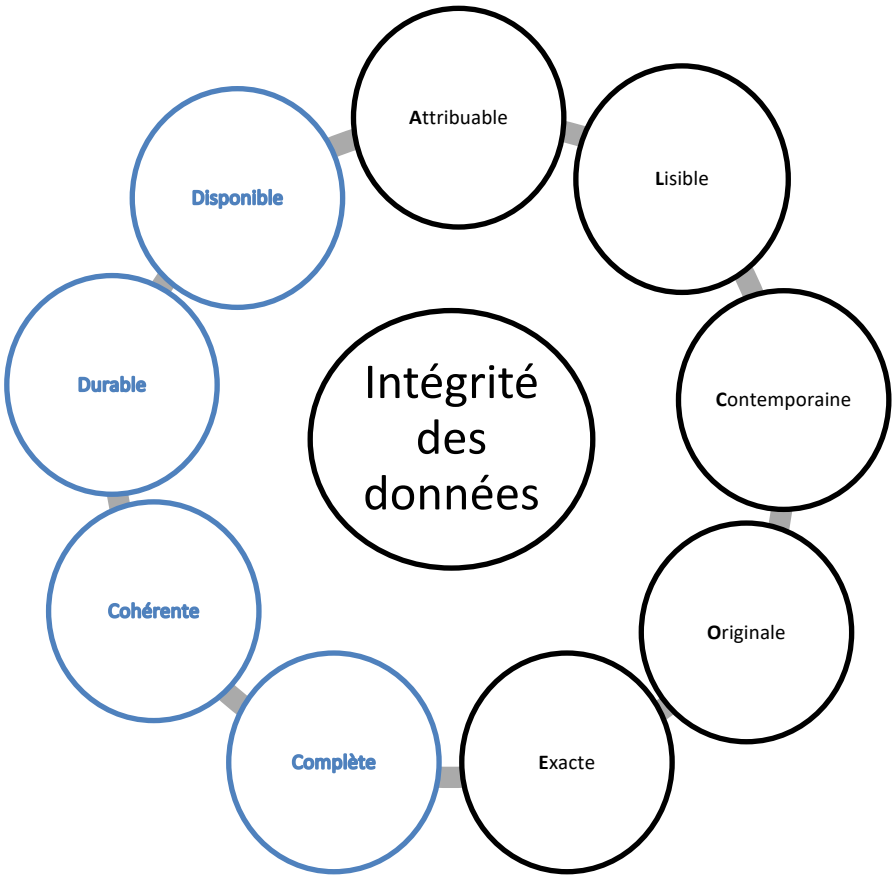


Figure 3 : les 9 principes de maitrise de l'intégrité des données ALCOA+

1.1.4.1. Attribuable (*Attributable*)

Lorsqu'une donnée est générée, l'identité de la personne ou du système qui a collecté ou généré cette donnée doit être enregistrée. [7]

Les données doivent être attribuables, c'est-à-dire pouvoir être rattachées à un individu et à un système. Dans les documents papiers, cela peut se faire par l'utilisation d'initiales, d'une signature manuscrite complète ou d'un sceau personnel. Dans les documents électroniques, cela peut se faire par l'utilisation d'identifiants uniques qui lient l'utilisateur aux actions de création, de modification ou de suppression des données, ou de signatures électroniques uniques, biométriques ou non. Une piste d'audit qui saisit l'identification de l'utilisateur, la date et l'heure et la signature électronique doit être liée de manière sûre et permanente au document signé.

Les éléments à maitriser pour s'assurer qu'une donnée est attribuable sont décrits dans la Figure 4 ci-dessous :

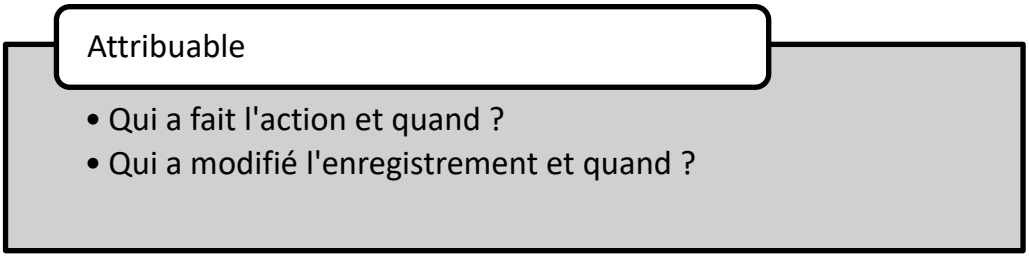


Figure 4 : une donnée attribuable

Les bonnes pratiques à appliquer sur un site de production pharmaceutique concernant ce principe peuvent être les suivantes :

- pouvoir retrouver la date et l'auteur (ou le créateur),
- créer des enregistrements qui garantissent la traçabilité du travail effectué,
- utiliser des signatures et des sceaux enregistrés pour les enregistrements.

1.1.4.2. Lisible (*Legible*)

Les données doivent pouvoir être lues et comprises des années, voire des décennies, après leur enregistrement. Lorsqu'elles sont manuscrites, il est donc important d'appliquer les bonnes pratiques documentaires décrites dans les Bonnes Pratiques de fabrication afin de ne pas reporter des données manuscrites illisibles, car il pourrait être difficile de les déchiffrer à

l'avenir sans obtenir des précisions de l'auteur des données, une personne qui n'est peut-être plus disponible. [7]

Cependant, la lisibilité des données ne se limite pas aux données manuscrites. Lorsque les données sont créées, générées ou mises à jour électroniquement, il est essentiel qu'elles puissent être lues quel que soit le format dans lequel elles ont été enregistrés. Avec la digitalisation croissante de l'industrie pharmaceutique et la migration des systèmes, maintenir la lisibilité des données électroniques tout au long de leur cycle de vie quels que soient les changements rencontrés reste un paramètre important à prendre en compte pour assurer la lisibilité d'une donnée. [8]

L'utilisation d'un langage cohérent, direct et universel dans toute l'organisation, quelle que soit la localité, est la meilleure approche.

Les éléments à maitriser pour s'assurer qu'une donnée est lisible sont décrits dans la Figure 5 ci-dessous :

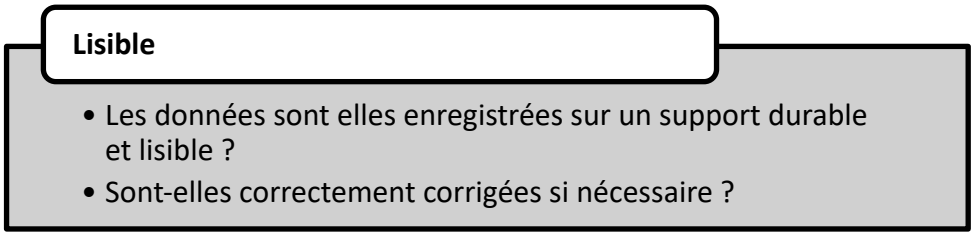


Figure 5 : une donnée lisible

Les bonnes pratiques à appliquer sur un site de production pharmaceutique concernant ce principe peuvent être les suivantes :

- faire des enregistrements de manière lisible et précise,
- faire des enregistrements qui peuvent être compris correctement et facilement.

1.1.4.3. Contemporaine (*Contemporaneous*)

Il est essentiel que les individus ou les systèmes enregistrent des données chaque fois qu'une activité ou une action a lieu. En général, l'enregistrement contemporain des données est davantage un point qui concerne la saisie manuelle des données. L'objectif principal est d'éviter la pratique consistant à créer ou à mettre à jour des données à un moment donné dans le futur. Lorsque les données sont enregistrées après un événement ou une action, des erreurs peuvent

se produire, c'est-à-dire que des éléments peuvent être oubliés, des parties peuvent être omises et des informations peuvent être enregistrées de manière inexacte. [7]

L'utilisation d'un support pour enregistrer une activité au nom d'un autre opérateur ne doit être envisagée qu'à titre exceptionnel et ne doit avoir lieu que lorsque l'enregistrement met le produit ou l'opérateur en danger, comme la documentation des interventions en ligne par des opérateurs de la zone aseptique. L'utilisation d'un support est donc envisageable mais elle doit être justifiée et documentée.

Les éléments à maitriser pour s'assurer qu'une donnée est contemporaine sont décrits dans la Figure 6 ci-dessous :

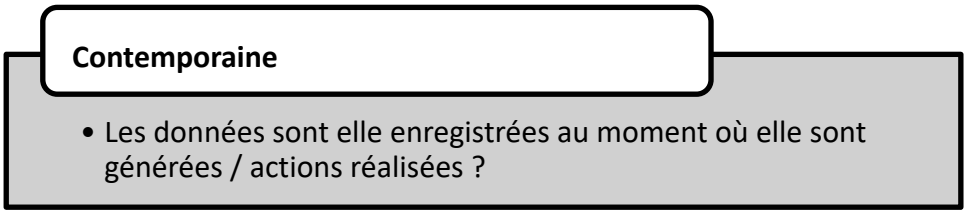


Figure 6 : une donnée contemporaine

Les bonnes pratiques à appliquer sur un site de production pharmaceutique concernant ce principe peuvent être les suivantes :

- effectuer les enregistrements en même temps que l'opération. Par exemple lorsqu'un échantillon est pesé ou préparé, toutes les données et métadonnées relatives à l'échantillon (date, heure, nom de la personne, numéro d'identification de la balance) doivent être enregistrées à ce moment-là et non avant ou à un stade ultérieur,
- s'assurer que les horloges des systèmes soient précises et que les fuseaux horaires soient enregistrés lors de l'utilisation de systèmes informatisés.

1.1.4.4. Originale (*Original*)

Pour s'assurer de la fiabilité d'une donnée il est nécessaire de conserver les enregistrements et ces enregistrements doivent être des originaux plutôt que des copies ou des transcriptions qu'ils soient sur papier ou sur un système informatisé.

Là encore, cela s'applique surtout aux données manuscrites. En effet, il est important d'enregistrer la donnée directement sur le support auquel elle sera destinée. Par exemple dans le cas où un document tiers, comme une feuille volante, est utilisé, il devra être conservé en tant que donnée brute car cela pourrait être source d'erreurs et de falsifications si il ne l'était pas. [7]

L’enregistrement original des données doit constituer l'enregistrement principal, que ce soit sur papier ou sur un système numérique. Dans le cas de données enregistrées numériquement, il est également important que des mesures techniques et organisationnelles soient mises en place pour garantir que l'enregistrement original des données ne puisse être modifié ou supprimé.

Toute analyse, tout rapport ou tout calcul basé sur des données collectées, générées ou mises à jour doit pouvoir être retracé jusqu'à la source originale.

En outre, les copies d'un enregistrement original doivent être formellement vérifiées comme étant des copies conformes, et elles doivent pouvoir être distinguées de l'original. L’OMS définit une copie certifiée comme une copie d'un enregistrement original de données qui préserve l'intégralité du contenu et de la signification de l'enregistrement original. La version originale des données doit également être préservée, même si des copies existent. [4]

Les éléments à maitriser pour s’assurer qu’une donnée est originale sont décrits dans la Figure 7 ci-dessous :

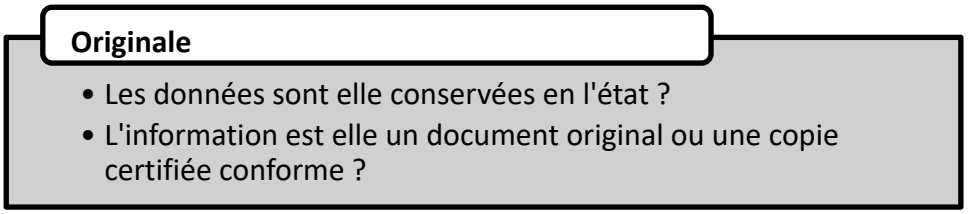


Figure 7 : une donnée originale

Les bonnes pratiques à appliquer sur un site de production pharmaceutiques concernant ce principe peuvent être les suivantes :

- ne pas inscrire les résultats de la mise en œuvre dans des formulaires d'enregistrement autres que ceux officiellement approuvés,
- ne pas utiliser de notes ou de papier pour mémoire dans les dossiers,
- ne pas utiliser de carnets personnels pour enregistrer des données ou faire des calculs. [9]

1.1.4.5. Exacte (*Accurate*)

L’exactitude des données fait référence à des enregistrements sans erreur qui peuvent être utilisés comme une source d'information fiable. Dans la gestion des données, l’exactitude des données est le premier et le plus important composant/standard du cadre de qualité des données. Dans son ouvrage « *Data Quality : The Accuracy Dimension* », Jack Olson explique que la forme et le contenu sont deux des caractéristiques les plus importantes de l'exactitude

des données. Il ne doit pas y avoir de modification des informations originales qui entraînerait la perte de ces informations. [10]

Si des modifications sont nécessaires, elles doivent être documentées de manière qu'il soit possible de se référer aux informations originales. Rien ne doit être supprimé, bloqué ou effacé.

Les éléments à maitriser pour s'assurer qu'une donnée est exacte sont décrits dans la Figure 8 ci-dessous :

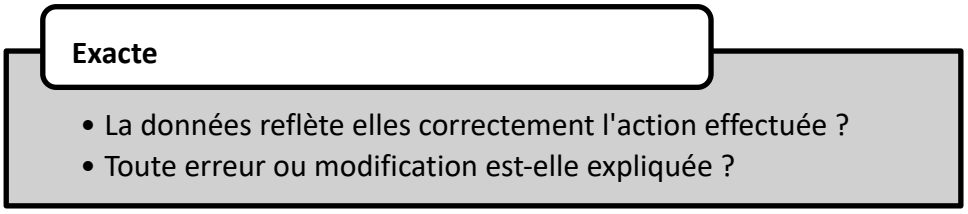


Figure 8 : une donnée exacte

Les bonnes pratiques à appliquer sur un site de production pharmaceutique concernant ce principe peuvent être les suivantes :

- Préparer les procédures écrites, effectuer les opérations conformément à celles-ci et établir des enregistrements,
- Rejeter strictement les pratiques malhonnêtes liées aux documents et aux enregistrements (falsification, altération, etc.),
- Les équipements de mesure doivent être régulièrement étalonnés dans le cadre de ce processus.

1.1.4.6. Cohérente (*Consistent*)

La chronologie des données doit être cohérente c'est-à-dire qu'elles ont une date et une heure qui correspondent à la séquence attendue. [7]

Les éléments à maitriser pour s'assurer qu'une donnée est cohérente sont décrits dans la Figure 9 ci-dessous :

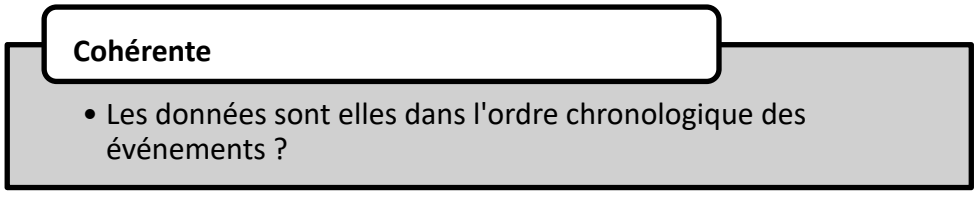


Figure 9 : une donnée cohérente

Les bonnes pratiques à appliquer sur un site de production pharmaceutique concernant ce principe sont les suivantes :

- S'assurer que les enregistrements (étapes de fabrication, déviations, saisie des données) sont horodatés et respectent bien l'ordre chronologique attendu.

1.1.4.7. Complete (*Complete*)

La complétude des données fait référence à l'exhaustivité des données. Il ne doit y avoir aucune lacune ou information manquante pour que les données soient complètes car l'utilisation d'une donnée incomplète peut entrainer des conclusions erronées. [7]

Les données ne sont pas complètes si toutes les données disponibles, y compris les métadonnées, ne sont pas recueillies et stockées correctement. Les données enregistrées sur des supports différents, et les interruptions pendant l'enregistrement ou l'archivage peuvent conduire à des données/métadonnées brutes manquantes.

Les éléments à maitriser pour s'assurer qu'une donnée est complète sont décrits dans la Figure 10 ci-dessous :

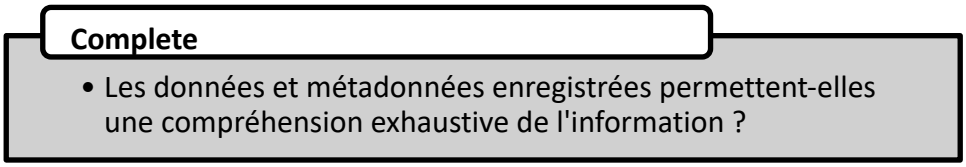


Figure 10 : une donnée complète

Les bonnes pratiques à appliquer sur un site de production pharmaceutique concernant ce principe sont les suivantes :

- transférer ou archiver les métadonnées (y compris les pistes d'audit et les signatures électroniques) avec les documents électroniques lorsque des documents électroniques sont intégrés d'un système informatisé à un autre système (c'est-à-dire lorsque les documents ne sont pas conservés dans le système d'origine),
- s'assurer que l'impression contient les données complètes avec la précision requise lorsque les données électroniques doivent être imprimées sur papier ou en PDF. [9]

1.1.4.8. Endurante (*Enduring*)

Bien que cet aspect soit abordé dans un principe précédent, ce principe de l'ALCOA+ met l'accent sur la nécessité de garantir la disponibilité des données longtemps après leur enregistrement - des décennies dans certaines situations ; à minima durant toute la période de rétention prévue.[11]

Les risques comprennent la diminution de la lisibilité de certains supports tels que les documents manuscrits. En ce qui concerne les documents électroniques, la durabilité fait référence au type de stockage utilisé. Les données et les enregistrements doivent être stockés de manière appropriée, dans des conditions adéquates pour qu'ils soient consultables tout au long de leur cycle de vie. Une solution de stockage électronique dans le « cloud », par exemple, peut ne pas être durable si un grand nombre de personnes y ont accès et peuvent modifier les données. De la même manière un stockage physique non sécurisé des données manuscrites peut être une source importante de perte d'endurance des données.

Les éléments à maitriser pour s'assurer qu'une donnée est endurante sont décrits dans la Figure 11 ci-dessous :

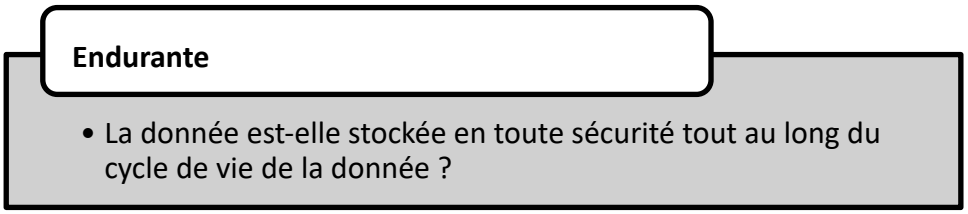


Figure 11 : une donnée endurante

Les bonnes pratiques à appliquer sur un site de production pharmaceutique concernant ce principe peuvent être les suivantes :

- constituer des enregistrements papier à l'encre permanente,
- maitriser le stockage des documents électroniques par des processus sécurisés et validés,
- maitriser le stockage des documents manuscrits par des processus validés et limiter l'accès,
- conserver les documents intacts pendant toute la durée du délai de conservation, en fonction du cycle de vie de ces documents.

1.1.4.9. Disponible (*Available*)

La disponibilité des données est le fait pour une organisation de s'assurer que toutes les données liées à son activité sont disponibles dans un temps raisonnable pour l'organisation, les partenaires ou autorités réglementaires à tout moment du cycle de vie de la donnée. Les données doivent non seulement exister, mais aussi être accessibles. Le moyen le plus efficace d'y parvenir est l'enregistrement électronique des données.

Les éléments à maitriser pour s'assurer qu'une donnée est disponible sont décrits dans la Figure 12 ci-dessous :

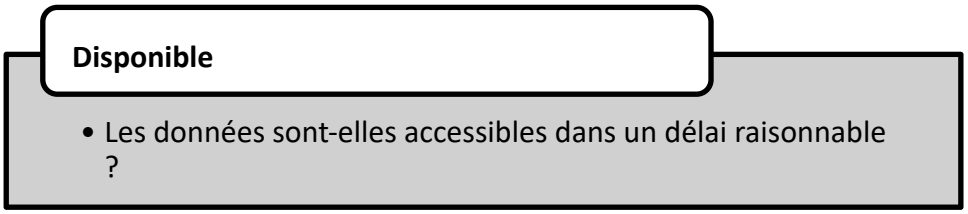


Figure 12 : une donnée disponible

Les bonnes pratiques à appliquer sur un site de production pharmaceutique concernant ce principe peuvent être les suivantes :

- conserver les dossiers de lot et les autres documents justifiant de la qualité du lot de manière sûre et fiable, de façon à pouvoir les retrouver dans un délai déterminé et à permettre une reconstitution complète de l'historique du lot,
- maitriser la mise à jour du système si un système informatisé est utilisé pour le stockage des données.

Les autorités s'accordent donc pour dire que l'intégrité des données est respectée lorsque les données pharmaceutiques sont attribuables, lisibles, contemporaines, originales, exactes, complètes, cohérentes, durables et disponibles tout au long du cycle de vie de la donnée et quelles que soient les frontières traversées. Mais pourquoi la data integrity est-elle importante et quels impacts une dérive peut-elle avoir sur la qualité, la sécurité et l'efficacité du médicament ? Nous allons donc nous intéresser dans la partie 1.2 ci-dessous à l'importance de la maitrise de l'intégrité des données sur un site de production pharmaceutique.

1.2. Pourquoi l'intégrité des données est-elle importante ?

1.2.1. Un pré requis à la prise de décision

La raison pour laquelle les autorités réglementaires se concentrent sur la maitrise des données en inspection ces 20 dernières années est le fait que les fabricants s'appuient sur des données claires et précises non seulement pour garantir la sécurité et la traçabilité des processus et des produits, mais aussi pour identifier les points d'inefficacité de leurs opérations et permettre à la direction de prendre des mesures correctives adaptées au risque pour le patient. [9]

La façon dont les données critiques sont générées a continué d'évoluer parallèlement au développement continu des technologies et de la digitalisation de l'industrie pharmaceutique, telles que l'utilisation croissante de la saisie électronique des données, l'automatisation des systèmes et l'utilisation des technologies à distance, ainsi que la complexité accrue des chaînes d'approvisionnement et des méthodes de travail, par exemple, via des sociétés extérieures. [8] Les systèmes destinés à soutenir ces méthodes de travail peuvent aller :

- de processus manuels avec des enregistrements uniquement sur papier,
- en passant par des systèmes hybrides, structure majoritairement rencontrée dans l'industrie pharmaceutique aujourd'hui,
- à l'utilisation de systèmes entièrement informatisés.

Cela rationnalise également la prise de bonnes décisions dans tous les domaines, comme la planification, les prévisions, la budgétisation. Si le site de production dispose d'une collecte de données fiables, un stock suffisant sera assuré pour satisfaire la demande des patients. La précision des données peut donc servir tous les secteurs d'un site de production pharmaceutique et pas uniquement la qualité.

1.2.2. Les exigences des autorités réglementaires

En réponse à l'utilisation croissante des systèmes informatisés, de nombreux référentiels et lignes directrices ont été publiés au cours des dernières années en matière d'intégrité des données afin de guider les laboratoires pharmaceutiques tels que :

- le « 21 CFR part 11 : Electronic Records; Electronic Signatures » de la Food and Drug Administration (FDA) publié en 2003 [12]. La FDA est chargée de protéger la santé publique en garantissant l'innocuité, l'efficacité et la sécurité des médicaments à usage humain et vétérinaire aux Etats-Unis. Ce document fournit des bonnes pratiques aux

industriels qui ont choisi de conserver et soumettre les enregistrements sous format électronique.

- les « Good Manufacturing Practices » de l'EMA : l'annexe 11 révisée en 2011 [11], le chapitre 4 publié en 2011 [13], le chapitre 5 publié en 2014 [14] et le chapitre 6 publié en 2014 [15] . La mission de l'EMA est de favoriser l'excellence scientifique dans l'évaluation et la surveillance des médicaments, au bénéfice de la santé publique et animale dans l'Union européenne (UE). Ces documents sont des bonnes pratiques régissant les médicaments dans l'Union européenne et contiennent des conseils pour l'interprétation des principes et des lignes directrices de bonnes pratiques de fabrication des médicaments à usage humain et vétérinaire établis dans les directives de la Commission 91/356/CEE, modifiée par les directives 2003/94/CE, et 91/412/CEE respectivement.
- le « Q&A data integrity » de l'Agence européenne des médicaments (EMA) publié en 2016 [1]. L'EMA fournit des réponses sous forme de questions et réponses (Q&A) aux problématiques fréquemment rencontrées sur les bonnes pratiques de fabrication (BPF) et les bonnes pratiques de distribution (BPD), telles que discutées et approuvées par le groupe de travail des inspecteurs BPF/BDP. Ces questions/réponses fournissent une interprétation supplémentaire des directives BPF de l'Union européenne (UE) et des directives BPD publiées par la Commission européenne. Le groupe de travail a préparé ce Q&A afin de faciliter l'implémentation de bonnes pratiques d'intégrité des données dans l'industrie pharmaceutique dans l'union européenne.
- le « GXP Data Integrity Guidance and Definitions » de la Medicines & Healthcare products Regulatory Agency (MHRA) publié en 2018 [16]. L'Agence de réglementation des médicaments et des produits de santé (*Medicines and Healthcare products Regulatory Agency*) réglemente les médicaments, les dispositifs médicaux et les médicaments dérivés du sang destinés à la transfusion au Royaume-Uni. Ce document fournit des conseils sur les attentes en matière d'intégrité des données qui doivent être prises en compte par les organisations impliquées dans tout aspect du cycle de vie pharmaceutique par la MHRA.
- le « Guideline on data integrity » de l'Organisation Mondiale de la Santé (OMS) publié en 2020 [4]. L'OMS est l'institution des Nations Unies qui met en relation les nations, les partenaires et les personnes pour promouvoir la santé, assurer la sécurité dans le

monde et servir les personnes vulnérables, afin que chacun, partout, puisse atteindre le niveau de santé le plus élevé. Avec cette ligne directrice, l'OMS tente d'harmoniser les autres lignes directrices internationales sur l'intégrité des données, notamment le "MHRA GxP data integrity guidance and definitions,", le "FDA guidance for industry Data integrity and compliance with CGMP - questions and answers" et le "PIC/S Good practices for data management and integrity in GMP/GDP environments". [17]

- les « Good practices for data management and integrity in regulated GMP/GDP environments » du Pharmaceutical Inspection Co-operation Scheme (PIC/S) publié en 2021 [18]. Le PIC/S vise à harmoniser les procédures d'inspection dans le monde entier en développant des normes communes dans le domaine des BPF et en offrant des possibilités de formation aux inspecteurs. Il vise également à faciliter la coopération et le travail en réseau entre les autorités compétentes et les organisations régionales et internationales, augmentant ainsi la confiance mutuelle. Les « Good practices for data management and integrity in regulated GMP/GDP environments" fournissent des conseils aux services d'inspection en ce qui concerne la bonne gestion des données et la conduite des inspections.
- la seconde version du « GAMP 5: A Risk-Based Approach to Compliant GxP Computerized Systems » de l'International Society for Pharmaceutical Engineering publié en 2022 . L'International Society for Pharmaceutical Engineering est une association à but non lucratif qui sert ses membres en menant des avancées scientifiques, techniques et réglementaires tout au long du cycle de vie pharmaceutique. Le GAMP 5 vise à fournir un cadre rentable de bonnes pratiques pour garantir que les systèmes informatisés sont efficaces et de haute qualité, adaptés à l'usage prévu et conformes aux réglementations applicables. Il s'agit de lignes directrices et non d'une exigence réglementaire. Il n'est donc pas obligatoire de suivre cette méthodologie. Cependant, le cadre décrit dans cette ligne directrice fournit une approche complète de la validation des systèmes informatiques qui est généralement acceptée dans l'industrie. En outre, l'approche préconisée, fondée sur le risque, est conforme à l'application des règlements de l'EMA et de la FDA régissant la validation des systèmes informatiques, respectivement l'annexe 11 et le 21 CFR Part 11. En plus d'être un excellent outil pour aider à répondre aux exigences réglementaires, le GAMP 5 est également utile pour déterminer l'effort à apporter à la validation des systèmes. L'approche basée sur le risque permet de concentrer les efforts de test sur les systèmes à haut risque tout en aidant à

fournir une justification pour effectuer des tests réduits sur les systèmes à faible risque. En conséquence, les tests peuvent être adaptés au système en cours de validation. Cela rend l'effort de validation plus efficace tout en démontrant que le système fonctionne comme prévu.

Le Tableau 1 ci-dessous présente les principes ALCOA+ et leur correspondance avec les différents chapitres des Bonnes Pratiques de Fabrication de l'European Medicines Agency (EMA) :

Tableau 1 : Principes d'ALCOA+ dans les Good Manufacturing Pratices (GMP)[1]

	Médicaments Chapitre 4/6	**Principes actifs** Chapitre 5/6	**Système informatisé** LD 11
Attribuable	[4.20], [4.21], [4.29]	[6.14], [6.18], [6.52]	[2], [12.4], [15]
Lisible	[4.1], [4.2], [4.7], [4.8], [4.9], [4.10]	[5.43] [6.11], [6.14], [6.15], [6.50]	[7.1], [9], [10], [17]
Contemporaine	[4.8]	[6.14]	[12.4], [14]
Originale	[4.9], [4.27],	[6.14], [6.15], [6.16]	[8.2], [9]
Exacte	[4.1], [6.17]	[5.40], [5.45], [6.6]	[5], [6], [10], [11]
Cohérente	[4.4],	[6.41], [6.52]	[12.4],[14]
Complete	[4.2], [4.8], [4.9], [4.12], [4.13 -> 4.21], [6.3]	[6.11], [6.14], [6.17], [6.52], [6.61]	[8.2], [9]
Endurante	[4.1], [4.7], [4.10], [4.11], [6.8]	[6.12]	[7.1], [7.2], [12], [17]
Disponible	[4.1], [4.11], [4.12], [4.28] [4.30], [6.8], [6.10]	[6.12], [6.13] , [6.15], [6.16],	[3.4], [9], [17]

L'intégrité des données est donc une composante qui est complétement intégrée à la réglementation internationale. Nous allons donc maintenant nous intéresser à une série de manquements remontés par la FDA et l'ANSM afin de comprendre l'importance de maitriser la data integrity sur un site de production pharmaceutique.

1.2.3. Le scandale de Vitarine Pharmaceuticals

En 1989, un scandale majeur a éclaté concernant les procédures utilisées par la FDA pour accepter une demande de mise sur le marché des médicaments génériques. Des accusations de corruption sont apparues pour la première fois en 1988, au cours d'une vaste enquête du Congrès sur la Food and Drug Administration (FDA). L'enquête a montré que plusieurs fabricants avaient falsifié les données soumises aux autorités pour obtenir l'autorisation de la FDA.[20]

Dans les années 80, le Dyazide, un diurétique indiqué dans le traitement de l'hypertension artérielle était l'un des médicaments les plus prescrits aux États-Unis et était sur le marché depuis 1965. En 1980, ses brevets ont expiré mais des difficultés sont apparues pour démontrer

le principe de bioéquivalence entre le princeps et le générique car la formulation du Dyazide donnait lieu à une variabilité importante entre les lots. [21]

La société Vitarine Pharmaceuticals de New York, était une des compagnies qui souhaitait mettre sur le marché une version générique du Dyazide. [21]

Le Vice-Président du département de recherche de Vitarine Pharmaceutical, Dr. Steve Colton, a été condamné par le tribunal fédéral de district de Baltimore pour avoir fait de fausses déclarations qui ont amené Vitarine à soumettre des résultats de tests pour le Dyazide. [22]

La seule autre société qui avait reçu l'autorisation de mise sur le marché pour un générique du Dyazide a également retiré son médicament du marché et a été condamnée pour des charges similaires.[21]

En 1989, la FDA a ainsi enquêté sur plusieurs fabricants pour des irrégularités similaires. Des dizaines de médicaments ont finalement été suspendus ou rappelés par les fabricants. [23]

1.2.4. Novartis et sa demande d'AMM du Zolgensma

Plus récemment en 2019, Novartis, groupe pharmaceutique suisse qui a été créé en 1996 par fusion de Ciba-Geigy et Sandoz et dont le siège social est à Bâle, en Suisse, a également été accusé par la FDA d'avoir manipulé des données relatives à sa demande d'AMM de Zolgensma (thérapie génique) et pour avoir tardé à alerter la FDA. En effet l'alerte à la FDA a été donnée après l'acceptation de mise sur le marché du médicament. [24]

Dans son rapport d'inspection, la FDA a démontré de multiples cas de " manipulation potentielle des données " lors de l'examen des dossiers. Par exemple, l'examen des rapports de non-conformité a révélé des " formulaires d'essai non remplis au moment de la génération et de l'approbation du CoA " et des formulaires avec des mentions de dates et heures incohérentes. Au total, cinq observations ont été répertoriées sur le formulaire 483 de la FDA concernant le manque de documentation, le manque d'indépendance de l'unité de qualité, le manque de respect des procédures établies et le manque d'enregistrement des données en temps réel. [25]

Dans sa réponse de 59 pages au formulaire 483 de la FDA, Novartis a affirmé qu'elle n'avait pas communiqué les problèmes d'intégrité des données à la FDA car une enquête interne était en cours. L'équipe d'enquête externe mandatée aurait passé quelque 2 000 heures à examiner des milliers de documents manuscrits et électroniques concernant les essais cliniques et à les comparer aux données d'entrée de centaines de feuilles de calcul. Des experts techniques ont

dû évaluer l'impact des divergences entre les études, les décisions de libération des lots et les données cliniques.[26]

Selon ces investigations ces problèmes de falsification des données n'ont heureusement eu aucun impact sur la sécurité des patients ou sur l'efficacité et la qualité du produit. Les responsables de la FDA ont réagi fortement à la communication tardive en envoyant un message non seulement à Novartis mais aussi au secteur en plein essor de la thérapie cellulaire et génique : « *si l'agence est prête à approuver rapidement de telles thérapies sur la base de preuves limitées, elle ne tolérera pas que ces preuves soient non intègres* ».[24]

Novartis s'est engagée à informer dorénavant l'agence dans les cinq jours ouvrables suivant la réception par son département qualité de toute allégation crédible liée à l'intégrité des données ayant un impact sur une demande d'autorisation de mise sur le marché de produits biologiques.[26]

Une mauvaise intégrité des données peut donc sérieusement compromettre la confiance entre les autorités réglementaires et l'industriel, en particulier lorsqu'elle soulève des questions concernant l'impact sur les patients.

1.2.5. Exemples de warning letters de la FDA

1.2.5.1. Maitrise des principes d'ALCOA chez un fabricant de matières premières à usage pharmaceutique

Cet écart impliquait un fabricant de matière première à usage pharmaceutique. Il s'agit d'un exemple récurrent qui porte sur 3 des 8 caractéristiques d'ALCOA+. L'écart mentionne que l'entreprise n'a pas tenu de registres de contrôle de laboratoire adéquats comprenant des données complètes et précises sur les tests effectués pour garantir la conformité aux spécifications et aux normes, et qu'ils n'ont pas non plus enregistré les activités au moment de leur exécution.[27]

En effet, il est mentionné que le personnel du laboratoire de contrôle analytique a antidaté l'approbation d'une feuille de travail interne décrivant la préparation des milieux de culture microbiologiques après que les milieux aient été utilisés.

De plus des résultats non conformes ont été modifiés en résultats conformes sur la base des résultats des nouveaux tests. Cependant, ils n'ont pas été en mesure de fournir des données justifiant les nouveaux tests. Et enfin, les dossiers d'analyse des échantillons étaient incomplets car ils ne contenaient pas d'informations sur la taille des échantillons, ni de référence aux réactifs et aux instruments utilisés.

Sans dossiers d'analyse complets, contemporains et précis, ils ne pouvaient donc pas évaluer adéquatement la qualité des excipients fabriqués et prendre des décisions appropriées concernant la libération des lots ou identifier l'impact potentiel de mauvaises pratiques de fabrication sur la qualité des excipients et *in fine* l'impact sur les patients.

1.2.5.2. Maitrise des systèmes informatisés dans un laboratoire de contrôle

Cet écart démontre cette fois ci une mauvaise maitrise des systèmes informatisés d'un laboratoire de contrôle. Selon la FDA, il s'agit de l'un des écarts les plus récurrents en matière de data integrity. [28]

Le laboratoire n'a pas exercé les contrôles appropriés sur les systèmes informatiques pour s'assurer que seul le personnel autorisé effectuait des changements dans les recettes de production et de contrôle, ou d'autres registres.

Les systèmes qui généraient les résultats des produits pharmaceutiques manquaient de contrôles appropriés. Il n'y avait aucune assurance que les systèmes disposaient des contrôles appropriés pour empêcher :

- la suppression des données,
- la traçabilité de toutes les modifications apportées aux données. Par exemple, les fichiers de données électroniques générés par le système.

De plus ils n'ont pas fourni une évaluation de leurs systèmes de données pour déterminer quelles données avaient été supprimées et leur impact sur les produits pharmaceutiques testés.

1.2.5.3. Recommandations de la FDA en matière d'intégrité des données

A la suite de ces écarts constatés par la FDA il a été demandé, malgré l'argumentaire des laboratoires, d'effectuer :

- une évaluation complète et indépendante des pratiques, procédures, méthodes, équipements, documentation et compétences des analystes du laboratoire. Sur la base de cette évaluation, ils devaient fournir un plan détaillé pour corriger et évaluer l'efficacité des systèmes informatiques, y compris les mesures spécifiques qu'ils allaient prendre pour garantir que toutes les données soient enregistrées au moment de l'action.
- une enquête complète sur l'étendue des inexactitudes dans les enregistrements et les rapports de données, y compris les résultats de l'examen des données en y incluant une

description détaillée de la portée et des causes racines aux manquements à l'intégrité des données.

- la mise en place d'une stratégie de gestion qui comprend les détails du plan global d'actions correctives et d'actions préventives. Le plan d'actions correctives devait détailler la façon envisagée pour garantir la fiabilité et l'exhaustivité de toutes les données générées, y compris les données microbiologiques et analytiques, les dossiers de fabrication et toutes les données soumises à la FDA. [28]

1.2.6. Les observations en matière d'intégrité des données sont en constante augmentation ces dernières années

Ces 15 dernières années, le nombre d'observations émises concernant l'intégrité des données, la documentation et les pratiques de gestion des enregistrements lors des inspections des bonnes pratiques de fabrication (BPF) a été en constante augmentation, signe que les autorités réglementaires portent une attention croissante à ce problème.[29]

En 2019, 65 % des lettres d'avertissement de la FDA étaient dues à des anomalies d'intégrité des données. Ce constat est un phénomène international et est en constante augmentation comme le démontre la Figure 13 ci-dessous. En effet, des cas de non-conformités ont été remontés majoritairement en Chine, aux USA, en Inde et en Europe. [30]

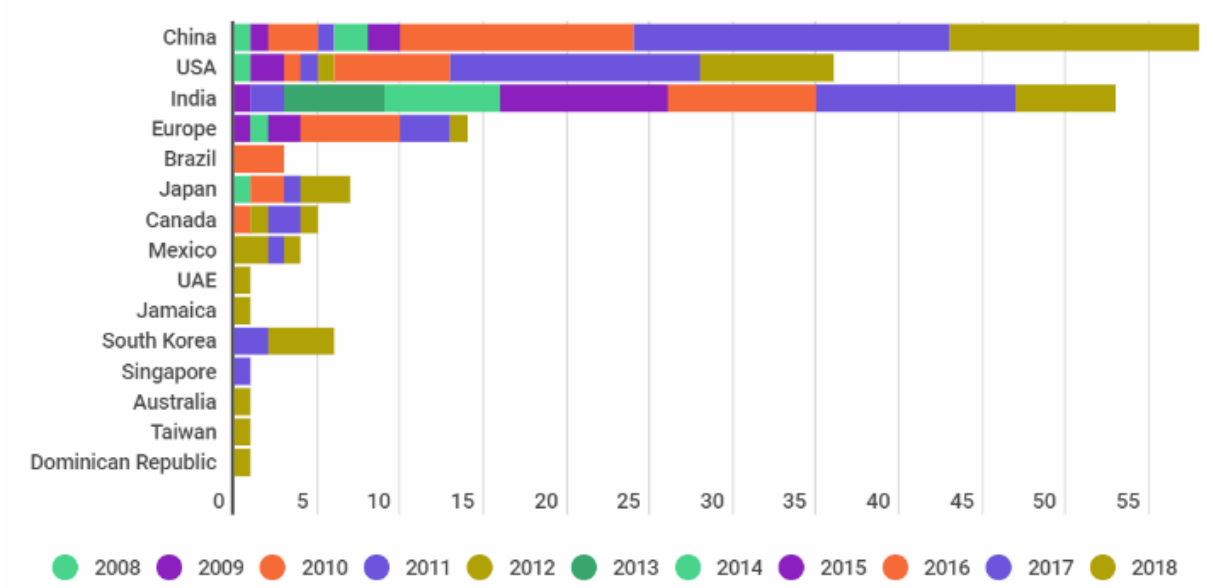


Figure 13 : évolution du nombre d'écarts data integrity de la FDA entre 2008 et 2018 par pays [30]

Dans son rapport rédigé à la suite d'une étude réalisée à partir d'une analyse rétrospective de 22 inspections conduites entre 2014 et 2019 concernant l'activité de fabrication de substances

actives issues de la technologie de l'ADN recombinant, l'ANSM mentionne que les principaux constats en lien avec l'intégrité des données électroniques générées dans les laboratoires de contrôle concernent des manquements relatifs à :

- *la gestion des profils utilisateurs et des privilèges associés ;*
- *la gestion des mots de passe, notamment l'utilisation d'un mot de passe générique commun à plusieurs utilisateurs ;*
- *la protection de l'intégrité des données électroniques, notamment l'absence de verrouillage de la date et de l'heure d'acquisition des données ;*
- *la fréquence de revue des « audit trails » et l'absence d'activation de cette fonction, le cas échéant ;*
- *l'utilisation de fichiers non validés et/ou non verrouillés pour réaliser des calculs utilisés dans le cadre de certaines analyses libératoires de substances actives ;*
- *l'absence de procédure décrivant les règles d'intégration manuelle des pics chromatographiques ;*
- *l'absence de procédures de sauvegarde des données électroniques et de fréquence de sauvegarde ;*
- *l'absence de vérification de l'intégrité, de l'exactitude et de la capacité à restaurer les données sauvegardées. [31]*

Mais ces constats ne s'arrêtent pas aux laboratoires de contrôle et s'appliquent également à toutes les activités de fabrication sur un site de production pharmaceutique. En effet, certains écarts relevés au cours de cette étude concernent des manquements aux exigences de l'annexe 11 des BPF pour les systèmes informatisés, comme le montre la figure 14 ci-dessous. [31]

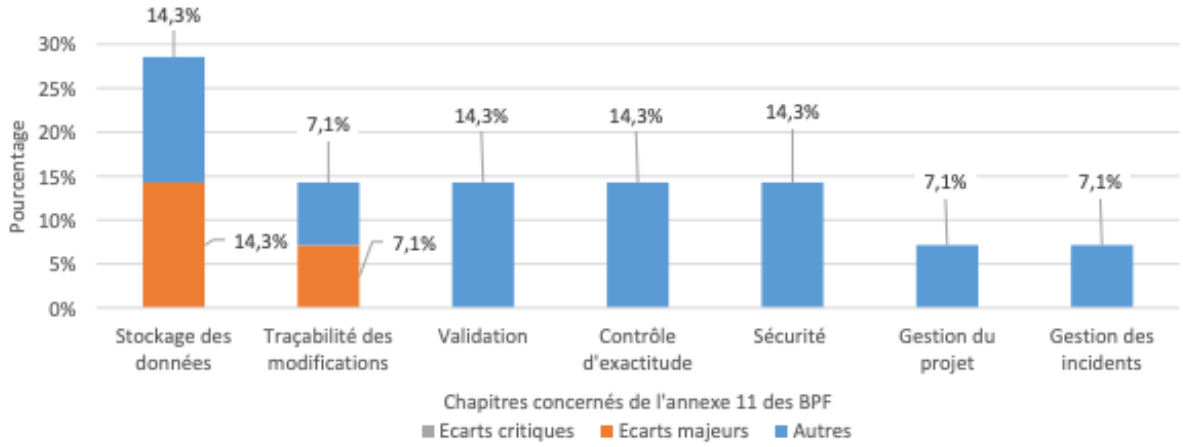


Figure 14 : contributions moyennes aux chapitres concernés de l'annexe 11 des BPF pour chaque niveau de criticité [31]

Selon cette étude, aucun écart critique n'a été observé. Les écarts majeurs ont été identifiés sur le stockage des données et la traçabilité des modifications. Avec 28,6% des écarts en lien avec le stockage des données dont 14,3% des écarts majeurs relevés, la principale thématique concerne le stockage des données. Les points qui ont été relevés ont été essentiellement des carences dans le système de sauvegarde des données électroniques générées au sein des laboratoires de contrôle, à savoir l'absence de procédures, des défaillances dans la stratégie de sauvegarde des données, l'absence de vérification de l'accessibilité, de la lisibilité et de l'exactitude des données sauvegardées [31].

7,1% d'écart majeurs sont relatifs à la traçabilité des modifications. Cela concerne essentiellement des carences dans la gestion des « audit trail » au sein des laboratoires de contrôle (stratégie, formation du personnel, revue). [31]

Les autres écarts relevés se répartissent de manière homogène sur plusieurs chapitres de l'annexe 11 des BPF à savoir le contrôle d'exactitude, la validation et la sécurité (environ 14% pour chacun d'entre eux).

Selon les dernières observations constatées par la FDA et l'ANSM ces dernières années lors d'inspection, les principales sources de risque de données non intègres sont :

- un recours à des pratiques humaines inadéquates : lorsque des personnes saisissent des informations de manière incorrecte, dupliquent ou suppriment des données, ne suivent pas les procédures appropriées ou font des erreurs lors de la mise en œuvre des procédures destinées à protéger les informations,

- un flux de données non maitrisé : lorsque les données ne peuvent pas être transférées avec succès d'un emplacement à un autre dans une base de données,
- l’utilisation de systèmes informatisés qui ne sont pas en mesure de répondre aux exigences réglementaires ou qui sont mal qualifiés et validés.

Stratégie globale de maitrise de l'intégrité des données sur un site de production pharmaceutique

Compte tenu de l'importance de maitriser l'intégrité des données et de la surveillance accrue des autorités de santé comme décrit dans la partie 1.1 et 1.2, les sites de production pharmaceutiques ont tout intérêt à implémenter une approche globale au système de management de la qualité existant. Nous nous intéresserons donc dans cette partie à illustrer cette approche globale de maitrise de l'intégrité des données sur un site de production pharmaceutique. Cette proposition s'inspire des guidelines présentées dans la partie 1.2.2 et de mon expérience personnelle acquise au sein des Laboratoires Servier Industrie.

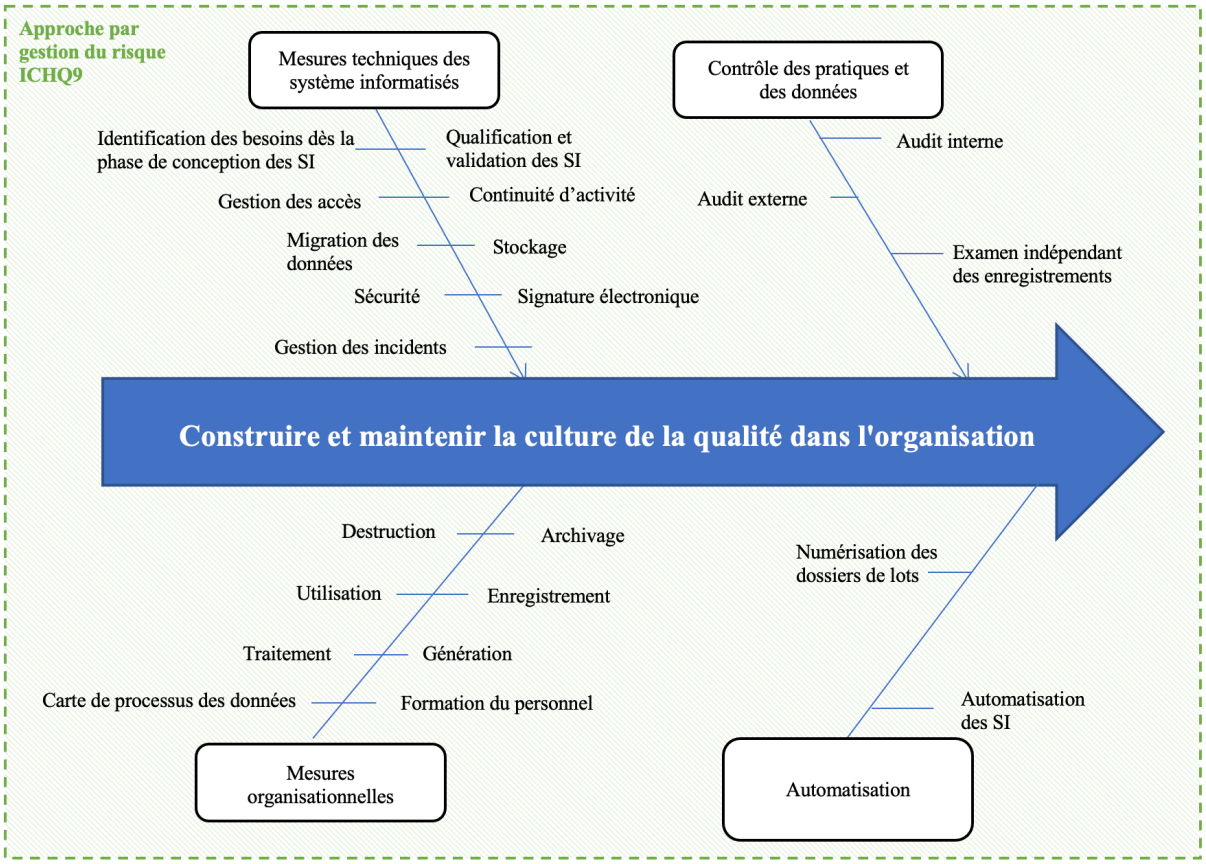


Figure 15 : les différents leviers pour une maitrise de l'intégrité des données

Les différents leviers de la stratégie globale illustrés dans la Figure 15 ci-dessus vont être détaillés dans les parties suivantes. Cette stratégie globale se compose de 5 axes principaux focalisés sur la mise en place d'une culture d'entreprise centrée sur la gouvernance des données en intégrant :

- des mesures techniques de maitrise des systèmes informatisés telles que décrit dans l'annexe 11 des bonnes pratiques de fabrication,
- des mesures organisationnelles nécessaires dans le système de management de la qualité pharmaceutique car elles permettent de consolider la maitrise des données tel que le développement de cartes de processus pour les données critiques afin que les industriels aient un contrôle sur leurs données tout au long du cycle de vie de la donnée,
- le contrôle des pratiques et des données pour s'assurer de la bonne compréhension et de la bonne application des grands principes d'ALCOA+,
- et la mise en place de l'automatisation comme outil de maitrise de la qualité.

Quels que soient les leviers utilisés, une approche de gestion de la qualité et du risque tel que décrit dans ICH Q9 « *ICH guideline Q9 on quality risk management* » doit être réalisée. Le degré d'effort et de ressources affectées à la maitrise de l'intégrité de données doit être proportionnel à la criticité des données (comment elles sont utilisées) et au risque inhérent (comment elles sont générées).

2.1. Approche par gestion du risque (ICHQ9)

Les données relatives au contrôle des processus critiques, aux décisions de libération des lots ou à la stabilité à long terme ont un impact significatif sur la qualité du produit. D'autres données, bien que pertinentes pour le fonctionnement du site de production, peuvent avoir une criticité moindre.

La manière dont les données sont générées influencera le risque inhérent à l'intégrité des données. Les données peuvent être générées à la suite d'une observation humaine sur un enregistrement papier ou, par des systèmes simples tels qu'une balance de pesée, jusqu'à des systèmes informatisés plus complexes et hautement configurables tels qu'un système de pilotage des colonnes de chromatographie. Les risques inhérents à l'intégrité des données diffèrent en fonction du degré de configuration des données générées par ces systèmes, et donc de leur manipulation potentielle.

Les fabricants concentrent leurs ressources en matière d'intégrité et de validation des données sur les systèmes informatisés complexes et de grande taille, tout en accordant moins d'attention aux autres systèmes dont la complexité semble moindre bien que les équipements simples puissent générer des données critiques. Il convient donc d'appliquer une approche par gestion du risque. Cette approche telle que décrit dans ICHQ9 repose sur deux principes fondamentaux :

- l’évaluation du risque doit être fondée sur des connaissances scientifiques et doit être guidée par la sécurité du patient,
- et le niveau d'effort doit être proportionnel au niveau de risque. [32]

La gestion des risques pour la qualité est un processus systématique d'évaluation, de contrôle, de communication et d'examen des risques pour la qualité du médicament tout au long du cycle de vie du produit. L'importance accordée à chaque composante peut varier d'un cas à l'autre, mais un processus solide tiendra compte de tous les éléments proportionnellement au risque [32].

Les étapes pour lancer et planifier un processus de gestion des risques de qualité peuvent être les suivantes :

- l’évaluation du risque,
- la maitrise du risque,
- la revue du risque.

2.1.1. Évaluer le risque

L'évaluation des risques consiste à identifier les dangers et à analyser et évaluer les risques associés à l'exposition à ces dangers : quel est l'impact des données sur la qualité ou la sécurité du produit ? Quelle décision les données influencent-elles ?

Le résultat d'une évaluation des risques permet une estimation quantitative ou qualitative du risque. Elle doit évaluer, par exemple, les systèmes informatisés pertinents, le personnel, la formation, les systèmes de qualité et l'étendue des activités externalisées.

L’évaluation des risques se fait en 3 étapes successives :

- l'identification des risques permet de repérer les dangers en se référant à la question ou à la description du problème : quel est le danger ?
- l'analyse des risques consiste à estimer le risque associé aux dangers identifiés : quelles sont les conséquences de ce danger ?
- l'évaluation du risque compare le risque identifié et analysé à des critères de risque donnés. A cette étape le but est de quantifier ou de qualifier et de hiérarchiser le risque afin de mettre en place des actions proportionnelles à son niveau de risque.

Lorsque l'évaluation des risques liés à l'intégrité des données a mis en évidence des domaines nécessitant des mesures correctives, la hiérarchisation des actions et la hiérarchisation des contrôles doivent être documentées et communiquées. [32]

2.1.2. La maitrise du risque

La maitrise du risque est la deuxième étape et permet la mise en place d'actions visant à réduire et/ou à maitriser les risques. L'objectif de cette étape est de réduire le risque à un niveau acceptable au regard de l'impact sur l'intégrité des données. Les risques doivent être évalués, atténués, communiqués et révisés tout au long du cycle de vie du document et des données et à une fréquence basée sur le niveau de risque. Cette étape se divise en deux sous étapes successives : [33]

- la réduction du risque se concentre sur les processus d'atténuation ou d'évitement du risque de qualité lorsqu'il dépasse un niveau acceptable. Les risques pour l'intégrité des données peuvent être minimisés ou éliminés. Ces mesures seront détaillées dans les parties suivantes,
- l'acceptation du risque correspond à la prise de décision formelle d'accepter le risque résiduel. [32]

2.1.3. La revue du risque

La revue du risque doit faire partie intégrante du processus de gestion de la qualité afin de mesurer l'avancement et l'effectivité des actions correctives et préventives mises en place. Elle doit être effectuée à fréquence régulière et intégrer tous les acteurs impliqués dans le processus. Elle permet également de prendre en compte les nouvelles connaissances et expériences car des événements planifiés ou non sont susceptibles d'impacter la proposition initiale de maitrise du risque.

2.2. Construire et maintenir la culture de la qualité

La politique d'intégrité des données est l'ensemble des dispositions qui permettent de garantir l'intégrité des données. La première étape est donc la mise en place d'une culture d'entreprise centrée sur la gouvernance des données. La gouvernance des données fait partie intégrante d'un système de management de la qualité pharmaceutique efficace tel que décrit dans l'ICH Q10.

La direction doit adopter une approche ouverte et encourager le personnel à tous les niveaux à signaler les erreurs, les omissions, les défaillances des systèmes informatisés, les résultats

anormaux, les mauvaises pratiques ou même les falsifications sans crainte de sanction. Ce n'est qu'en établissant une culture d'entreprise qui met l'accent sur l'intégrité des données, l'ouverture et la transparence, que les fabricants auront plus de chances d'atténuer les risques liés à l'intégrité des données. Le système de gouvernance des données doit également être revu par la direction et le personnel à tous les niveaux afin de garantir son efficacité à mesure du déploiement des leviers de maitrise et de l'évolution des exigences réglementaires.

La mise en place d'un tel système permet aux laboratoires de définir, de hiérarchiser et de communiquer ses activités de gestion des risques liés à l'intégrité des données de manière cohérente et globale aux autorités réglementaires. L'absence d'un système de gouvernance des données peut conduire à des systèmes d'intégrité des données non coordonnés, avec un potentiel de lacunes dans les mesures de contrôle, comme évoqué avec l'exemple de Vitarine Pharmaceutical ou plus récemment avec Novartis.

Cette politique doit également englober la conception du système de management de la qualité en considérant les données critiques, quels que soient le processus, le format ou la technologie dans lesquels elles sont générées, traitées, enregistrées, utilisées ou même stockées. En effet, l'effort et les ressources affectés à la gouvernance des données doivent également être équilibrés avec les autres demandes de ressources en matière de qualité.

Les défaillances de l'intégrité des données ne résultent pas uniquement d'actes de fraude délibérée. Elles sont également liées à de mauvaises pratiques involontaires, à une mauvaise organisation et à des systèmes non maitrisés, qui créent des opportunités de défaillance. [31]

2.3. Maitrise technique des systèmes informatisés

Un système informatisé est défini comme un système comprenant le système de traitement des données et le système d'exploitation (le « *software* ») ainsi que la partie physique de l'équipement (le « *hardware* »). Tous les systèmes informatisés qui comprennent des applications susceptibles d'affecter la qualité du médicament doivent être évalués conformément aux principes et aux exigences des BPF. [34]

Les exigences de l'Agence Européenne du Médicament (EMA) concernant les systèmes informatiques figurent dans l'annexe 11 des GMP et fournissent des critères cohérents pour une mise en œuvre, un contrôle et une utilisation efficaces de systèmes informatisés. [11]

L'annexe 11 est applicable aux logiciels utilisés dans toutes les activités soumises à la réglementation des bonnes pratiques de fabrication qu'il s'agisse d'outils de production tels que

les logiciels qui pilotent les équipements de production, ou de logiciels utilisés dans le système de contrôle de la qualité tels que les systèmes de gestion de l'information du laboratoire de contrôle. Un système informatique doit garantir que les méthodes d'enregistrement et de conservation des données permettent d'atteindre au moins le même degré de confiance que celui offert par les systèmes sur papier. [2]

L'exigence de base de l'EMA concernant l'intégrité des données provient des directives 2003/94/CE et 91/412/CEE du Conseil de l'UE :

> *"Les données stockées électroniquement doivent être protégées, par des méthodes telles que la duplication ou la sauvegarde et le transfert sur un autre système de stockage, contre la perte ou l'endommagement des données, et des pistes d'audit doivent être maintenues".*

Les moyens de maitrise des systèmes informatisés peuvent être les suivants :

- l'identification des besoins dès la phase de conception,
- la qualification et la validation des systèmes,
- la gestion des accès,
- la mise en place d'un audit trail,
- la formation du personnel à l'utilisation de ces systèmes,
- la maitrise de la migration des données,
- le stockage des données brutes,
- la sécurité,
- la gestion des incidents,
- la continuité d'activité,
- la mise en place d'une signature électronique.

2.3.1. Identification des besoins dès la phase de conception des systèmes informatisés

L'identification des besoins se fait dès l'étape d'initiation du projet lors de la rédaction du cahier des charges du système informatisé. Le cahier des charges permet de définir les besoins de l'utilisateur ainsi que les exigences réglementaires. En outre, il comprend les conditions commerciales, notamment l'expédition, les modalités de paiement, la garantie, la marche à suivre en cas de litige et surtout les spécifications techniques attendues. Il est rédigé par le fournisseur du système et par l'industriel, et le plus souvent réalisé avec la participation du service d'assurance qualité et constitue la base des exigences fonctionnelles d'un système pendant sa phase de conception. [35]

L'émergence des systèmes informatisés ces dernières années dans l'industrie pharmaceutique à mis en évidence la nécessité de concevoir des équipements pour supporter les recommandations relatives à l'intégrité des données. En intégrant cette stratégie dès la phase de conception de l'équipement au travers de recommandations d'intégrité des données dans le cahier des charges, on limite la nécessité de mettre en place des mesures de mitigation. En effet une conception mal effectuée peut conduire le cas échant à la nécessité de mettre en place des mesures organisationnelles ou de surveillances plus complexes et moins fiables.

Parmi les éléments à prendre en compte voici une liste non exhaustive des grandes thématiques à définir pour s'assurer de concevoir un équipement qui respecte les critères relatifs à l'intégrité des données [36]:

- la gestion des accès au système : chaque utilisateur doit pouvoir disposer de son propre compte dans le système avec un mot de passe unique, un nombre limité d'essais et une périodicité limitée. Le mot de passe doit être différent à chaque nouveau renouvellement et il doit être possible de créer différents types de profils correspondant à différents groupes de privilèges tel qu'un profil « Administrateur » et un profil « Utilisateur ». De plus les droits d'accès doivent être adaptés au profil : un profil administrateur ne doit pas forcément avoir accès à tous les privilèges. Enfin, le système doit être capable de déconnecter automatiquement un utilisateur dont le profil est inactif depuis un laps de temps défini.
- l'horodatage : le système doit préférentiellement être connectable à un système d'horloge de référence et, afin d'éviter toute erreur humaine, il doit être impossible, y compris pour un administrateur, de modifier l'heure. L'horodatage doit inclure à minima l'année, le mois, le jour, l'heure, les minutes et l'UTC. Enfin, lorsque les impressions de données sont nécessaires, elles doivent également être horodatées.

- le stockage et la restauration des données : les données doivent être stockées sur un support non amovible permettant un transfert automatisé vers un périphérique réseau. Les sauvegardes doivent être stockées dans un endroit défini et accessible. De plus l'extraction ne doit pas avoir d'impact sur la donnée originale stockée et doit permettre de récupérer des copies conformes complètes de la donnée d'origine. Enfin la restauration doit permettre de récupérer les données présentes sur l'ancien système.

- l'audit trail : le système doit être capable d'enregistrer toutes les actions, dont les actions qui créent, modifient ou suppriment les données. Il doit comporter l'identification de l'utilisateur, l'horodatage complet auquel l'enregistrement a été créé, modifié ou supprimé, le type d'action réalisée, l'identification de l'enregistrement concerné, la nouvelle valeur et l'ancienne valeur et le motif expliquant la raison de la modification. De plus, des fonctions permettant de faire des requêtes sur les données d'audit trail doivent être disponibles pour permettre de fournir les informations demandées par les auditeurs ou les utilisateurs du système et il ne doit pas être possible de désactiver l'audit trail.

- la signature électronique : le système doit demander un identifiant et un mot de passe pour une signature électronique. Elle doit contenir le prénom et le nom du signataire, l'horodatage complet et la raison associée à la signature. La signature électronique doit être liée de façon permanente aux enregistrements des données signées et il doit être impossible de dissocier la signature électronique de l'enregistrement correspondant.

- la capacité du système à s'intégrer au réseau de l'entreprise. En effet le système doit pouvoir fonctionner sur le réseau de l'industriel.

Ces critères ont été développés par le Groupe Data Integrity Management (DIM), groupe pluridisciplinaire des Laboratoires Servier Industrie sur le site Gidy, France.

Une fois que l'étape de définition du système a été menée à bien par le fournisseur et le client et que le système a été conçu en accord avec les principes fondamentaux d'intégrité des données, les étapes de qualification et de validation peuvent débuter.

2.3.2. Qualification et validation des systèmes informatisés

Les exigences décrites dans le cahier des charges sont évaluées dès la qualification de conception chez le fournisseur puis lors des phases de qualification opérationnelle et de performance chez le client afin de vérifier que le système répond bien au besoin initial, comme indiqué sur la figure 17 ci-dessous décrivant les différentes étapes du processus de qualification et de validation des systèmes.

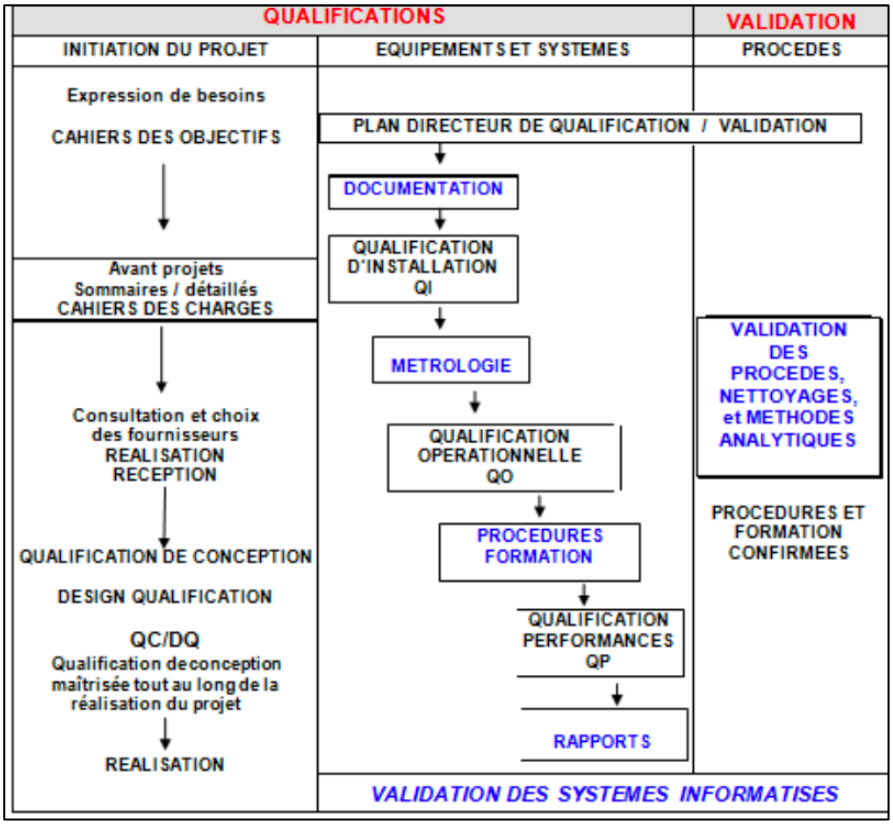


Figure 16 : les étapes de qualification des équipements et de validation des systèmes informatisés

La validation des systèmes informatisés permet de vérifier que le produit répond bien au besoin initial défini dans le cahier des charges conformément aux directives présentes dans l'annexe 15 « Qualification et validation » [35] et l'annexe 11 « système informatisés ». [37]

Elle prend en compte l'impact que les systèmes ont sur la capacité à répondre aux exigences réglementaires et de l'impact que ces systèmes peuvent avoir sur la fiabilité des données.

Ainsi une validation des systèmes informatisés doit suivre chorologiquement les grandes étapes suivantes :

- Qualification d'installation (QI) : Preuve documentée qui démontre que le système à qualifier répond à toutes les spécifications, qu'il est installé correctement et conformément aux conditions environnementales recommandées, et que tous les

composants et la documentation nécessaires au fonctionnement continu sont installés et en place. [35]

- Qualification opérationnelle (QO) : Preuve documentée qui démontre que tous les aspects opérationnels du système fonctionnent correctement et conformément aux exigences de l'utilisateur. [35]
- Qualification de performance (QP) : Preuves documentées qui démontrent que le système fonctionne comme prévu, de manière cohérente dans le temps, et qu'il répond aux exigences de l'utilisateur pendant son fonctionnement. [35]

C'est pendant la QO et la QP que les industriels évaluent la conformité aux principes d'intégrité des données, dans l'environnement de production, afin de s'assurer que les exigences définies dans le cahier des charges sont bien respectées. Ces évaluations se font sous la forme de protocoles de test et reprennent tous les aspects identifiés durant la phase de conception concernant la gestion des utilisateurs, l'horodatage, le stockage et restauration des données, le fonctionnement de l'audit trail, la conformité de la signature électronique et la capacité du système à s'intégrer au réseau de l'entreprise tel que défini dans la partie 2.3.1.

La validation seule ne garantit pas nécessairement que les documents générés sont protégés de manière adéquate et les systèmes validés peuvent être vulnérables à la perte et à l'altération par des moyens accidentels ou malveillants. La validation doit donc être complétée par des mesures organisationnelles appropriées, ainsi que par la formation des utilisateurs.

2.3.3. Gestion des accès

La gestion des accès permet de maintenir l'intégrité des données en s'assurant que seuls les utilisateurs appropriés peuvent y accéder et les modifier. Sans ce type de solution robuste, il peut être difficile pour les industriels d'avoir une vision claire des personnes qui ont accès aux données et de ce qu'elles font avec ces données. Les composants de base de la gestion des accès sont les suivants :

- la gestion des sessions car elle garantit une visibilité sur toutes les actions des utilisateurs qui accèdent à des données importantes. Une gestion de session fournit aux équipes de sécurité des pistes d'audit inaltérables qui peuvent non seulement être examinées en cas de suspicion de violation, mais aussi simplifier le processus de respect des règles de conformité. Un outil de gestion de session robuste peut aller au-delà de la simple création d'une piste d'audit, en empêchant les utilisateurs privilégiés de tenter des actions

interdites et/ou en créant des alertes ou encore en fermant l'accès en cas de tentative de telles actions. [38]

- la centralisation des mots de passes afin de conserver tous les mots de passes dans un endroit unique afin d'empêcher les utilisateurs finaux d'avoir un accès direct aux mots de passe.
- la mise en place d'un gestionnaire d'accès centralisé afin de fournir un point d'accès unique pour tous les utilisateurs. Les administrateurs peuvent rapidement ajouter ou supprimer des utilisateurs selon les besoins et modifier l'accès et les autorisations en fonction des changements dans les responsabilités professionnelles. Ceci est crucial pour la capacité pratique des administrateurs à maintenir le principe du moindre privilège, c'est-à-dire que les utilisateurs ne reçoivent que le minimum de privilèges nécessaires pour effectuer leur travail, et que ces privilèges puissent être rapidement révoqués lorsqu'ils ne sont plus nécessaires.

Un système documenté doit être en place afin de définir l'accès et les privilèges des utilisateurs des systèmes informatisés. Il ne devrait pas y avoir de divergence entre les dossiers papiers et les dossiers électroniques, y compris au niveau de la création et de l'inactivation des utilisateurs.

L'accès et les privilèges doivent être en cohérence avec le rôle et la responsabilité de l'individu, avec les contrôles appropriés pour garantir l'intégrité des données. Le but principal de la gestion des accès est d'éliminer tout conflit d'intérêts en matière de données. Certains droits d'accès tels que la suppression de données, la modification de la base de données ou les changements de configuration du système ne doivent pas être attribués aux opérateurs par exemple.

De plus ces activités doivent être tracées, les enregistrements doivent être conservés et des pistes d'audit doivent être activées afin de suivre toutes les activités des administrateurs système. [33]

2.3.4. Migration des données

La migration des données est le processus de transfert des données. Une migration peut se faire entre deux types de formats identiques « papier vers papier » ou « numérique vers numérique », d'un format papier vers un format numérique (saisie des valeurs) ou d'un format numérique vers un format papier (impression).

Les données peuvent être enregistrées manuellement en reflétant une observation, un résultat ou d'autres données et informations sur papier, ou électroniquement en utilisant des

équipements et des instruments, y compris ceux liés à des systèmes informatisés. Une combinaison de systèmes manuels et électroniques peut également être utilisée, appelée "système hybride". Il s'agit d'une considération essentielle pour toute mise en œuvre, mise à niveau ou consolidation de système. Si les données sont transférées vers un autre format ou système de données, la vérification de la migration des données doit inclure la confirmation que les données ne sont pas altérées, par exemple une piste d'audit ou le cas échéant la mise en place d'un transfert automatisé des données, pour éliminer tout risque de perte ou de falsification.

2.3.5. Stockage des données

Le stockage des données fait référence à tout dispositif qui enregistre (stocke) ou récupère (lit) des informations (données) à partir de tout support, y compris le support lui-même. Une fois que les données sont dans le dispositif de stockage, leur intégrité doit être garantie. Les protections logiques et physiques doivent être adaptées à la criticité du système informatique. Il doit y avoir un enregistrement de toute modification des données, y compris de l'entrée précédente, de l'auteur de la modification et de la date à laquelle elle a été effectuée. Pour réduire le risque de perte de données et garantir la disponibilité des données aux utilisateurs, des audits de la méthode de stockage et des sauvegardes périodiques doivent être effectuées. Les sauvegardes doivent être stockées séparément du lieu de stockage initial. L'efficacité des processus de sauvegarde et de restauration doit être vérifiée dans le cadre du processus de qualification et des revues périodiques doivent être effectuées.

2.3.6. Sécurité

Une sécurité informatique forte est le principal moyen de protéger l'intégrité des documents électroniques.

Seuls les personnels autorisés peuvent modifier les composants du système informatique et assurer la sécurité des documents résidant dans le système. Une procédure définie doit être mise en place pour l'émission, l'annulation et la modification de l'autorisation d'entrer et de modifier les documents, y compris la modification des mots de passe. Les contrôles d'accès des utilisateurs sont configurés et appliqués de manière à interdire l'accès non autorisé aux données, leur modification et leur suppression. [5]

Des examens périodiques doivent être effectués après la validation initiale tels que :

- l'entrée de données et les modifications des enregistrements informatisés ne doivent être faites uniquement par le personnel autorisé,

- des identifiants et des mots de passe individuels doivent être créés et attribués à tous les membres du personnel qui doivent accéder au système électronique spécifique et l'utiliser,
- les systèmes doivent permettre plusieurs niveaux d'accès des utilisateurs et l'attribution de ces accès doit suivre la règle du moindre privilège, c'est-à-dire qu'il faut attribuer le niveau d'accès minimum nécessaire pour toute fonction.

Les documents électroniques doivent être vérifiés, stockés, sauvegardés et archivés dans le cadre des examens périodiques d'accessibilité, de lisibilité et d'exactitude. La sortie des sauvegardes doit être vérifiée afin de garantir l'exactitude des données de la piste d'audit. Lorsqu'un document est supprimé avant la date de conservation prévue, une piste d'audit de la suppression doit être conservée jusqu'à la fin de la période de conservation approuvée.

2.3.7. Gestion des incidents

Une documentation incorrecte, des erreurs de données, un fonctionnement inadéquat et des erreurs d'interface entre les systèmes informatiques peuvent affecter le fonctionnement du système. Ces événements doivent être entièrement documentés pour être évalués et analysés afin d'identifier la cause racine et pour mettre en place les actions correctives ou préventives appropriées afin d'éviter qu'ils se reproduisent. [11]

2.3.8. Continuité des activités

La continuité des activités en cas de panne d'un système doit également être assurée. Il s'agit du degré de préparation nécessaire pour assurer le fonctionnement de l'entreprise en cas de panne ou de problème du système. Les contrôles nécessaires à la restauration du système doivent être procédurés de manière adéquate et testés régulièrement. [11]

2.3.9. Audit trail

L'audit trail est un des outils privilégiés pour s'assurer de l'intégrité des données. Les « audit trail » ou piste d'audit désignent un enregistrement électronique sécurisé, généré par ordinateur et horodaté, qui permet de reconstituer le déroulement des événements liés à la création, à la modification ou à la suppression d'une donnée. Un audit trail est la chronologie du "qui, quoi, quand et pourquoi" d'un élément. [39]

Par exemple, l'audit trail d'une HPLC lors d'une exécution en laboratoire doit inclure l'utilisateur, la date et l'heure de l'exécution, les paramètres opératoires utilisés et les raisons d'un retraitement, le cas échéant.

Les audit trail électroniques se classent en deux grandes catégories :

- ceux qui suivent la création, la modification ou la suppression de données telles que les paramètres de traitement et les résultats,
- ceux qui suivent les actions du système, telles que les tentatives d'accès, de changement de paramètre opératoire ou de changement de recettes, etc.

Ces audit trail doivent :

- contenir tous les enregistrements électroniques pertinents conformément aux BPF et ayant un impact potentiel sur l'intégrité des données,
- décrire quand, par qui et pour quelle raison des modifications ont été apportées à l'enregistrement électronique. Les informations originales ne doivent pas être cachées,
- être disponible,
- être accessibles de manière maitrisée,
- et être régulièrement révisés. [5]

Ils peuvent être des outils d'investigation utiles dans le cadre d'une investigation où l'intégrité des données est incertaine, ou en tant que composante de l'examen de l'intégrité des données dans le cadre d'un processus opérationnel établi, tel que l'évaluation d'un dossier de lot. Il peut donc être un outil puissant pour aider à déterminer la fiabilité des documents.

Dans certains cas particuliers, les pistes d'audit qui capturent les modifications apportées aux données critiques pourraient être examinées à chaque lot avant la certification par le pharmacien responsable.

Comme l'indique la dernière ligne directrice de la Medicines and Health Products Regulatory Agency (MHRA) du Royaume-Uni sur l'intégrité des données, une piste d'audit sur papier peut être mise en œuvre si elle "est équivalente aux pistes d'audit informatiques". Si l'équivalence ne peut être démontrée, les entreprises doivent "passer à un système de piste d'audit". [16]

Les orientations de l'OMS adoptent une approche un peu plus stricte et déclarent que l''utilisation de systèmes hybrides est déconseillé, mais lorsque des systèmes anciens sont en attente de remplacement, des contrôles d'atténuation doivent être mis en place. [4]

2.3.10. Signature électronique

Les enregistrements peuvent être signés électroniquement. Ces signatures doivent être liées de manière permanente à leur enregistrement respectif et doivent inclure l'horodatage

complet à laquelle elles ont été appliquées. Les exigences réglementaires sont décrites dans la Part 11, Electronic Records; Electronic Signatures de la FDA. [12]

2.4. Mesures organisationnelles

Devant la multitude de systèmes et de données, les mesures organisationnelles sont nécessaires dans le système de management de la qualité pharmaceutique car elles permettent de consolider la maitrise des données. En effet, dans un système hybride où les données manuscrites et électroniques coexistent, à elles seules, les mesures techniques ne permettent pas d'assurer le contrôle des données sur la totalité du cycle de vie de la donnée.

2.4.1. Maitrise du data life cycle

Avec le soutien de la culture organisationnelle appropriée, l'élément important suivant d'une gouvernance des données réussie est de comprendre le cycle de vie des données. Cela permettra de mettre en œuvre un système conçu pour garantir l'intégrité des données tout au long de sa vie, au-delà des limites de l'examen des données.

Le cycle de vie des données prend en compte toutes les phases de la vie des données, de la génération initiale et de l'enregistrement, en passant par le traitement, l'utilisation, l'archivage, la récupération et finalement la destruction. Le fait de ne traiter qu'un seul élément du cycle de vie des données affaiblira l'efficacité des mesures mises en œuvre ailleurs dans le système.

L'EMA dans ses questions/réponses parues en 2018 sur la maitrise de l'intégrité des données identifie les questions que le laboratoire devra se poser lors de la mise en place d'une stratégie globale. Le Tableau 2 ci-dessous représente les questions à se poser pour assurer une maitrise des données tout au long du cycle de vie de la donnée [6]:

Tableau 2 : Les points de vigilances pour assurer une maitrise des données tout au long du cycle de vie de la donnée

Étape du cycle de vie	Les éléments de maitrise
Génération	• Comment et où les données originales sont-elles créées (sur papier ou sous forme électronique) ? • L'enregistrement permet-il de reconstituer l'activité ? • Où se trouvent les données et les métadonnées ? • Existe-t-il une gestion des accès à l'équipement ? • Est-il possible de modifier ou de supprimer les données et métadonnées d'origine ?
Traitement / Enregistrement	• Comment les données sont-elles traitées ? • Comment ce traitement est-il enregistré ? • Le système est-il validé conformément à l'annexe 15 des BPF ? • Si le traitement et/ou l'enregistrement est effectué manuellement, est-il possible d'influencer le traitement et l'enregistrement ?
Vérification de la donnée	• La donnée originale est-elle accessible ? (Ticket de pesée ou donnée électronique par exemple) • Jusqu'à cette étape, existe-t-il des périodes durant lesquelles il n'existe pas d'audit trail ? La donnée aurait-elle pu être modifiée/supprimée sans traçabilité ? • L'évaluateur des données a-t-il la visibilité et l'accès à toutes les données générées (Y compris celles qui ont été supprimées) ?
Utilisation de la donnée pour la prise de décision	• A quelle moment la décision est-elle prise ? Peut-on encore modifier la donnée après avoir pris la décision d'acceptabilité ou de refus ?
Archivage	• Où est stockée la donnée ? La donnée originale est-elle archivée ? • L'accès (physique/informatique) est-il sécurisé ?

Étape du cycle de vie	Les éléments de maitrise
	• Les données archivées sont-elles complètes ?
Suppression	• La période de rétention est-elle définie ? • La stratégie de rétention et de destruction est-elle définie et procédurée ?

Il doit y avoir une approche planifiée de l'évaluation, du contrôle et de la gestion des données et des risques pour ces données, d'une manière proportionnelle à l'impact potentiel sur la sécurité des patients, la qualité des produits et/ou la fiabilité des décisions prises tout au long des phases du cycle de vie.

2.4.1.1. Génération et traitement de la donnée

Tous les documents à caractère pharmaceutique doivent avoir un identifiant unique (y compris le numéro de version) et doivent être vérifiés, approuvés, signés et datés et l'utilisation de documents non contrôlés doit être interdite par les procédures locales. L'utilisation de pratiques d'enregistrement temporaires, par exemple des bouts de papier, doit être évitée car elles ne répondent pas au principe de la donnée brute.

Les documents non contrôlés augmentent la possibilité d'omission ou de perte de données critiques, car ces documents peuvent être jetés ou détruits sans qu'il soit possible de les retracer. Les documents non contrôlés peuvent ne pas être conçus pour enregistrer correctement les données critiques car :

- il peut être plus facile de falsifier des enregistrements non contrôlés,
- l'utilisation de pratiques d'enregistrement temporaires peut entraîner l'omission de données, et ces enregistrements originaux temporaires ne sont pas spécifiés pour la conservation,
- si les enregistrements peuvent être créés et accessibles sans contrôle, il est possible que les documents n'aient pas été enregistrés au moment où l'événement s'est produit,
- et il y a un risque d'utiliser des formulaires périmés s'il n'y a pas de contrôle de version ou de contrôle d'émission.

La conception du document ou du système doit prévoir un espace suffisant pour la saisie des données.

Les documents maîtres doivent comporter des marques distinctives permettant de distinguer le document maître d'une copie, par exemple l'utilisation de papiers ou d'encres de couleur. Les documents maîtres (sous forme électronique) doivent être protégés contre toute modification non autorisée ou involontaire grâce à la maitrise des accès du système de gestion électronique documentaire

2.4.1.2. Enregistrement

Les méthodes d'enregistrement des données doivent être approuvées, identifiables et contrôlées par version. Dans le cas du traitement électronique des données, les méthodes doivent être verrouillées pour empêcher toute modification non autorisée.

La méthode de traitement doit être enregistrée. Lorsque des données brutes ont été traitées plus d'une fois, chaque modification doit être accessible au contrôleur des données pour vérification.

2.4.1.3. Transfert

Les interfaces doivent être évaluées et traitées pendant la validation afin de garantir un transfert sécurisé et complet des données. Les interfaces doivent inclure des contrôles intégrés appropriés pour la saisie et le traitement corrects et sécurisés des données, afin de minimiser les risques d'intégrité des données. Les méthodes de vérification peuvent inclure l'utilisation d'outil de sécurisation de transfert. Le cryptage peut être également une solution adaptée à la sécurisation du transfert.

Le cas échéant, les interfaces entre les systèmes doivent être conçues et qualifiées pour inclure un transfert automatisé des données.

2.4.1.4. Archivage

Cette étape intervient après l'utilisation de la donnée. Elle est nécessaire pour assurer une traçabilité tout au long du cycle de vie de la donnée. Il faut mettre en place un système décrivant les différentes étapes de l'archivage des documents (identification des boîtes d'archives, liste des documents par boîte, durée de conservation, lieu d'archivage, etc.). Des instructions concernant les contrôles du stockage, de l'accès et de la récupération des documents doivent être mises en place.

Tous les enregistrements à caractère pharmaceutique sur papier doivent être archivés:

- dans des endroits sûrs pour éviter tout dommage ou perte,
- d'une manière telle qu'ils soient facilement traçables et récupérables,

- d'une manière qui garantit que les documents sont durables pendant toute la période de conservation.

Tous les documents doivent être protégés contre les dommages ou la destruction par :

- le feu,
- des liquides (par exemple, l'eau, les solvants et les solutions tampons),
- les rongeurs,
- l'humidité, etc.
- l'accès d'un personnel non autorisé.[5]

2.4.1.5. Suppression

La suppression ne doit être effectuée que par les personnes autorisées. Le temps de rétention doit être adapté à la criticité de la donnée et à la réglementation en vigueur. Cette suppression doit être documentée et procédurée. [4]

2.4.1.6. Cartographie des données critiques

L'élaboration d'une cartographie des données critiques est un aspect important de la gestion de la manière dont les données sont utilisées, par qui et où. En cartographiant le cycle de vie d'une donnée - idéalement avant qu'elle ne soit utilisée pour la prise de décision - les organisations ont un meilleur contrôle sur leurs données dans leur intégralité.

La cartographie nécessite au préalable d'identifier les données critiques et doit être élaborée au regard du cycle de vie de la donnée, de la génération jusqu'à la destruction. Elle fournit une vision globale et permet ainsi d'identifier les défaillances et de mettre en place les actions correctives et/ou préventives adaptées au niveau du risque.

Une cartographie efficace doit permettre d'identifier tous les risques susceptibles d'impacter l'intégrité des données tout au long de son cycle de vie, afin d'effectuer pour chacun des risques :

- l'évaluation du risque en y intégrant la référence de l'item, le processus, l'étape du cycle de vie de la donnée impactée, la description de la défaillance, la sévérité, la récurrence, la détectabilité et la criticité,
- la maitrise du risque afin d'identifier le type d'action corrective et/ou préventive et la description de l'action mise en place pour maitriser la défaillance identifiée,

- et la revue du risque qui permet de mesurer l'avancée et l'efficacité des mesures mises en place afin de valider, ou le cas échéant de modifier, les mesures correctives et/ou préventives.

La Figure 17 : ci-dessous représente une application de cette approche centrée sur la donnée. L'exemple correspond à la prise de masse réalisée en cours de production lors de la phase de compression.

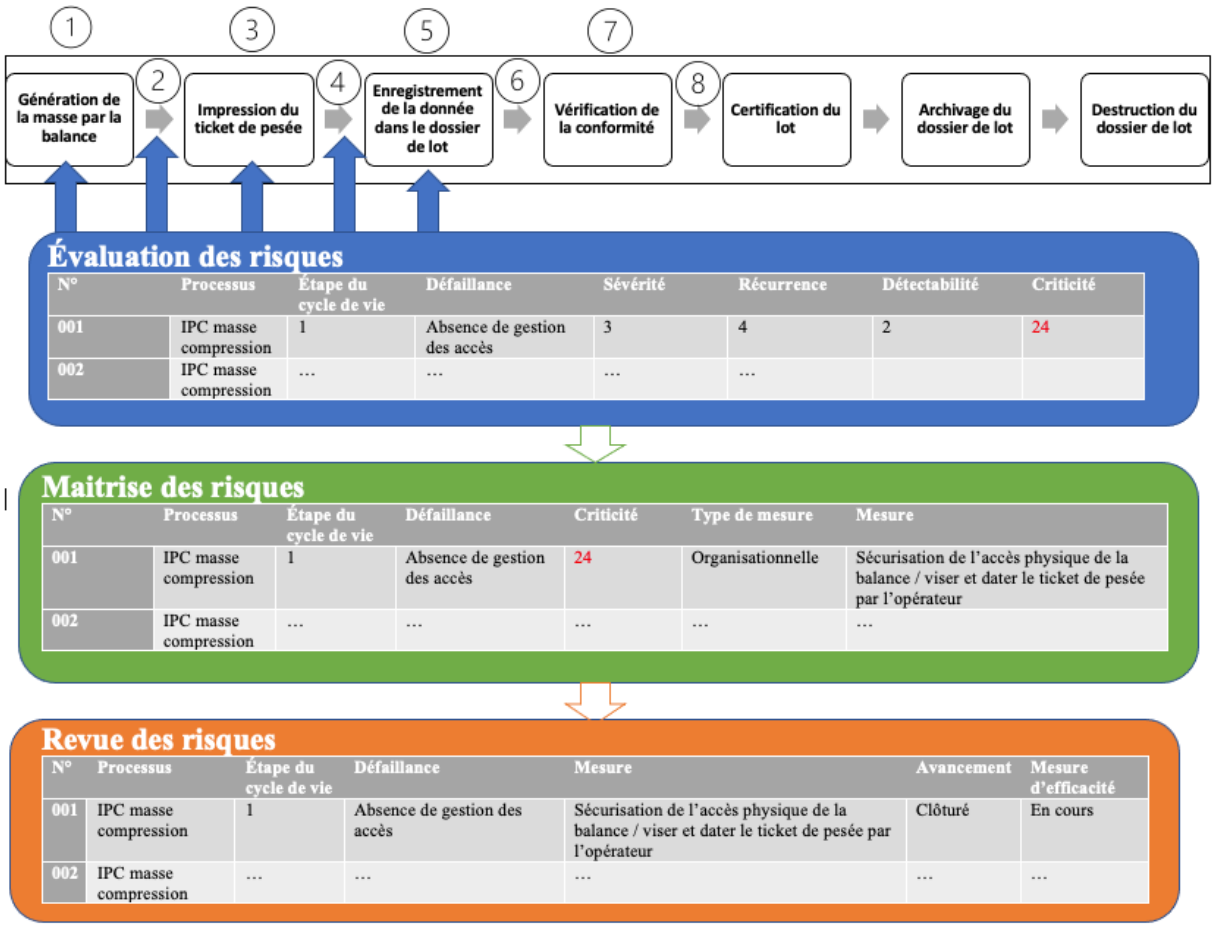


Figure 17 : cartographie du cycle de vie de la masse des comprimés en cours de production

2.4.2. Formation du personnel

Le personnel doit être sensibilisé afin qu'il puisse contribuer à cet effort et signaler les préoccupations avant qu'elles ne deviennent des problèmes à part entière. Les auditeurs internes doivent être formés afin qu'ils comprennent ce qu'ils doivent rechercher lorsqu'ils détectent des lacunes en matière d'intégrité des données.

Tout le personnel qui interagit avec les données GxP et qui effectue des activités GxP doit être formé aux principes d'intégrité des données et respecter les politiques et procédures de l'organisation avec notamment une sensibilisation et un rappel périodique en cas de dérive aux

principes fondamentaux d'ALCOA+. Lorsque des problèmes sont identifiés, les responsables doivent adopter une approche ouverte et encourager le personnel à signaler les erreurs, les omissions, les défaillances, les résultats anormaux, les mauvaises pratiques ou même les falsifications sans crainte de sanction.

Le personnel doit respecter les principes d'intégrité des données et doit être informé des conséquences potentielles en cas de non-respect.

Le personnel doit être formé aux bonnes pratiques de documentation et aux mesures permettant de prévenir et de détecter les problèmes relatifs à l'intégrité des données. Une formation spécifique peut être mise en place dans les cas où des systèmes informatisés sont utilisés pour la génération, le traitement, l'interprétation et la communication des données et lorsque l'évaluation des risques a montré que cela peut être nécessaire. Cette formation doit comprendre, par exemple, l'évaluation de la sécurité du système, la sauvegarde, le transfert, l'archivage, la destruction, les paramètres de configuration et l'examen des données et métadonnées électroniques, telles que les pistes d'audit, pour les systèmes informatisés individuels utilisés dans la production, la génération, le traitement et la communication des données.[33]

2.5. Contrôle des pratiques et des données

2.5.1. Examen indépendant des enregistrements

Procéder à un examen indépendant des données brutes sous forme de copies papiers et d'enregistrements électroniques permet de garantir l'exactitude, la précision et la traçabilité des données par la mise en place de procédures qui décrivent le processus de révision et d'approbation des données. L'examen doit également inclure un examen des métadonnées pertinentes, y compris la piste d'audit.

2.5.2. Audit interne et externe

Les activités de vérification de l'intégrité des données doivent être intégrées dans le processus d'audit interne et externe et doivent être effectuées périodiquement. Les points qui doivent être audités sont en priorités :

- la connaissance des bonnes pratiques d'intégrité des données tels que les principes d'ALCOA+,
- la maitrise des systèmes informatisés ,
- et la maitrise du cycle de vie des données pharmaceutiques critiques, de leur génération jusqu'à leur archivage.

2.6. Vers une automatisation des systèmes et une numérisation des dossiers de lot

Comme nous l'avons souligné précédemment, garantir l'intégrité des données en suivant les principes de l'ALCOA+ est devenu une évidence pour les fabricants du secteur pharmaceutique. Cependant, cela peut devenir complexe lorsque les fabricants utilisent encore des documents papier dans leurs opérations où les systèmes manuscrits et électroniques coexistent. [40]

De telles approches entraînent davantage d'erreurs, rendant les données inutilisables et le processus de maitrise des données très difficile. En outre, les méthodes de collecte manuelle risquent de ne pas prendre en compte certains points essentiels et utiles, ce qui fournit aux fabricants des informations incomplètes ou non exploitables comme le montrent les écarts relevés par les autorités réglementaires ces dernières années. [40]

De nombreux fabricants ont historiquement documenté leurs dossiers de lot en format manuscrit, et par conséquent, ont rencontré des problématiques de saisie de données inexactes ou illisibles. [40]

Pour éviter ces problèmes, certains fabricants se sont tournés vers des solutions digitales pour automatiser la collecte des données, leur permettant de numériser leurs dossiers de production et de réduire les erreurs humaines. [40]

Grâce aux applications digitales, les fabricants sont en mesure de tracer chaque opération et chaque personne impliquée dans un processus de production donné, créant ainsi une piste d'audit numérique qui garantit le respect de tous les principes de l'ALCOA+. [40]

Les systèmes informatisés de l'ensemble de l'architecture de l'entreprise peuvent être connectés, ce qui permet de convertir les données de base en instructions à exécuter par l'équipement de fabrication et de saisir électroniquement les données de production. Les systèmes Electronic Batch Record (EBR) suppriment le facteur humain de l'équation de la tenue des registres, ce qui améliore l'intégrité des données et accélère le processus de libération des lots.

La traçabilité est importante tout au long du processus de production, notamment sur des lignes de production qui autorisent la fabrication de plusieurs médicaments et où le risque de contaminations croisées est plus important, par exemple à l’étape d’engagement des matières premières. Dans ce cas des contrôles de traçabilité rigoureux sont nécessaires pour garantir qu'aucun produit A ne se retrouve dans la production d’un produit B ce qui pourrait avoir un impact très important pour le patient. Un système EBR permet donc :

- d’intégrer à l'équipement de production en temps réel des contrôles afin de s'assurer que les bonnes pratiques sont appliquées pour un lot spécifique de produits et ce tout au long du processus de production : mise en place de scannette, vérification des dates limites avant engagement des matières, vérification des dates limites avant nettoyage des équipements, automatisation des contrôles en cours de production, sécurisation de l’engagement de matières premières, automatisation des paramètres opératoires des équipements, etc.
- d’améliorer de façon significative la traçabilité des dossiers de lots. Le dossier de lot électronique se comporte alors comme un audit trail de tout le circuit de production et devient le reflet exhaustif des évènements qui se sont produits durant la production. Le personnel de l'assurance qualité (AQ) chargé de l’évaluation des lots n'a plus besoin de revoir des quantités importantes de documents manuscrits avant de libérer un lot de produits pharmaceutiques. Lorsque la totalité des systèmes de l’architecture sont validés et automatisés, les lots peuvent être libérés par exception : c’est-à-dire que seuls les écarts par rapport aux procédures standards doivent être examinés avant la libération du lot.
- de pouvoir gérer la production en temps réel. L’implémentation de Key Performance Indicators (KPI) automatisés permettra de mettre en place un tableau de bord de suivi de la production pour analyser les tendances en temps réel et d’appliquer des actions correctives et préventives plus pertinentes.

Bien que les coûts d'investissement initiaux soient élevés, les gains d'efficacité potentiels sont suffisants pour assurer un retour sur investissement important.

Un tel système automatisé et connecté ne devra tout de même pas se substituer à l’humain pour la prise de décision notamment en cas de non-conformités rencontrées sur le site de production. Ce type de système où la maitrise des données est contrôlée de bout en bout pourra par la suite permettre l’implémentation de la libération paramétrique des lots de production tel qu’indiqué dans l’Annexe 17 des GMP.

En effet, habituellement les médicaments doivent être conformes à des spécifications définies dans le dossier d’AMM et, sous réserve du respect des BPF, peuvent normalement être mis sur le marché en effectuant un ensemble complet de tests sur les produits finis. Lorsque la libération paramétrique est autorisée, sur la base de la connaissance du produit et de la compréhension du processus, les informations recueillies au cours du processus de fabrication peuvent être

utilisées à la place des contrôles finaux sur le produit fini pour la libération des lots. Un tel système met en avant l'assurance de la qualité au contrôle de la qualité et nécessite une maitrise parfaite des données de production de leur génération à leur utilisation.

En conclusion, avec des processus de fabrication pharmaceutique de plus en plus complexes, des données générées en quantité de plus en plus importante et des systèmes d'information de plus en plus nombreux, le maintien de l'intégrité des données au sein d'un site de fabrication pharmaceutique est un enjeu majeur pour produire des médicaments sûrs et de qualité pour les patients. Implémenter une approche globale au système de management de la qualité est donc la stratégie la plus adaptée afin de garantir que les données pharmaceutiques générées, traitées, enregistrées, utilisées ou même stockées, constituent un enregistrement attribuable, lisible, contemporain, original, exact, complet, cohérent, durable et disponible tout au long du cycle de vie de la donnée et centrée sur une approche par analyse de risque.

Un exemple de stratégie de mise en place d'une démarche de maitrise de l'intégrité des données sur un site de production pharmaceutique va être présenté dans la dernière partie.

Mise en place d'une stratégie de maitrise des systèmes informatisés sur un site de production pharmaceutique

Les sites de fabrication pharmaceutique sont confrontés à un certain nombre de défis à l'ère du numérique. En effet, l'industrie 4.0 révolutionne la façon dont elle fabrique, améliore et distribue ses produits. Les fabricants intègrent de nouvelles technologies, notamment :

- l'Internet des objets (IoT) qui correspond au réseau d'objets qui sont équipés de capteurs, de logiciels et d'autres technologies dans le but de se connecter et d'échanger des données avec d'autres dispositifs et systèmes sur le réseau,
- le « *cloud computing* » qui correspond à l'utilisation de serveurs informatiques à distance pour stocker, gérer et traiter des données en masse,
- et l'utilisation de l'Intelligence Artificielle dans l'ensemble des installations de production. [41]

Alors que les nouvelles technologies ont multiplié les possibilités d'amélioration des processus, la surveillance réglementaire a ralenti leur adoption au sein des laboratoires pharmaceutiques par rapport à d'autres secteurs où la régulation est moins importante. [40]

Comme évoqué dans la partie 1.2.2, les exigences strictes en matière de documentation, d'intégrité des données et de validation des processus créent un environnement où la conformité réglementaire l'emporte sur l'amélioration continue des processus alors même que des outils digitaux peuvent améliorer la qualité et l'efficacité des processus comme évoqué dans la partie 2.6. [40]

Dans cette dernière partie nous allons nous concentrer sur le déploiement d'une stratégie permettant la maitrise des systèmes d'information en matière d'intégrité des données de sa phase de conception à sa phase de déploiement. Cette stratégie est une proposition qui a été élaborée en mode projet et n'est pas représentative de ce qui a été appliquée réellement.

3.1. Objectif

Le projet a été développé avec pour objectif de revendiquer cette industrie 4.0 par la mise en place d'outils tels que :

- la GTC (Gestion technique centralisée),
- l'EMS (Système de supervision des paramètres environnementaux),
- le MES (Logiciel de pilotage de la production),

- l'utilisation d'automates afin d'optimiser les transferts des données des équipements vers d'autres systèmes.

Dans un tel système l'intégrité des données doit absolument être maitrisée tout au long du cycle de vie du produit. Les étapes en aval telles que le stockage, l'utilisation, l'archivage ou la destruction étaient maitrisées par la validation des systèmes informatisés. Le besoin initial était ainsi de réaliser un état des lieux et de maitriser l'intégrité des données en amont, durant les premières étapes du cycle de vie de la donnée. L'objectif était donc de mettre en place un outil :

- qui soit capable d'évaluer la conformité relative à l'intégrité des données des systèmes d'information d'un site de production pharmaceutique,
- qui soit applicable à tous les équipements quel que soit leur niveau de complexité : donnée papier, donnée électronique, présence d'un audit trail, possibilité de réaliser une signature électronique, possibilité de connexion au réseau, niveau d'automatisation, etc,
- et qui soit applicable à des équipements déjà qualifiés.

Pour le bon déroulement de cette implémentation trois objectifs ont été identifiés :

- définir une stratégie de déploiement : Quel type d'outil ? A quelle étape ? Comment ?
- définir les responsabilités : Qui fait quoi ? Quand ?
- définir une grille d'évaluation applicable à tous les équipements du site quel que soit son niveau de complexité : Quel est le niveau de maitrise d'intégrité des données des équipements ?

La gestion du projet s'est faite par application du principe de gestion de risque décrit dans l'ICHQ9. La chronologie des étapes est décrite dans la Figure 18 ci-dessous :

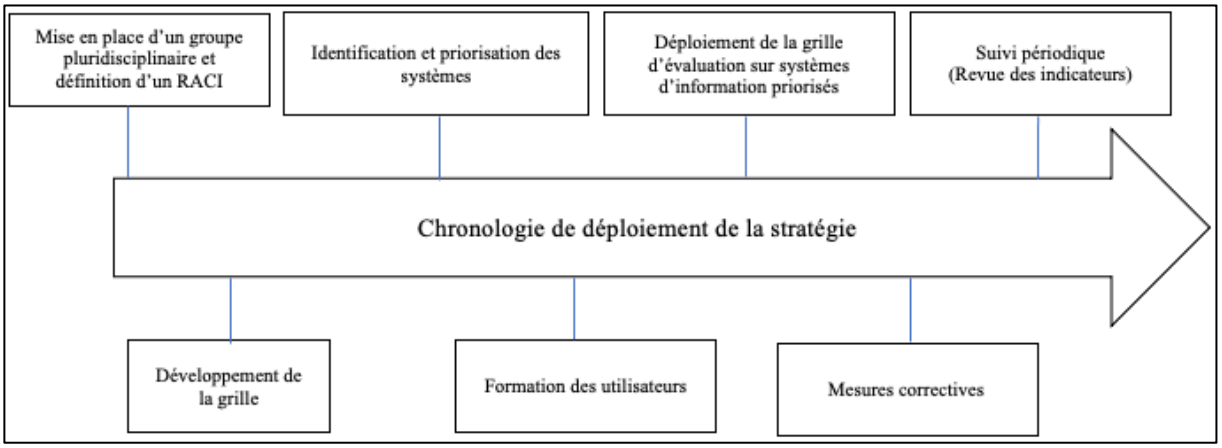


Figure 18 : les étapes chronologiques du déploiement de la grille d'évaluation des systèmes informatisés

3.2. Mise en place d'un groupe pluridisciplinaire et définition des responsabilités

La mise en place d'un groupe pluridisciplinaire est un pré requis à la bonne réussite d'un tel projet afin d'avoir une vision globale de la réglementation, des équipements, de la production et du système qualité.

Ainsi les ateliers à intégrer en priorité seront :

- la maintenance pour l'expertise des équipements,
- la production pour l'expertise fabrication et conditionnement,
- le service utilité pour les équipements supports,
- les responsables de pôle impactés pour évaluer la faisabilité du projet au regard de la charge de déploiement,
- l'assurance qualité,
- la qualification
- et un expert réseau et automatisation.

Le groupe pluridisciplinaire a adapté la stratégie de déploiement, défini les responsabilités, challengé la matrice de priorisation des équipements et établi la grille d'évaluation de maitrise de l'intégrité des données.

Un RACI, également appelé matrice de responsabilité, est l'outil qui a été utilisé afin de définir les responsabilités et les actions associées. Il s'agit d'un outil qui identifie les principaux rôles et responsabilités des utilisateurs par rapport aux tâches d'un projet et permet une représentation visuelle du rôle fonctionnel de chacun. La création de ce tableau permet également d'équilibrer la charge de travail et de définir le décideur (*Accountable*). On identifie 4 types de profils dans un RACI :

- « ***R****esponsible* » doit réaliser la tâche du projet,
- « ***A****ccountable* » est responsable de la réussite de la tâche et est le décideur. Il s'agit du chef de projet,
- « ***C****onsulted* » est consulté pour des détails et des informations supplémentaires sur le sujet,
- « ***I****nformed* » : est informé des mises à jour majeures.

Le tableau ci-dessous décrit le RACI qui a été développé pour ce projet. Il a été élaboré en s'inspirant des principes de maitrise du risque (ICHQ9) : Identification, maitrise et revue du risque. [42]

Tableau 3 : RACI du projet de déploiement d'une démarche sur un site de production pharmaceutique

Action			Maintenance	Production	Laboratoire	Utilités	Responsable de pôle	AQ Produit	AQ Technique	AQ DIM	Qualification	Réseau	Groupe DIM
			Utilisateurs					AQ			DT		
Organisation	Création et mise à jour de la grille		I	I	I	I	I	I	I	A/R	I	I	R
	Identification des Systèmes Automatisés prioritaires soumis au processus		I	I	I	I	R	C	C	A/R	R	R	C
	Planning d'exécution de la grille		I	I	I	I	A/R	I	I	C	I	C	C
Identification et Evaluation Exigences DI	Formation à la grille d'évaluation		I	I	I	I	I	I	I	A/R	I	I	R
	Exécution de la grille d'évaluation	Équipements process	R	R			A	C		C	C	C	I
		Équipements laboratoires			R		A			C		C	I
		Utilités				R	A	I	C	C	C	C	I
	Signature de la grille d'évaluation	Équipements process	I	I			C	A/R		C	C		I
		Équipements laboratoires			I		A/R			C			I
		Utilités				I	C		A/R	C	C		I
Maitrise du risque	Identification des mesures de mitigation / équipement	Équipements process	R	R			A/R	R		C	C	C	I
		Équipements laboratoires			R		A/R			C	C	C	I
		Utilités				R	A/R		R	C	C	C	I
	Validation des mesures de mitigation / équipement	Équipements process					C	C		R	I	I	A/R
		Équipements laboratoires					C			R	I	I	A/R
		Utilités					C		C	R	I	I	A/R
Revue du risque	Suivi du plan d'action	Équipements process						A/R		I			I
		Équipements laboratoires					A/R			I			I

3.3. Développement du protocole de test d'évaluation des systèmes informatisés

Des essais ont été réalisés sur des équipements du site avec deux objectifs principaux :

- déployer l'outil auprès d'unités différentes : sur des systèmes informatisés de production, sur des utilités ou des systèmes du laboratoire de contrôle pour évaluer son applicabilité sur différentes structures,
- déployer la grille sur des équipements :
    - « worst case[1] » qui correspond à un équipement avec un niveau de data integrity faible,
    - et « best case[2] » : qui correspond à un équipement avec un niveau de data integrity élevé.

L'objectif était de recueillir des informations concernant :

- la pertinence des items évalués,
- la compréhension des utilisateurs de la grille par le recueil de feedback, avec pour objectif de reformuler, de simplifier les items non compris et d'élaborer le contenu des formations à venir,
- le temps passé pour exécuter la grille afin de mieux évaluer la charge nécessaire au déploiement
- le temps passé pour élaborer les mesures de mitigation,
- l'applicabilité des mesures de mitigation.

Après validation par le groupe pluridisciplinaire, une phase pilote a été réalisée afin de collecter suffisamment de données représentatives du déploiement et de la stratégie, pour une validation par la direction.

Dans ce cadre, un formulaire à compléter a été distribué aux utilisateurs en charge du déploiement de ces essais afin de collecter :

- un premier retour sur le niveau de conformité des équipements,
- un état d'avancement du déploiement,
- des indicateurs de performance tels que le temps nécessaire à la réalisation de la grille,
- et les points d'amélioration tels que la compréhension des items, l'applicabilité ou la qualité de la formation.

[1] Expression anglaise qui signifie « pire cas »
[2] Expression anglaise qui signifie « meilleur cas »

Le formulaire distribué aux équipes est disponible en Annexe 1.

3.4. Formation du personnel

Une formation des utilisateurs en charge de ces équipements a été réalisée en deux étapes. D'abord une session théorique afin de sensibiliser les opérateurs aux problématiques d'intégrité des données. Cette formation s'est composée :

- de notions générales de data integrity tel que les 9 principes d'ALCOA+,
- d'un rappel de l'importance de la data integrity et des risques associés,
- des exemples d'injonction de l'ANSM,
- des exemples d'écart de data integrity relevés sur le site,
- de la stratégie de déploiement de la grille,
- d'une explication des différents modules de la grille.

Puis une session pratique avec les « producteurs » a finalisé la formation afin d'expérimenter la grille sur un équipement en zone de production avec une revue des items proposés, des non-conformités et des pièces justificatives nécessaires à la validation de ces items.
Les utilisateurs formés ont eu par la suite la charge de déployer l'outil sur les équipements identifiés à risque dans la matrice de priorisation décrite dans la partie 3.5 ci-dessous.
Ce formulaire est disponible en annexe 1. De plus, des revues ont été réalisées à chaque étape du projet afin de corriger ou clarifier les différents items de la grille, la stratégie de déploiement ainsi que les responsabilités associées.

3.5. Priorisation des équipements

Chaque équipement a été priorisé en fonction de son analyse de criticité. Les équipements ont été évalués par 5 questions :

- le système génère t-il de la donnée GxP ?
- le système est-il en contact avec le produit ?
- le système fournit-il des données nécessaires à la libération du produit ?
- le système peut-il contrôler le procédé de façon à influencer la qualité, l'efficacité ou la sécurité du produit ?
- quelle est la fréquence d'utilisation de l'équipement ?

Seuls les équipements générant de la donnée ont été priorisés. Le Tableau 4 ci-dessous représente les critères appliqués et leurs scores associés en fonction du niveau de criticité.

Tableau 4 : Paramètres de l'analyse de risque afin de prioriser les équipements

Criticité	Données générées GxP	Données nécessaires à la libération du produit	Fréquence d'utilisation	Contact direct produit	Influence la qualité, sécurité ou efficacité du produit
Fort	Oui (priorisé)	Oui (10 points)	Plusieurs fois par jours (5 points)	Direct (5 points)	Oui (10 points)
Moyen			Plusieurs fois par semaine (2 points)		
Faible	Non (non priorisé)	Non (1 point)	Quelques fois par mois/an (1 point)	Indirect (1 point)	Non (1 point)

Une somme de tous les paramètres a ensuite été effectuée. La criticité des équipements produisant des données nécessaires à la libération du lot et qui influencent la qualité, la sécurité ou l'efficacité du médicament ont un score deux fois plus important que la criticité des autres paramètres:

[Score données nécessaires à la libération du produit] + [score fréquence d'utilisation] + [score contact direct produit] + [Influence la qualité, sécurité ou efficacité du produit] = Score total

Le score minimal de 4 représente les équipements les moins critiques et le score maximal égal à 30 représente les équipements les plus critiques. Le résultat de cette analyse est décrit dans le Tableau 5 ci-dessous :

Tableau 5 : Résultat de l'analyse de criticité des systèmes informatisés d'un site de production pharmaceutique

Identification du système	Données générées GxP	Données nécessaires à la libération du produit	Fréquence d'utilisation	Contact direct produit	Influence la qualité, sécurité ou efficacité du produit	Score total
Équipement 1	Oui	Oui	Fort	Direct	Oui	30
Équipement 2	Oui	Oui	Fort	Direct	Oui	30
Équipement 3	Oui	Oui	Fort	Direct	Oui	30
Équipement 4	Oui	Non	Fort	Direct	Oui	22
Équipement 5	Oui	Non	Fort	Direct	Oui	22
Équipement 6	Oui	Non	Fort	Direct	Oui	22
Équipement 7	Oui	Oui	Fort	Direct	Non	22
Équipement 8	Oui	Oui	Fort	Direct	Non	22
Équipement 9	Oui	Oui	Fort	Direct	Non	22
Équipement 10	Oui	Non	Fort	Direct	Non	12
Équipement 11	Oui	Non	Fort	Direct	Non	12
Équipement 12	Oui	Non	Fort	Direct	Non	12
Équipement 13	Oui	Non	Faible	Indirect	Non	4
Équipement 14	Oui	Non	Faible	Indirect	Non	4
Équipement 15	Oui	Non	Faible	Indirect	Non	4
Équipement 16	Oui	Non	Faible	Indirect	Non	4
Équipement 17	Oui	Non	Faible	Indirect	Non	4
Équipement 18	Oui	Non	Faible	Indirect	Non	4

Les équipements ayant un score > 20 ont été priorisés pour le déploiement du protocole de test.

3.6. Déploiement du protocole de test d'évaluation sur les systèmes informatisés

L'arbre décisionnel de déploiement du protocole de test d'évaluation est décrit dans l'Annexe 2. Stratégie d'implémentation du protocole de test data integrity sur un site de production pharmaceutique. Cette stratégie permet d'appliquer le protocole de test :

- aux équipements pour lesquels le cahier des charges n'est pas encore approuvé en intégrant les items directement aux cahiers des charges de l'équipement dès la phase de conception avec le fournisseur du système,
- aux équipements pour lesquels le cahier des charges est approuvé mais le protocole de qualification n'est pas encore rédigé en intégrant les tests lors des phases de qualification de performance,

- aux équipements actuellement qualifiés en appliquant le protocole de test tel que décrit dans la partie 3.7.

3.7. Protocole de test d'évaluation des systèmes informatisés

3.7.1. Organisation générale

L'outil proposé pour évaluer l'intégrité des données générées, enregistrées et transférées est sous la forme d'une grille d'évaluation modulable en fonction de la plus ou moins grande complexité de l'équipement. Elle a été conçue avec 10 modules portant chacun sur un thème :

- un premier module obligatoire qui permet de s'assurer de la conformité réglementaire minimale pour un système,
- 9 thèmes optionnels dont l'applicabilité dépend de la complexité technique de l'équipement. Par exemple seuls certains équipements ont la possibilité d'appliquer une signature électronique. Pour les équipements qui n'en sont pas dotés, ce module ne s'appliquera pas. A chaque fois qu'un module ne sera pas appliqué, il sera nécessaire de donner une justification claire et précise afin de permettre à l'approbateur du protocole de test de comprendre les choix des utilisateurs.

La Figure 19 ci-dessous décrit la structure du protocole de test et des modules :

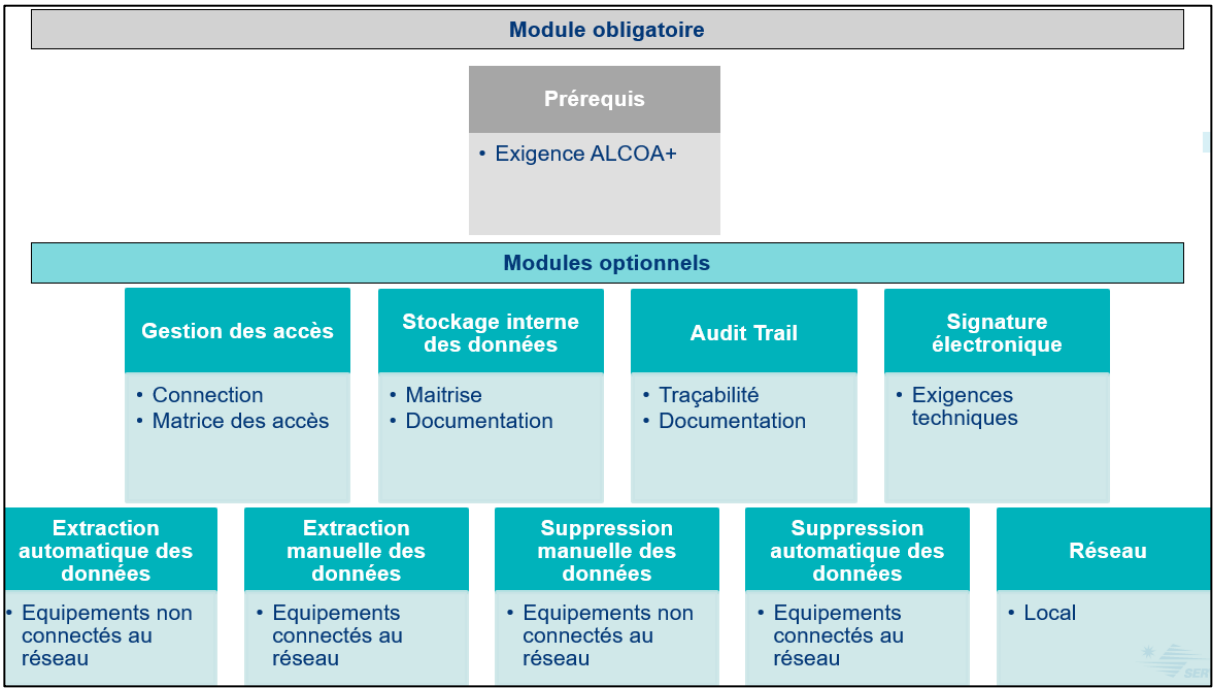


Figure 19 : organisation du protocole de test d'évaluation

Chaque module est composé d'un nombre prédéfini d'items. Lorsque le module est applicable alors il sera obligatoire d'appliquer la totalité des items le composant. Pour chaque item, il est précisé :

- la référence de l'item,

- l’exigence attendue,
- la conformité avec comme possibilité « conforme » ou « non-conforme »,
- un commentaire optionnel en cas de non-conformité ou lorsqu’une précision est nécessaire.

Chaque non-conformité doit être justifiée et faire l'objet d'une action corrective et/ou préventive. Les preuves demandées sont à joindre au rapport.

3.7.2. Module 1 - Exigence ALCOA+

Ce premier module est obligatoire. Il comprend 20 items qui reprennent les recommandations retrouvées dans les différentes lignes directrices parues ces dernières années. Ce module est décrit dans le Tableau 6 ci-dessous :

Tableau 6 : module exigence ALCOA+

Item	Exigences
1.1	Il est possible d'associer un utilisateur avec l'opération qu'il a effectuée. (Attribuable)
1.2	La donnée est associée à sa source. (Attribuable)
1.3	Les données générées sont lisibles. (Lisible)
1.4	La date (année, mois et jour) et l'heure (heure, minute et seconde) d'enregistrement des données sont connues. (Contemporaine)
1.5	Les données sont créées au moment de l'opération. (Contemporaine)
1.6	Les modifications de données sont documentées. (Précise)
1.7	Les données sont enregistrées dans un format pérenne pendant la durée de rétention prévue. (Pérenne)
1.8	Les données originales et les métadonnées sont enregistrées dans un format lisible et sont disponibles pendant la durée de rétention prévue (Originale, Complète et Disponible)
1.9	Les données sont horodatées et dans l’ordre prévu (Cohérent)
1.10	Les personnes intervenant dans le système (conception, maintenance, utilisation) sont formées et/ou sensibilisées pour la réalisation de leurs tâches (fiche de formation, de poste, …)
1.11	Le système possède un mode dégradé dans la cadre de la continuité d'activité (par exemple : mode dégradé papier, mode dégradé interne, arrêt de la production ...)
1.12	Le système est périodiquement qualifié/validé et en cohérence avec la procédure en vigueur.
1.13	Il existe un processus permettant l'archivage des données du système.
1.14	La sauvegarde et la restauration du système sont vérifiées périodiquement
1.15	La déconnexion est automatique et se fait après un temps de non-utilisation défini (dossier de paramétrage).
1.16	L'exactitude de l'heure est vérifiée périodiquement

Item	Exigences
1.17	Les données critiques du process sont auditées à fréquence définie.
1.18	L'extraction et la sauvegarde sont un prérequis à la suppression.
1.19	Les droits/fonctions sont défini(e)s dans la matrice des accès du système.
1.20	La revue du paramétrage est réalisée périodiquement et inscrite dans une procédure approuvée.

3.7.3. Module 2 - Gestion des accès

La gestion des accès correspond aux mesures prises pour autoriser les personnes à accéder au système. Pour réaliser ce module, le système doit répondre positivement à la question suivante : le système possède-t-il une gestion des accès ?

Ce module comprend 7 items qui sont décrits dans le Tableau 7 ci-dessous :

Tableau 7 : module de gestion des accès

Item	Exigences
2.1	La connexion au système nécessite un identifiant et un mot de passe.
2.2	Après un nombre défini de tentatives de connexions erronées le compte se verrouille.
2.3	Le système permet d'avoir à minima 2 profils d'utilisateur avec des droits d'accès adaptés à chaque profil (utilisateur et administrateur).
2.4	La matrice des accès est définie et adaptée au métier.
2.5	Les paramètres et les données peuvent être modifiées uniquement par des personnes habilitées.
2.6	Le mot de passe est sécurisé : - renouvellements périodiques - Exigence d'une complexité du mot de passe - Non-réutilisation des anciens mots de passe
2.7	Toute modification des accès est tracée.

3.7.4. Module 3 - Stockage interne des données

Le stockage est dit interne lorsque les données sont stockées directement sur l'ordinateur et non sur un serveur. Pour réaliser ce module, le système doit répondre positivement à la question suivante : le système possède-t-il un système de stockage interne des données ?

Ce module comprend 2 items qui sont décrits dans le Tableau 8 ci-dessous :

Tableau 8 : module stockage interne des données

Item	Exigences
3.1	L'accès à ces données est limité et sécurisé.
3.2	La limite de stockage est connue et une procédure est mise en place pour assurer périodiquement le transfert de ces données vers le site de stockage et d'archivage.

3.7.5. Module 4 - Audit trail

Un audit trail est un enregistrement des changements qui ont été effectués sur une base de données ou un dossier. Pour réaliser ce module, le système doit répondre positivement à la question suivante : le système possède-t-il un audit trail ?

Ce module comprend 6 items qui sont décrits dans le Tableau 9 ci-dessous :

Tableau 9 : module audit trail

Item	Exigences
4.1	Il est uniquement possible de supprimer et de désactiver un audit trail par une personne indépendante au processus. Les actions sont procédurées.
4.2	L'action tracée dans l'audit trail est clairement identifiée.
4.3	L'auteur de l'action est clairement identifié.
4.4	L'ancienne et la nouvelle valeur de l'objet est disponible.
4.5	La raison/un commentaire est demandé lors d'une modification ou d'une suppression de la donnée.
4.6	L'horodatage contient à minima les éléments suivants pour un format d'horodate locale : - L'année, - Le mois, - Le jour - L'heure - Les minutes - Les secondes - (UTC)

3.7.6. Module 5 - Signature électronique

La signature électronique a la même valeur que la signature manuscrite. Pour réaliser ce module, le système doit répondre positivement à la question suivante : la signature électronique est-elle appliquée ?

Ce module comprend 6 items qui sont représentés dans Tableau 10 ci-dessous :

Tableau 10 : module de signature électronique

Item	Exigences
5.1	Le système enregistre les éléments suivants dans le cadre du processus de signature électronique : - Horodatage - ID utilisateur et nom complet du ou des signataires - L'objet de la signature, sur une liste préconfigurée de raisons possibles (création, vérification, approbation) - En option, un commentaire supplémentaire du signataire lors de l'exécution - Référence de l'équipement où la signature a été faite
5.2	La signature électronique nécessite : - L'identification de l'utilisateur, - Le mot de passe associé.
5.3	La signature électronique est liée de façon irréversible à l'enregistrement électronique et ne peut pas être séparée, copiée ou transférée de son document d'origine.
5.4	Le système fait la distinction entre une signature électronique attribuée et liée à un enregistrement électronique, et une autorisation d'accès contrôlé au système, par exemple pour ouvrir une vanne ou pour planifier une recette par lots.
5.5	Des actions de signature électronique par simple ou double authentification sont possibles (suivant la criticité des données).
5.6	Les informations associées à la signature sont toujours présentes sur le support papier et/ou numérique.

3.7.7. Module 6 - Extraction manuelle des données

Une extraction est dite manuelle lorsque les données sont collectées ou récupérées grâce à une intervention humaine. Pour réaliser ce module, le système doit répondre positivement à la question suivante : l'extraction des données est-elle manuelle ?

Ce module comprend 2 items qui sont représentés dans le Tableau 11 ci-dessous :

Tableau 11 : module d'extraction manuelle des données

Item	Exigences
6.1	L'extraction des données est procédurée et approuvée (archivage, sauvegarde, exploitation).
6.2	L'extraction des données est adaptée à la capacité de stockage du système.

3.7.8. Module 7 - Extraction automatique des données

Lorsque les données sont collectées ou récupérées sans intervention humaine, l'extraction des données est dite automatique. Pour réaliser ce module, le système doit répondre positivement à la question suivante : l'extraction des données est-elle automatique ?

Ce module comprend 5 items qui sont représentés dans le Tableau 12 ci-dessous :

Tableau 12 : module d'extraction automatique des données

Item	Exigences
7.1	L'extraction des données est procédurée et approuvée (archivage, sauvegarde, exploitation)
7.2	Le système d'extraction des données est validé
7.3	L'extraction des données est adaptée à la capacité de stockage du système
7.4	Le transfert des données possède un mode dégradé de fonctionnement
7.5	Une alerte doit notifier un dysfonctionnement de l'extraction du système

3.7.9. Module 8 - La suppression manuelle des données

Lorsque les données peuvent être supprimées par une intervention humaine, la suppression est dite manuelle. Pour réaliser ce module, le système doit répondre positivement à la question suivante : la suppression des données est-elle manuelle ?

Cet item comprend 2 items qui sont représentés dans Tableau 13 ci-dessous :

Tableau 13 : module de suppression manuelle des données

Item	Exigences
8.1	La suppression est procédurée et approuvée
8.2	La suppression est uniquement possible par un profil défini indépendant au processus métier

3.7.10. Module 9 - La suppression automatique des données

La suppression est dite automatique lorsque les données sont supprimées sans intervention humaine. Pour réaliser ce module, le système doit répondre positivement à la question suivante : la suppression des données est-elle automatique (sans intervention) ?

Ce module comprend 2 items qui sont représentés dans le Tableau 14 ci-dessous :

Tableau 14 : module de suppression automatique des données

Item	Exigences
9.1	La suppression est procédurée et approuvée.
9.2	L'outil de suppression utilisé est validé.

3.7.11. Module 10 – La connexion au réseau

Un réseau est un ensemble d'équipement reliés entre eux pour échanger des informations. Pour réaliser ce module, le système doit répondre positivement à la question suivante : la suppression des données est-elle automatique (sans intervention) ?

Ce module comprend 1 item qui est représenté dans le Tableau 15 ci-dessous.

Tableau 15 : module de connexion au réseau

Item	Exigences
10.1	L'ensemble du système a une synchronisation avec un serveur de temps de référence.

3.8. Synthèse d'évaluation

Chaque protocole de test possède une partie « synthèse » pour avoir une vision d'ensemble des non-conformités et des conformités sous la forme d'un tableau comme illustré dans le Tableau 16 ci-dessous. Ce tableau représente la première partie de la synthèse. Pour chaque item nous aurons :

- la réponse qui indique si le thème a été appliqué pour l'équipement ciblé,
- le score de conformité qui représente la somme des items conformes,
- le score de non-conformité qui représente la somme des items non conformes,
- le total de la partie qui représente le nombre d'items totaux dans le module,
- et le pourcentage de conformités du module.

Tableau 16 : Tableau de synthèse du protocole de test d'évaluation des systèmes informatisés

SYNTHÈSE DE L'ÉVALUATION						
Partie	**Réponses**	**Nb de conformes**	**Nb de non-conformités**	**Non applicables**	**Total**	**Pourcentage**
1. Exigences ALCOA+ (Prérequis)	Oui	14	6	0	20	70,00%
2. Le système possède-t-il une gestion d'accès ?	Oui	4	3	0	7	57,14%
3. Le système possède-t-il un système de stockage interne des données ?	Oui	1	1	0	2	50,00%
4. Le système possède-t-il un audit trail ?	Oui	5	1	0	6	83,33%
5. La signature électronique est-elle appliquée ?	Non	0	0	6	0	NA
6. L'extraction des données est-elle manuelle ? (Action physique)	Oui	1	0	0	2	50,00%
7. L'extraction des données est-elle automatique ?	Non	0	0	5	0	NA
8. La suppression des données est-elle manuelle ? (Action physique)	Oui	2	0	0	2	100,00%
9. La suppression des données est-elle automatique ? (Sans intervention)	Non	0	0	2	0	NA
10. Le système est-il connecté au réseau ?	Non	0	0	1	0	NA
Total		**27**	**11**	**14**	**40**	**67,50%**

Ensuite une présentation graphique de cette synthèse a été proposée afin d'avoir un indicateur visuel simple et intuitif comme on peut le voir dans la Figure 20 ci-dessous.

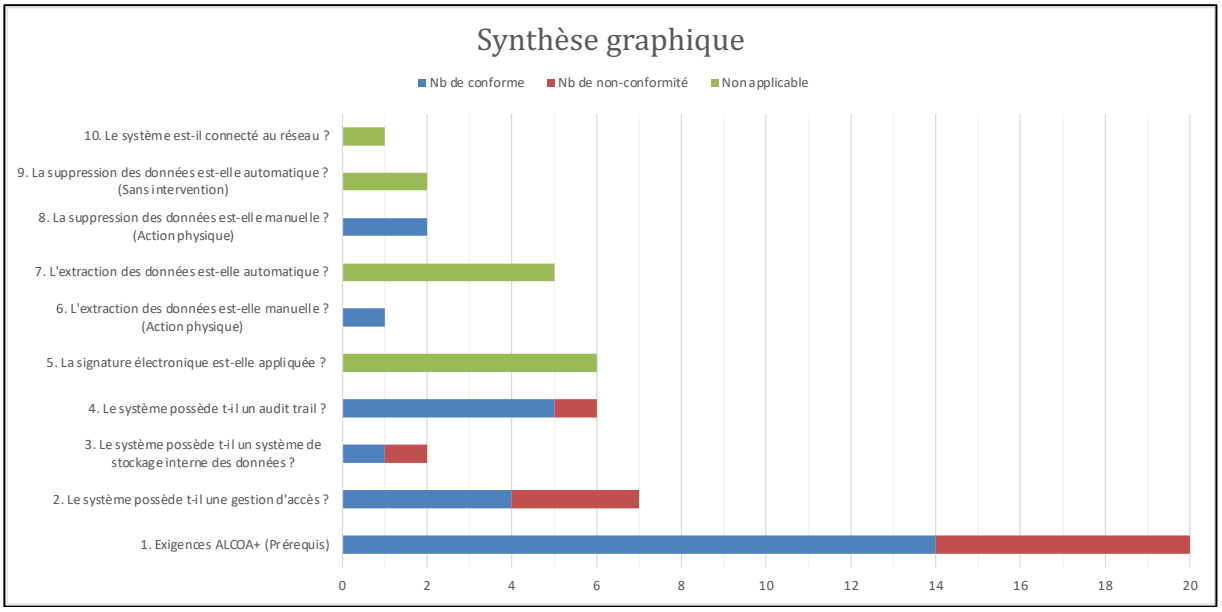


Figure 20 : graphique de synthèse du protocole de test d'évaluation des systèmes informatisés

Ces indicateurs permettront de mettre en évidence les tendances des équipements en fonction des unités du site de production. Les récurrences pourront être identifiées et il sera possible de se concentrer sur les 20% de causes qui entrainent 80% des non-conformités (Pareto).
Ce protocole de test pourra donc servir de données d'entrée pour définir les axes prioritaires de demain sur le site en matière de gouvernance des données.

3.9. Retour d'expérience

Le protocole de test a permis de former les équipes, y compris celles qui ne participaient pas au déploiement du protocole. Ainsi l'ensemble du personnel a été impliqué et sensibilisé aux notions d'intégrité des données. L'importance d'un audit trail ou d'une matrice des accès maitrisée a été comprise par chacun. De plus l'application de ce protocole a nécessité une coopération pluridisciplinaire (utilisateurs, automaticiens, maintenance ou fournisseurs). Les non-conformités révélées ont permis d'initier des réflexions et des discussions pour améliorer l'intégrité des données au sein de l'unité.

Les points positifs ont été :

- la maitrise de ces équipements grâce à l'identification de ces non-conformités et la mise en place d'action correctives et préventives le cas échant,
- la rapidité de déploiement sur un équipement : environ 1h30 pour réaliser l'évaluation,
- l'adaptabilité de la grille d'évaluation pour l'intégration de la data integrity dès les phase de conception de l'équipement et jusqu'à la qualification de performance, ce qui a permis de couvrir l'ensemble du parc d'équipement du projet,
- la mise en place d'indicateurs de performance.

Des points de vigilance pour la mise en place des items ont été identifiés :

- la nécessité d'avoir des items clairs qui ne laissent pas la place à l'interprétation par les utilisateurs,
- la durée un peu trop courte de la formation qui a pu entrainer un ralentissement du déploiement par manque de compréhension des items et des enjeux par les utilisateurs,
- l'importance de la charge associée au vu du nombre d'équipements sur le site. La priorisation des équipements est un pré requis au bon déploiement de ce protocole.

3.10. Action et validation des actions correctives

L'étape suivante consiste à définir les mesures correctives et préventives afin de maitriser les non-conformités révélées durant le déploiement du protocole. Les actions de mitigation appliquées sont celles décrites dans la partie II. Il pourra s'agir de trois types d'actions correctives ou préventives :

- les actions organisationnelles : mise en place de procédures et mode opératoire, formation du personnel, action de sécurisation, etc.

- les actions techniques : intégration de la data integrity dès la qualification de performance, mise en place d'audit trail, connexion au réseau des équipements, prise en compte de la data integrity dès la phase de conception, automatisation des transferts des données, mise en place de dossiers de lots électroniques, etc.
- les actions de surveillance : audit interne, audit externe et auto-inspection.

Elles devront se faire en présence de tous les acteurs concernés :

- la maintenance pour la faisabilité technique de l'action corrective si elle est de nature à modifier le système,
- la production pour la faisabilité des actions au regard de l'impact sur le processus de production,
- les responsables de pôles impactés pour évaluer la faisabilité du projet au regard de la charge de déploiement,
- l'assurance qualité pour le respect des recommandations,
- la qualification si les actions impactent l'état validé du système,
- et une expertise réseau et automatisme.

Ces actions correctives et préventives devront tenir compte du type de données (manuscrite ou électronique) et de la faisabilité des actions techniques. Les actions techniques devront être priorisées aux actions organisationnelles et de surveillance car elles limiteront le facteur humain, dans un monde où le volume de données stockées dans l'environnement informatique d'une organisation continue de croître de façon exponentielle.
Le choix des action correctives et préventives devra être validé par la direction et s'appuyer sur les indicateurs obtenus grâce aux évaluations réalisées sur le site. En effet la standardisation du protocole d'évaluation à tous les équipements facilite la mise en place d'indicateurs de performance du site. Les éléments de sortie de la grille d'évaluation tels que le pourcentage de non-conformités en fonction du thème et de l'atelier, deviennent alors des éléments d'entrée aux indicateurs de performances du site de production permettant d'identifier les récurrences afin de se concentrer sur les 20% de causes qui entrainent 80% des non-conformités au travers d'un diagramme de Pareto.

De nombreuses lignes de conduites et référentiels ont été publiés ces dernières années pour guider les industriels. Certaines guidelines permettront également d'aider à la mise en place des actions organisationnelles, techniques et de surveillance, les plus exhaustives étant :

- *Guideline on data integrity* de l'Organisation Mondiale de la Santé, [4]
- *Good practices for data management and integrity in regulated GMP/GDP environments* du PIC/S. [5]

3.11. Suivi périodique et revue des indicateurs

La promotion d'une culture centrée sur la maitrise de l'intégrité des données ainsi que la mise en œuvre des mesures organisationnelles, techniques et de surveillance qui garantissent l'intégrité des données relèvent de la responsabilité de la direction et requièrent la participation et l'engagement du personnel à tous les niveaux de l'entreprise. La direction doit donc s'assurer de l'avancement de la mise en œuvre des actions correctives et préventives au travers des bilans périodiques et annuels. Les indicateurs suivants peuvent être pertinents dans le cadre de cette stratégie :

- Pourcentage d'équipements prioritaires évalués,
- Pourcentage d'actions correctives/préventives réalisées,
- Score moyen des équipements par thème,
- Score moyen des équipements par atelier,
- Score moyen des équipements par étape de fabrication,

Ces revues pourront être réalisées par unité et impliquer tous les acteurs, des managers aux opérateurs.

Conclusion

Alors que le volume de données stockées dans l'environnement informatique d'une organisation pharmaceutique croît de façon exponentielle en raison de la progression des nouvelles technologies, la tâche de gestion et de contrôle de l'intégrité de ces données devient de plus en plus complexe et n'est que trop rarement prise en considération. Or les entreprises dépendent constamment des données relatives à leurs opérations pour leur prise de décision.

Les organisations doivent donc absolument construire une politique d'intégrité des données et s'assurer qu'elle soit correctement mise en œuvre, comprise et acceptée dans toute l'entreprise. Les données étant devenues une ressource organisationnelle inestimable, garantir leur intégrité est nécessaire. Plus celle-ci sera maitrisée sur un site de production pharmaceutique, plus elle aura un impact positif sur la qualité, la sécurité et l'efficacité du médicament.

Les outils automatisés contribuent à cette amélioration, en éliminant les processus manuels, en augmentant la précision et en réduisant le coût de maitrise. Grâce aux outils automatisés de l'intégrité, les organisations peuvent facilement minimiser les temps d'arrêt, améliorer les processus et permettre aux données d'éclairer la prise de décision. Bien que les coûts d'investissement initiaux soient élevés, les gains d'efficacité potentiels sont suffisants pour assurer un retour sur investissement important.

Un tel système automatisé et connecté ne devra tout de même pas se substituer totalement à l'humain pour la prise de décision, notamment en cas de non-conformités rencontrées sur le site de production. Néanmoins un système où la maitrise des données est contrôlée de bout en bout pourra par la suite permettre l'implémentation de la libération paramétrique des lots de production tel qu'indiqué dans l'annexe 17 des GMP.

En élaborant une stratégie appropriée autour de l'intégrité des données, les entreprises s'assurent de prendre des décisions basées sur des données fiables.

Références bibliographiques

[1] European Medicines Agency, « Guidance on good manufacturing practice and distribution practice: Questions answers ». 17 septembre 2018. Consulté le: 17 août 2022. [En ligne]. Disponible sur: https://www.ema.europa.eu/en/human-regulatory/research-development/compliance/good-manufacturing-practice/guidance-good-manufacturing-practice-good-distribution-practice-questions-answers

[2] Tulip, « Pharma 4.0: The Ultimate Guide to Digital Transformation For Life Sciences Manufacturers ». Consulté le: 18 février 2023. [En ligne]. Disponible sur: https://tulip.co/ebooks/pharma-4-0/

[3] N. A. Charoo, M. A. Khan, et Z. Rahman, « Data integrity issues in pharmaceutical industry: Common observations, challenges and mitigations strategies », janv. 2023, Consulté le: 4 mars 2023. [En ligne]. Disponible sur: https://pubmed.ncbi.nlm.nih.gov/36529357/

[4] Organisation Mondiale de la santé, « Guideline on data integrity ». 1 juin 2021. Consulté le: 20 octobre 2022. [En ligne]. Disponible sur: https://cdn.who.int/media/docs/default-source/medicines/norms-and-standards/guidelines/trs966-annex05-fr-who-record-management-practices.pdf?sfvrsn=6218a4e6_4&download=true

[5] Pharmaceutical Inspection Convention, « Good practices for data management and integrity in regulated GMP/GDP environments ». 1 juin 2021. Consulté le: 6 octobre 2022. [En ligne]. Disponible sur: https://picscheme.org/docview/4234

[6] European Medicines Agency, « Data integrity (New August 2016) ». août 2016. Consulté le: 17 septembre 2022. [En ligne]. Disponible sur: https://www.ema.europa.eu/en/human-regulatory/research-development/compliance/good-manufacturing-practice/guidance-good-manufacturing-practice-good-distribution-practice-questions-answers#data-integrity-(new-august-2016)-section

[7] Mark Durivage, « Data Integrity for the FDA Regulated Industry ». 1 décembre 2019. Consulté le: 4 mars 2022. [En ligne]. Disponible sur: https://qscompliance.com/wp-content/uploads/2019/01/ALCOA-Principles.pdf

[8] L'usine Nouvelle, « L'ingénierie pharmaceutique relève le défi de la digitalisation », oct. 2022, Consulté le: 16 octobre 2022. [En ligne]. Disponible sur: https://www.usinenouvelle.com/article/l-ingenierie-pharmaceutique-releve-le-defi-de-la-digitalisation.N2056902

[9] GMP Expert Committee, Quality and Technology Committee, Japan Pharmaceutical Manufacturers Association, « Education and Training Materials ». mars 2019. Consulté le: 3 janvier 2023. [En ligne]. Disponible sur: https://www.jpma.or.jp/english/reports/quality_technology_committee/di.html

[10] lbarrera, « Qu'est-ce que l'exactitude des données, pourquoi c'est important et comment les entreprises peuvent s'assurer qu'elles disposent de données exactes. » 25 septembre 2020. Consulté le: 12 septembre 2022. [En ligne]. Disponible sur: https://dataladder.com/fr/quest-ce-que-lexactitude-des-donnees-pourquoi-cest-important-et-comment-les-entreprises-peuvent-sassurer-quelles-disposent-de-donnees-exactes/

[11] European commission, « Annex 11: Computerised Systems ». 30 juin 2011. Consulté le: 4 décembre 2022. [En ligne]. Disponible sur: https://health.ec.europa.eu/system/files/2016-11/annex11_01-2011_en_0.pdf

[12] Center for Food Safety and Applied Nutrition, Center for Veterinary Medicine, Office of Regulatory Affairs, Center for Drug Evaluation and Research, Center for Devices and Radiological Health, et Center for Biologics Evaluation and Research, « Part 11, Electronic Records; Electronic Signatures - Scope and Application ». 6 novembre 2020. Consulté le: 5 février 2023. [En ligne]. Disponible sur: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/part-11-electronic-records-electronic-signatures-scope-and-application

[13] European commission, « Chapter 4: Documentation ». 30 juin 2011. Consulté le: 10 décembre 2022. [En ligne]. Disponible sur: https://health.ec.europa.eu/system/files/2016-11/chapter4_01-2011_en_0.pdf

[14] European commission, « Chapter 5: Production ». 13 août 2014. Consulté le: 26 février 2022. [En ligne]. Disponible sur: https://health.ec.europa.eu/system/files/2016-11/chapter_5_0.pdf

[15] European commission, « Chapter 6: Quality Control ». 28 mars 2014. Consulté le: 20 mars 2022. [En ligne]. Disponible sur: https://health.ec.europa.eu/system/files/2016-11/2014-11_vol4_chapter_6_0.pdf

[16] Medicines & Healthcare products Regulatory Agency (MHRA), « 'GXP' Data Integrity Guidance and Definitions.pdf ». Consulté le: 28 janvier 2023. [En ligne]. 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

[17] Organisation mondiale de la santé, « Guideline on data integrity ». Consulté le: 2 août 2021. [En ligne]. Disponible sur: https://cdn.who.int/media/docs/default-source/medicines/norms-and-standards/current-projects/qas19-819-rev1-guideline-on-data-integrity.pdf?sfvrsn=653c05c0_2

[18] Pharmaceutical Inspection Convention and Pharmaceutical Inspection Co-operation Scheme, « Good practices for data management and integrity in regulated gmp/gdp environments ». Consulté le: 2 août 2021. [En ligne]. Disponible sur: https://picscheme.org/docview/4234

[19] International Society for Pharmaceutical Engineering, « GAMP 5 Guide: Compliant GxP Computerized Systems ». Consulté le: 2 août 2021. [En ligne]. Disponible sur: https://ispe.org/publications/guidance-documents/gamp-5.

[20] U. S. C. H. C. on E. and C. S. on H. and the Environment, *Penalties for Illegal Activities in the Approval of Drugs: Hearing Before the Subcommittee on Health and the Environment of the Committee on Energy and Commerce, House and Representatives, One Hundred First Congress, Second Session, on H.R. 4810 ... June 28, 1990*. U.S. Government Printing Office, 1990.

[21] Wikipedia, « Mylan ». 12 janvier 2023. Consulté le: 28 janvier 2023. [En ligne]. Disponible sur: https://en.wikipedia.org/w/index.php?title=Mylan&oldid=1133167219

[22] Baltimore Sun, « 4 charged in continuing generic-drug probe Ex-Vitarine vice president given 27-month prison term in cover-up. » 6 septembre 1991. Consulté le: 18 février 2023. [En ligne]. Disponible sur: https://www.baltimoresun.com/news/bs-xpm-1991-09-06-1991249211-story.html

[23] Deborah Mesce, « Federal Approval of Generics Fell Sharply After Scandal | AP News ». 18 janvier 1990. Consulté le: 1 février 2023. [En ligne]. Disponible sur: https://apnews.com/article/482892c825958399de8367202f860b04

[24] Bowman Cox, « US FDA Decides Against Zolgensma Data Integrity Penalties As Novartis Bureaucratizes AveXis ». 1 avril 2020. Consulté le: 16 octobre 2022. [En ligne]. Disponible sur: https://pink.pharmaintelligence.informa.com/PS141967/US-FDA-Decides-Against-Zolgensma-Data-Integrity-Penalties-As-Novartis-Bureaucratizes-AveXis

[25] B. Nowatzke, « The Novartis Data Scandal Explained », 12 août 2019. Consulté le: 18 février 2023. [En ligne]. Disponible sur: https://www.pearlpathways.com/the-novartis-data-scandal-explained/

[26] Angus Liu, « Novartis to FDA: Ousted AveXis execs doctored Zolgensma data themselves ». 24 septembre 2019. Consulté le: 16 novembre 2022. [En ligne]. Disponible sur: https://www.fiercepharma.com/pharma/ousted-avexis-execs-altered-or-instructed-others-to-alter-zolgensma-data-novartis-form-483

[27] Food and Drug Administration, « DuPont Nutrition USA Inc. - 627211 - 12/02/2022 ». FDA, 20 décembre 2022. Consulté le: 22 janvier 2023. [En ligne]. Disponible sur: https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/warning-letters/dupont-nutrition-usa-inc-627211-12022022

[28] Food and Drug Administration, « Warning Letters ». FDA, 11 février 2022. Consulté le: 4 février 2023. [En ligne]. Disponible sur: https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/compliance-actions-and-activities/warning-letters

[29] Organisation Mondiale de la Santé, « Guideline on data integrity ». Consulté le: 17 janvier 2023. [En ligne]. Disponible sur: https://www.who.int/docs/default-source/medicines/norms-and-standards/current-projects/qas19-819-rev1-guideline-on-data-integrity.pdf

[30] Ympronta srl, Info Ympronta, « What is data integrity in healthcare : understanding complex regulations and designing an effective implementation strategy within a short time (part 1) ». 13 février 2022. Consulté le: 28 janvier 2023. [En ligne]. Disponible sur: https://www.ympronta.it/en/blog/ympronta-blog-1/data-integrity-in-pharmaceutical-industry-2

[31] Agence National de Sécurité du Médicament et des produits de santé, « Synthèses d'inspection des médicaments ». 26 novembre 2020. Consulté le: 28 janvier 2023. [En ligne]. Disponible sur: https://ansm.sante.fr/documents/reference/syntheses-dinspection-des-medicaments

[32] Committee for Human Medicinal Products, « ICH guideline Q9 on quality risk management ». septembre 2015. Consulté le: 25 novembre 2022. [En ligne]. Disponible sur: https://www.ema.europa.eu/en/documents/scientific-guideline/international-conference-harmonisation-technical-requirements-registration-pharmaceuticals-human-use_en-3.pdf

[33] 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), et Center for Veterinary Medicine (CVM), « Data Integrity and Compliance With CGMP Guidance for Industry », Consulté le: 4 mai 2022. [En ligne]. Disponible sur: https://www.fda.gov/files/drugs/published/Data-Integrity-and-Compliance-With-Current-Good-Manufacturing-Practice-Guidance-for-Industry.pdf

[34] Amina HABIB ZAHMANI, Mokhtar HABIB ZAHMANI, « La validation des systèmes informatisés dans l'industrie pharmaceutique ». Consulté le: 3 mars 2023. [En ligne]. Disponible sur: https://www.oralogsoft.com/static/La%20validation%20des%20SI.524fe271.pdf

[35] European commission, « Annex 15: Qualification and Validation ». 30 mars 2015. Consulté le: 3 novembre 2022. [En ligne]. Disponible sur: https://health.ec.europa.eu/system/files/2016-11/2015-10_annex15_0.pdf

[36] Les Laboratoires Servier Industrie, « Groupe Data Integrity Management ».

[37] Agence Nationale de Sécurité du Médicament et des produits de santé, « Guide des bonnes pratiques de fabrication.pdf ». Consulté le: 29 janvier 2023. [En ligne]. Disponible sur: https://ansm.sante.fr/uploads/2020/10/20/2019-guide-bpf-mai-2019-3.pdf

[38] Titan HQ, « Les attaques contre l'intégrité des données s'intensifient – Comment s'en protéger ? » 29 mai 2019. Consulté le: 25 octobre 2022. [En ligne]. Disponible sur: https://www.titanhq.fr/blog/attaques-contre-integrite-donnees-intensifient-comment-proteger/

[39] David Jensen, « Recommandation de la FDA : questions et réponses sur la Data Integrity ». Consulté le: 14 novembre 2022. [En ligne]. Disponible sur: https://apsalys.com/2018/01/12/recommandation-de-fda-questions-reponses-data-integrity/

[40] Patrick Lemay, « Principes de l'ALCOA : Guide de l'intégrité des données pour les fabricants du secteur des sciences de la vie ». 29 juin 2022. Consulté le: 20 décembre 2022. [En ligne]. Disponible sur: https://tulip.co/fr/blog/alcoa-principles-a-guide-to-data-integrity/

[41] IBM, « What is Industry 4.0? » Consulté le: 18 février 2023. [En ligne]. Disponible sur: https://www.ibm.com/topics/industry-4-0

[42] Committee for Human Medicinal Products, « ICH guideline Q9 on quality risk management ». September 2015. Consulté le: 22 décembre 2022. [En ligne]. Disponible sur: https://www.ema.europa.eu/en/documents/scientific-guideline/international-conference-harmonisation-technical-requirements-registration-pharmaceuticals-human-use_en-3.pdf

Annexes

Annexe 1. Questionnaire d'évaluation de la formation sur l'intégrité des données

Feedback grille d'évaluation data integrity

Le sondage prendra environ 12 minutes.

...

Bonjour Arnaud. Lorsque vous enverrez ce formulaire, son propriétaire pourra voir votre nom et votre adresse de courrier.

* Obligatoire

1. A combien estimez-vous votre niveau de connaissance concernant les exigences liées à l'intégrité des données **avant** la formation et le déploiement de la grille ? *

0	1	2	3	4	5	6	7	8	9	10

Aucune connaissance — Expert

2. Justification : *

Entrez votre réponse

3. A combien estimez-vous votre niveau de connaissance concernant les exigences liées à l'intégrité des données **après** la formation et le déploiement de la grille ? *

0	1	2	3	4	5	6	7	8	9	10

Aucune connaissance — Expert

4. Justification : *

Entrez votre réponse

5. Niveau d'appréciation concernant la formation théorique : *

0	1	2	3	4	5	6	7	8	9	10

A revoir — Très bien

6. Lors de la **formation théorique**, vous avez été satisfait de *

	Pas d'accord	Neutre	Plutôt d'accord	Tout à fait d'accord
l'accessabilité de la formation	○	○	○	○
la pédagogie des formateurs	○	○	○	○
l'interactivité durant la session	○	○	○	○

Feedback grille d'évaluation data integrity

Le sondage prendra environ 12 minutes.

...

Bonjour Arnaud. Lorsque vous enverrez ce formulaire, son propriétaire pourra voir votre nom et votre adresse de courrier.

* Obligatoire

1. A combien estimez-vous votre niveau de connaissance concernant les exigences liées à l'intégrité des données **avant** la formation et le déploiement de la grille ? *

0	1	2	3	4	5	6	7	8	9	10

Aucune connaissance — Expert

2. Justification : *

Entrez votre réponse

3. A combien estimez-vous votre niveau de connaissance concernant les exigences liées à l'intégrité des données **après** la formation et le déploiement de la grille ? *

0	1	2	3	4	5	6	7	8	9	10

Aucune connaissance — Expert

4. Justification : *

Entrez votre réponse

5. Niveau d'appréciation concernant la formation théorique : *

0	1	2	3	4	5	6	7	8	9	10

A revoir — Très bien

6. Lors de la **formation théorique**, vous avez été satisfait de *

	Pas d'accord	Neutre	Plutôt d'accord	Tout à fait d'accord
l'accessabilité de la formation	○	○	○	○
la pédagogie des formateurs	○	○	○	○
l'interactivité durant la session	○	○	○	○

7. Lors de la **formation pratique**, vous avez été satisfait de *

	Pas d'accord	Neutre	Plutôt d'accord	Tout à fait d'accord
l'accessabilité de la formation	◯	◯	◯	◯
la pédagogie des formateurs	◯	◯	◯	◯
l'interactivité durant la session	◯	◯	◯	◯

8. Concernant le temps de formation *

0	1	2	3	4	5	6	7	8	9	10

Trop court — Trop long

9. Quels sont les éléments que vous avez le plus retenu durant la formation ? *

Entrez votre réponse

10. Avez-vous des points à améliorer pour les prochaines formations ? *

Entrez votre réponse

11. Votre niveau de connaissance de la stratégie de déploiement de la grille *

0	1	2	3	4	5	6	7	8	9	10

Pas du tout — Très bien

12. Justification : *

Entrez votre réponse

13. Concernant votre niveau de compréhension des items de la grille d'évaluation *

0	1	2	3	4	5	6	7	8	9	10

Aucun item — Tous les items

14. Justification : *

Entrez votre réponse

15. Quels sont les items qui ont posé le plus de difficultés ?

Entrez votre réponse

16. Avez-vous des propositions de correction ?

Entrez votre réponse

17. Quel temps en moyenne avez-vous passé par équipement pour déployer la grille ? *

- ◯ Moins de 1h00
- ◯ Entre 1h et 1h30
- ◯ Entre 1h30 et 2h
- ◯ Plus de 2h

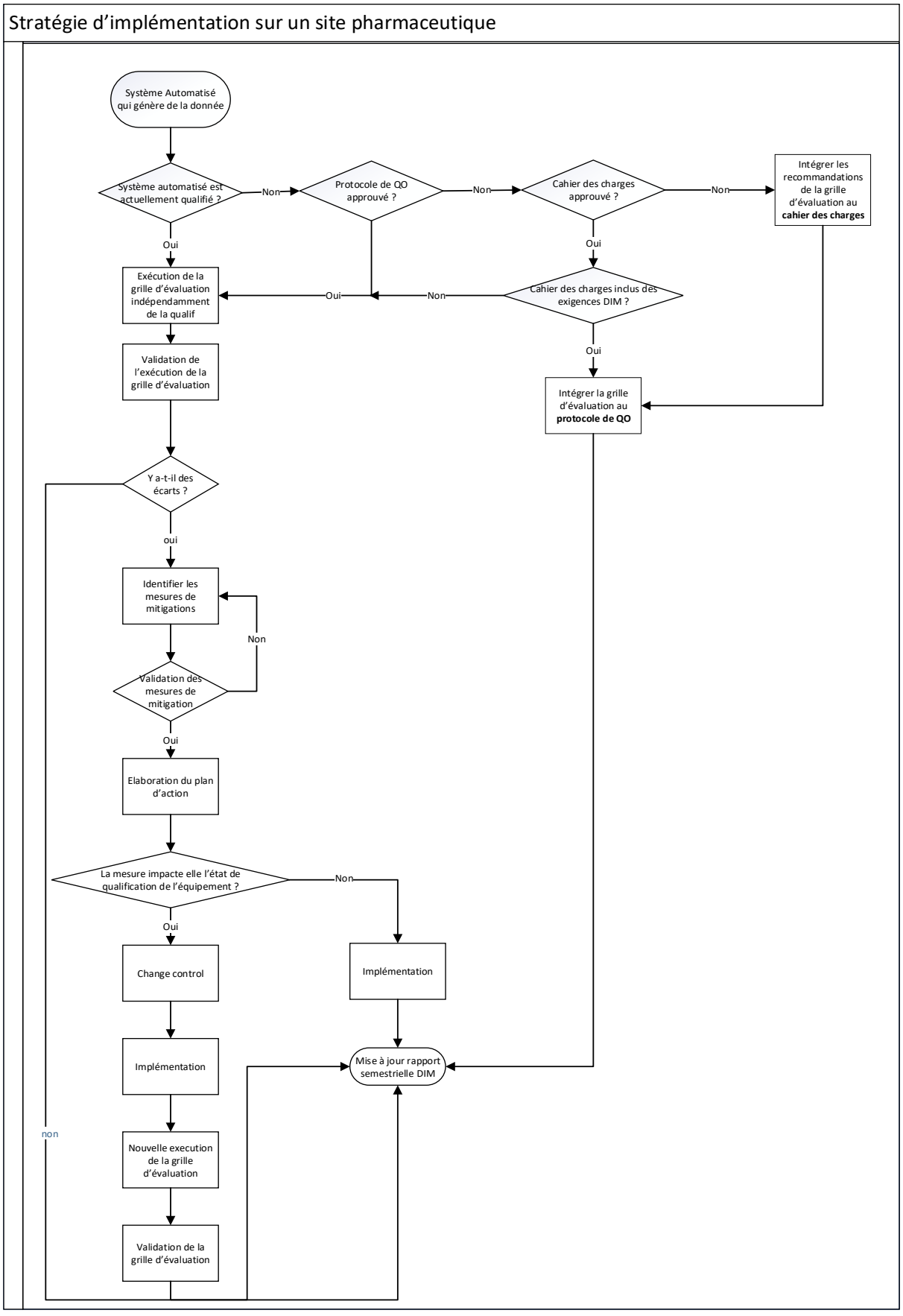
18. Quels ont été les facteurs qui ont pu ralentir la progression ? *

Entrez votre réponse

19. Avez-vous d'autres remarques ?

Entrez votre réponse

Annexe 2. Stratégie d'implémentation du protocole de test data integrity sur un site de production pharmaceutique



Serment De Galien

Je jure en présence de mes Maîtres de la Faculté 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, mes devoirs envers le malade et sa dignité humaine, de respecter le secret professionnel.

En aucun cas, je ne consentirai à utiliser mes connaissances et mon état pour corrompre les mœurs et favoriser les 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.

Attention, ne supprimez pas le saut de section suivant (page suivante non numérotée)

Maitrise de l'intégrité des données sur un site de production pharmaceutique et stratégie d'implémentation sur les systèmes informatisés

---

La maitrise de l'intégrité des données au sein d'un site de production pharmaceutique est un enjeu majeur car elle permet aux laboratoires et aux autorités réglementaires de prendre des décisions éclairées. L'augmentation des écarts ces 20 dernières années montrent que la maitrise des données est un axe important d'amélioration continue. Cette thèse s'applique à démontrer l'importance de maitriser l'intégrité des données sur un site de production pharmaceutiques par la mise en place d'une approche globale tout au long du cycle de vie de la donnée et centrée sur une approche par analyse de risque. Dans ce cadre, une stratégie de maitrise des systèmes informatiques est proposée.

Mots-clés : intégrité, donnée, site de production

Data integrity control on a pharmaceutical manufacturing site and implementation strategy on computerized systems

---

Data integrity control within a pharmaceutical manufacturing site is a major issue because it allows laboratories and regulatory authorities to provide good decision making. Increase of deviations over the last 20 years shows that data integrity is an important axis of improvement. This thesis aims to demonstrate importance of controlling data integrity on a pharmaceutical manufacturing site by implementing a global approach throughout data life cycle using a risk-based approach. In this context, a data integrity control strategy for computer systems is proposed.

Keywords : Integrity, data, manufacturing site