Gestion de l'intégrité des données : contraintes dans l'industrie pharmaceutique et application d'un outil de suivi dit " audit trail "

Adeline Lauriot

Service Commun de la Documentation
Chemin la censive du Tertre - BP 32211
44322 Nantes cedex 3

www.bu.univ-nantes.fr

NANTES UNIVERSITE

UFR SCIENCES PHARMACEUTIQUES ET BIOLOGIQUES

ANNEE 2023 N°

THESE

pour le

DIPLOME D'ETAT

DE DOCTEUR EN PHARMACIE

par

Adeline LAURIOT

Présentée et soutenue publiquement le 10 Novembre 2023

Gestion de l'intégrité des données : contraintes dans l'industrie pharmaceutique et application d'un outil de suivi dit « audit trail »

Président : Mr Jean-Michel Robert, PharmD, PhD, HDR, UFR Sciences Pharmaceutiques et Biologiques de Nantes

Directeur : Mr Samuel Bertrand, Maitre de conférence (Associate Professor),Ph.D. Chimie, M.Sc. Chimie (ENSCL), UFR Sciences Pharmaceutiques et Biologiques de Nantes

Membres du jury : Mr Antoine Pierson, Responsable Assurance Qualité en Data integrity, Servier, Gidy

Mr Julien Wang, Consultant Pharmacien Qualité, Caduceum, Rouen

Remerciements

La réalisation de cette thèse a été possible grâce au concours de plusieurs personnes à qui j'aimerai témoigner ma gratitude.

Je souhaite premièrement remercier mon directeur de thèse, Monsieur Samuel BERTRAND, Maitre de Conférences à l'Université de Nantes, qui m'a conseillé et guidé pendant ce projet. Son expérience et ses observations avisées m'ont été précieuses dans la réalisation du présent travail. Mes remerciements vont également à Monsieur Jean-Michel Robert, Professeur à l'Université de Nantes pour la présidence du jury.

Je remercie Antoine PIERSON, responsable assurance qualité système informatique aux Laboratoires Servier Industrie, pour m'avoir proposé ce sujet. Je tiens également à le remercier pour m'avoir accompagné, pour m'avoir donné tous ces précieux conseils et pour la bienveillance dont il a fait preuve à mon égard.

Mes remerciements vont également à Anne Sophie GAUJARD et Tony TROTTE et à toute la DIM team, pour leur bonne humeur, la confiance et l'écoute qu'ils m'ont accordé au quotidien.

Je souhaite aussi remercier l'ensemble du corps professoral de l'Université de Nantes ainsi que du Master 2 Responsabilité et Management de la Qualité dans les Industries de Santé de Bordeaux pour leurs encadrements et leurs enseignements pendant ces années d'études.

Un merci tout particulier à Anouk, Clémence, Clément, Florian, Julien, Kilian, Marine, pour avoir rendu ces années d'études inoubliables et pour m'avoir soutenu quoiqu'il arrive. Je n'oublie pas non plus Anaïs, Julie, Lucie, Romain, Mathieu, Théo et Michael pour tous ces merveilleux moments passés à Bordeaux.

Je tiens à exprimer ma reconnaissance à ma famille qui m'a donné les moyens de réaliser mon parcours.

Enfin, je remercie Romain pour son soutien indéfectible.

Abréviations

Abréviation	Signification
ALCOA+	Attributable, Legible, Contemporaneous, Original, Accurate, Complete, Consistent, Enduring, Available
ANSM	Agence Nationale de la Sécurité du Médicaments et des produits de santé
BPF	Bonnes Pratiques de Fabrication
BPPV	Bonnes Pratiques de Pharmacovigilance
CDS	Chromatography Data System
CFR	Code of Federal Regulation
CGMP	Current Good Manufacturing Practices
DM	Dispositif(s) medical(ux)
DIV	Dispositif In Vitro
DMIL	Dispositifs Médicaux Intégrant du Logiciel
DMS	Document Management System
EMA	European Medical Agency, Agence Européenne du médicament
ERP	Enterprise Resource Planning
FDA	Food and Drug Administration
FIPEC	Fournisseurs, Intrants, Processus, Extrants, Clients
GAMP	Good Automated Manufacturing Practice
IACS	Industrial Automation Control System Système d'Automatisation et de Commande Industrielles
ICH	International Council for Harmonisation of Technical

ISO	Organisation Internationale de Normalisation
ISPE	International Society for Pharmaceutical Engineering
LIMS	Laboratory Management System
MDCG	Medical Device Coordination Group
MES	Manufacturing Execution System
MHRA	Medicines and Health products Regulatory Agency
NQA	Niveau de Qualité Acceptable
PDCA	Plan, Do, Check, Act
PIC/S	Pharmaceutical Inspection Convention et Pharmaceutical Inspection Co-operation Scheme
SBU	Spécifications des Besoins Utilisateurs

Introduction

L'industrie pharmaceutique a pour but de fournir des médicaments pour répondre aux besoins sanitaires des patients et de l'Etat. En effet, les médicaments doivent être d'une qualité suffisante pour ne pas mettre en péril la sécurité des patients.

Pour cela, l'industrie pharmaceutique transforme des matières premières en produits finis, les médicaments. Avant de mettre les médicaments sur le marché, ils doivent passer par la libération du lot. Cette étape est réalisée par des pharmaciens sur la base d'un dossier de lot composé de données issues de la production ainsi que des résultats issus du contrôle de la qualité du médicament.

Pour pouvoir réaliser la libération des produits, il est nécessaire d'avoir des données fiables. La gestion de l'intégrité des données a pour but d'assurer que les données sont exploitables et qu'il est possible de prendre des décisions basées sur ces informations. L'assurance qualité est le service qui développe et aide l'ensemble des services à mettre en place des processus pour fournir à une société l'aptitude de satisfaire un niveau de qualité désiré. Différents systèmes sont gérés par l'assurance qualité dont les systèmes informatiques et la gestion de l'intégrité des données.

Une des contraintes de l'industrie pharmaceutique est de pouvoir donner confiance en ses produits, la maîtrise de l'intégrité de ses données est un des fondements pour fournir cette confiance aux patients et aux autorités. Pour la traçabilité, les industries sont, encore aujourd'hui, dans un modèle hybride entre le papier et l'électronique. C'est ce cas qui est le plus contraignant pour la gestion des données car cela signifie que le personnel doit être formé aux spécificités propres à chaque cas et qu'il doit s'adapter au fonctionnement de chaque système.

La première partie de ce document porte sur la définition de l'ensemble des éléments nécessaire pour la gestion de l'intégrité des données. De plus, dans cette partie, sera détaillé l'évolution de l'intérêt portée à la gestion de l'intégrité des données et aux outils de suivi en règle générale et par les organismes d'état. La deuxième partie est un état des lieux de l'état de l'art autour de ces sujets en se basant sur les réglementations, les référentiels et différentes études réalisées à ce propos. La troisième partie est une présentation d'un cas concret de mise en place et d'exploitation d'un outil de suivi utilisé dans un laboratoire de contrôle de la qualité. En ouverture, la place de l'apprentissage automatique et de la chaine de blocs au service de l'outil de suivi et de l'industrie pharmaceutique sera abordée.

Partie 1 : Gestion de l'intégrité des données

I. Contexte

Historique de l'évolution des industries

L'industrie 4.0 est au centre de l'actualité et des évolutions. Elle correspond à une industrie où la production est entièrement automatisée et où les décisions sont prises par des Intelligences Artificielles. Avant d'en arriver là, l'industrie a évolué selon différents stades [1].

L'industrie 1.0 correspond à la première moitié du 19ème siècle. Cette révolution voit la formation de la production industrielle avec les premiers équipements. Ainsi le travail manuel a été remplacé par la technologie industrielle.

Dans la deuxième moitié du 19ème siècle et au début du 20ème siècle, l'industrie devient 2.0. Elle est définie par une rationalisation de la chaîne de production et une accumulation des innovations technologiques afin de produire plus rapidement et à moindre coût.

La troisième révolution industrielle s'inscrit dans la seconde moitié du 20ème siècle, elle est marquée par l'apparition des technologies numériques et l'organisation de l'industrie dans une infrastructure mondiale. La production se base sur des technologies utilisant le numérique.

Actuellement, avec l'apparition d'internet, de la robotique et de l'intelligence artificielle, nous entrons dans la quatrième révolution industrielle. Une industrie 4.0 a une production entièrement automatisée où l'homme n'intervient pas physiquement. L'utilisation de l'intelligence artificielle au cœur du système de production permet l'optimisation des processus et permet un échange d'information et des prises de décisions en temps réel.

Les systèmes de traçabilité ont évolué simultanément à ces différentes révolutions. L'industrie 2.0 correspond à l'ère du tout papier, le 3.0 incarne l'ère du tout numérique et l'industrie 4.0 correspond à l'ère de l'intelligence artificielle.

La traçabilité

A l'heure actuelle, la plupart des industries pharmaceutiques oscillent entre l'industrie 2.0 et l'industrie 4.0. Chaque industrie a ses propres particularités en termes de traçabilité. Si elle est en transition du papier vers le numérique, l'industrie s'appuie sur la formation de son personnel qui doit s'adapter au fonctionnement de chaque processus pour déterminer la traçabilité nécessaire et adaptée. Selon le Larousse, la traçabilité c'est la possibilité de suivre un produit aux différents stades de sa production, de sa transformation et de sa commercialisation. La traçabilité est constituée de l'ensemble des données nécessaires pour recréer la vie d'un produit [2]. Comme nous nous appuyons sur ces données pour avoir une traçabilité fiable, il faut s'assurer qu'elles sont intègres, c'est-à-dire qu'elles sont conservées sans altération, dans son état originel. Pour cela, un ensemble d'actions sont effectuées dans le cadre de la gestion de l'intégrité des données.

L'Agence Nationale de Sécurité du Médicament et des produits de santé (ANSM), demande, au nom de l'Etat français, aux industriels de suivre l'ensemble des règles écrites dans les Bonnes Pratiques de Fabrication (BPF). Le chapitre 4 « Documentation » porte sur la gestion des documents. Pour la gestion de l'intégrité des données numériques, le chapitre 4 est complété par l'annexe 11 « Système Informatisé » [3]. Pour les BPF, les industriels doivent assurer une bonne traçabilité des modifications apportées et assurer que les données présentes et exploitées n'ont pas été corrompues au cours de leur cycle de vie. Par exemple, si une modification est apportée sur un document papier, l'auteur et la date doivent être inscrits sur ce document. La modification doit être effectuée de façon que la donnée précédente soit toujours lisible (en la rayant proprement). Si une modification est réalisée sur un document numérique, le système doit, a minima, enregistrer la modification, la donnée d'origine, ainsi que l'auteur et la date de la modification. Ces mesures sont nécessaires pour garantir que les principes de sécurité pour l'intégrité des données sont appliqués avec la même rigueur pour le format papier que pour le format électronique. En effet, dans l'annexe 11 « Système informatisé », il est noté [3] :

> « *Lorsqu'un système informatisé remplace une opération manuelle, il ne doit pas en résulter une baisse de la qualité du produit, de la maîtrise du processus ou de l'assurance de la qualité. Il ne doit pas non plus en découler une augmentation du risque général lié au processus.* »

La réglementation et les référentiels

En France, la sécurité des médicaments et des produits de santé est assurée par l'ANSM. C'est un acteur public qui agit au nom de l'Etat. L'EMA, l'Agence Européenne des Médicaments, est l'équivalent de l'ANSM au niveau européen. Le texte qui régit la production de médicament est les BPF. La gestion de l'intégrité des données numériques, est principalement décrite dans l'Annexe 11 des BPF : « Systèmes Informatisés » [3].

Pour les dispositifs médicaux (DM), en France, la réglementation en vigueur est le règlement (UE) 2017/745. Pour la gestion de l'intégrité des données, la nouvelle réglementation demande que l'état de l'art soit appliqué [4]. Les cosmétiques sont régis par le règlement (CE) n°1223/2009. Le paragraphe 16 de ce règlement demande que les BPF soit appliqué [5]. L'état de l'art pour la gestion de l'intégrité des données pour les médicaments correspond à l'état de l'art appliqué pour les DM et les cosmétiques.

Le Medicines and Health products Regulatory Agency (MHRA) est l'équivalent anglais de l'ANSM. Le MHRA a publié le document « Data Integrity Definitions and Guidance » pour légiférer sur la gestion de l'intégrité des données dans le domaine pharmaceutique en 2015 [6].

Aux Etats-Unis, la Food and Drug Administration (FDA) est l'organisation assurant la sécurité et l'efficacité des médicaments. Les règles pour l'alimentation et les médicaments sont présentes dans le titre 21 du Code of Federal Regulation (CFR). Les parties 210 et 211 regroupent les Current Good Manufacturing Practices (cGMP) c'est-à-dire l'équivalent des BPF [7], [8]. La partie 11 « Electronic Records ; Electronic signature » permet de réglementer les attendus en termes de gestion de l'intégrité des données et de gestion documentaire [9].

Le Pharmaceutical Inspection Convention et Pharmaceutical Inspection Co-operation Scheme (PIC/S) est un comité regroupant les autorités réglementaires de 54 pays dans le domaine des BPF. Le but du PIC/S est de mettre en œuvre et de maintenir des BPF harmonisés entre les pays. Il publie des guides, réalise des formations et différents événements dans cette optique. Le PIC/S a notamment publié des guides comme « Good Practices for Computerised Systems in regulated GXP environments », en 2007 [10], et « Good Practices for Data Management and integrity in regulated GMP/GDP environments » en 2021 [11].

L'International Society for Pharmaceutical Engineering (ISPE) est une association à but non lucratif menant des activités autour des avancées scientifiques, techniques et réglementaires du domaine pharmaceutique. Ils ont publié différents guides dont les Good Automated Manufacturing Practice (GAMP).

Les GAMP sont des guides aidant à l'interprétation des normes réglementaires. Dans le cadre des systèmes informatiques, il existe le GAMP 5 : « Une approche de la conformité des systèmes informatisés BPx basée sur les risques » [12]. Pour la gestion de l'intégrité des données, il existe deux autres guide GAMP : « Records & Data Integrity » [13] et « Data Integrity by design » [14].

Les systèmes

Les systèmes correspondent à tous les outils pouvant générer des données. Cela correspond au système informatique qui servent au traitement et à l'utilisation des données ainsi qu'au système automatisé qui, par exemple, permettent de piloter des équipements de production. Le PIC/S définit les systèmes comme indiqué dans la figure 1 [10].

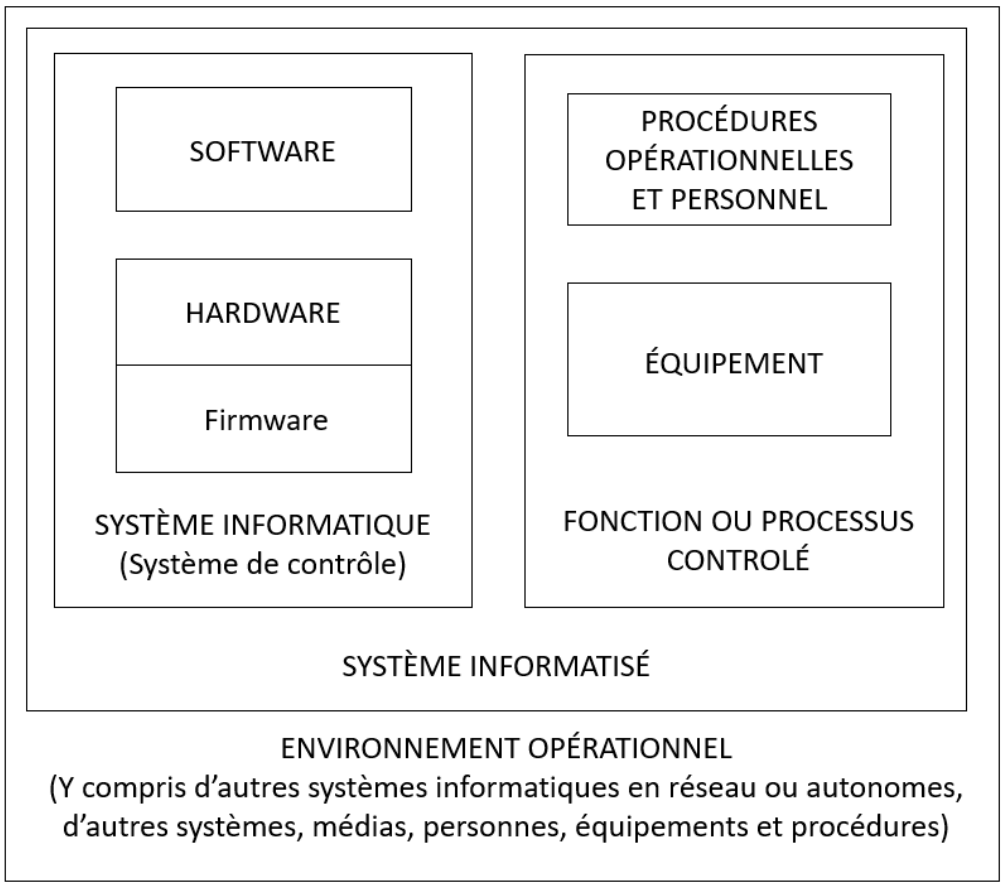


Figure 1 Schéma des relations entre les composants d'un système informatisé et son environnement opérationnel, traduit du guide « Good Practices for Computerised System in regulated GXP environnement » du PIC/S (Pharmaceutical Inspection Convention et Pharmaceutical Inspection Co-operation Scheme) [10]

Les systèmes informatisés sont présents au sein de l'environnement opérationnel au même titre que la main d'œuvre, les procédures ou les équipements. Parmi les systèmes informatisés, il existe deux types de systèmes :

- Les systèmes informatiques qui sont des systèmes de contrôle,
- Les systèmes qui permettent d'avoir des fonctions ou des processus contrôlés, comme les équipements, les procédures ou la main d'œuvre.

Les systèmes informatisés sont composés des logiciels (software), du matériel (hardware) et des systèmes embarqués (firmware) [15]. Ce dernier est un système présent dans un équipement matériel. Il dote cet équipement d'autonomie, c'est-à-dire d'une capacité de perception, de traitement, d'action et de communication en interaction avec son environnement physique. Par exemple, un système embarqué permet de commander les fonctionnalités d'un clavier d'ordinateur. Pour plus de simplicité, les systèmes informatiques sont appelés « logiciels », et les équipements comprenant un système embarqué sont appelés des systèmes automatisés ou automatiques. L'ensemble des systèmes informatique et automatique correspond aux systèmes informatisés.

Il existe plusieurs types de systèmes informatiques interfacés entre eux (Figure 2) [16] :

- Entreprise Resource Planning (ERP),
- Manufacturing Execution System (MES),
- Laboratory Management System (LIMS)
- Document Management System (DMS)
- Systèmes de gestion des ressources matérielles (Logistique) et humaines.

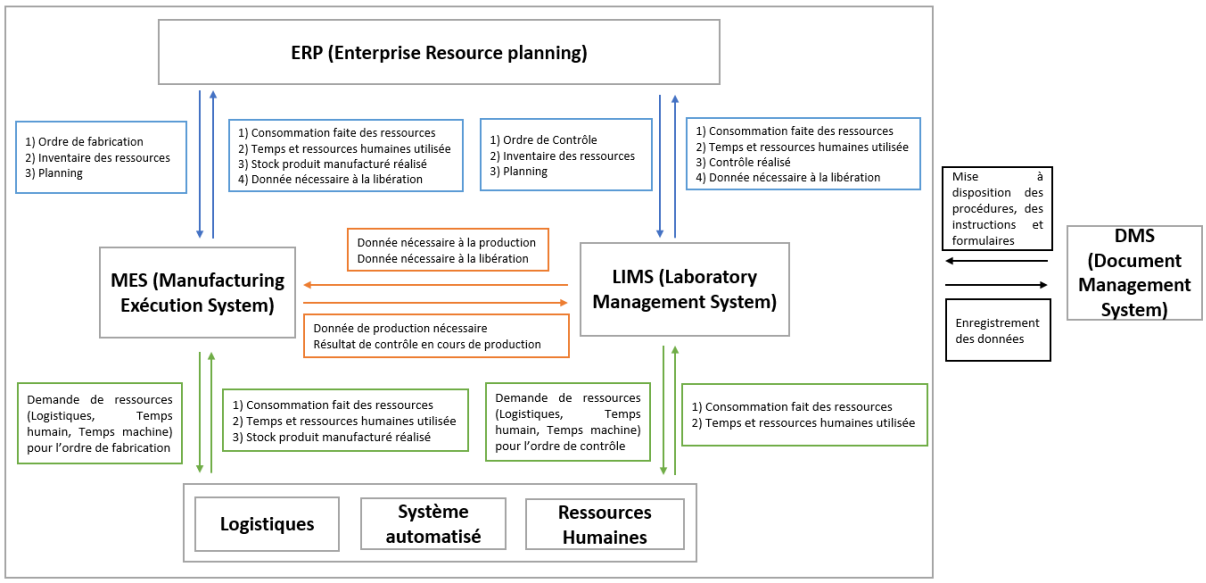


Figure 2 Représentation des interfaces entre les systèmes

L'objectif principal de l'ERP est de planifier les processus de production en fonction des ressources matérielles et des besoins. Il est en interface avec le MES pour émettre les ordres de fabrication et/ou de contrôle. Cette interface permet à l'ERP de connaître les ressources

disponibles. Le MES permet, quant à lui, la gestion des activités de l'atelier en collectant et en analysant, en temps réel, les données qui en sont issues. Par ailleurs, il fait de même avec les données issues des systèmes avec lesquels il est en interface. Ces derniers correspondent aux LIMS, aux systèmes de gestion des ressources matérielles et humaines. Le LIMS est chargé de la gestion des contrôles qualité et de la récupération des résultats des contrôles qualité. Le DMS est un système qui regroupe toute la documentation comme les procédures, les instructions et les formulaires. Le DMS peut aussi inclure l'enregistrement de données.

Pour une analyse faite en laboratoire de contrôle qualité, tous ces systèmes sont nécessaires et sont interfacés. L'ERP émet l'ordre de fabrication d'un contrôle vers le MES. Le MES transfère la demande de ressources matérielle et humaine auprès des systèmes concernés. L'analyse de contrôle qualité est réalisée par les systèmes automatisés et les résultats sont enregistrés dans le LIMS. Le LIMS transfère les résultats vers le MES. Ce dernier transfère ensuite les informations vers l'ERP. L'ERP regroupe les informations concernant un lot pour former le dossier de lot nécessaire à la libération.

La donnée et son cycle de vie

Une donnée est un fait, un chiffre présent dans les enregistrements originaux. Cela comprend les données sources, les métadonnées et toutes les transformations et rapports générés ultérieurement. Chaque donnée possède un cycle de vie (Figure 3) qui est composé de différentes phases. Ce cycle commence par la génération initiale et l'enregistrement, puis il y a les étapes de traitement, d'utilisation, de conservation et d'archivage. Le cycle peut être complété par des étapes de récupération et de destruction de la donnée [6].

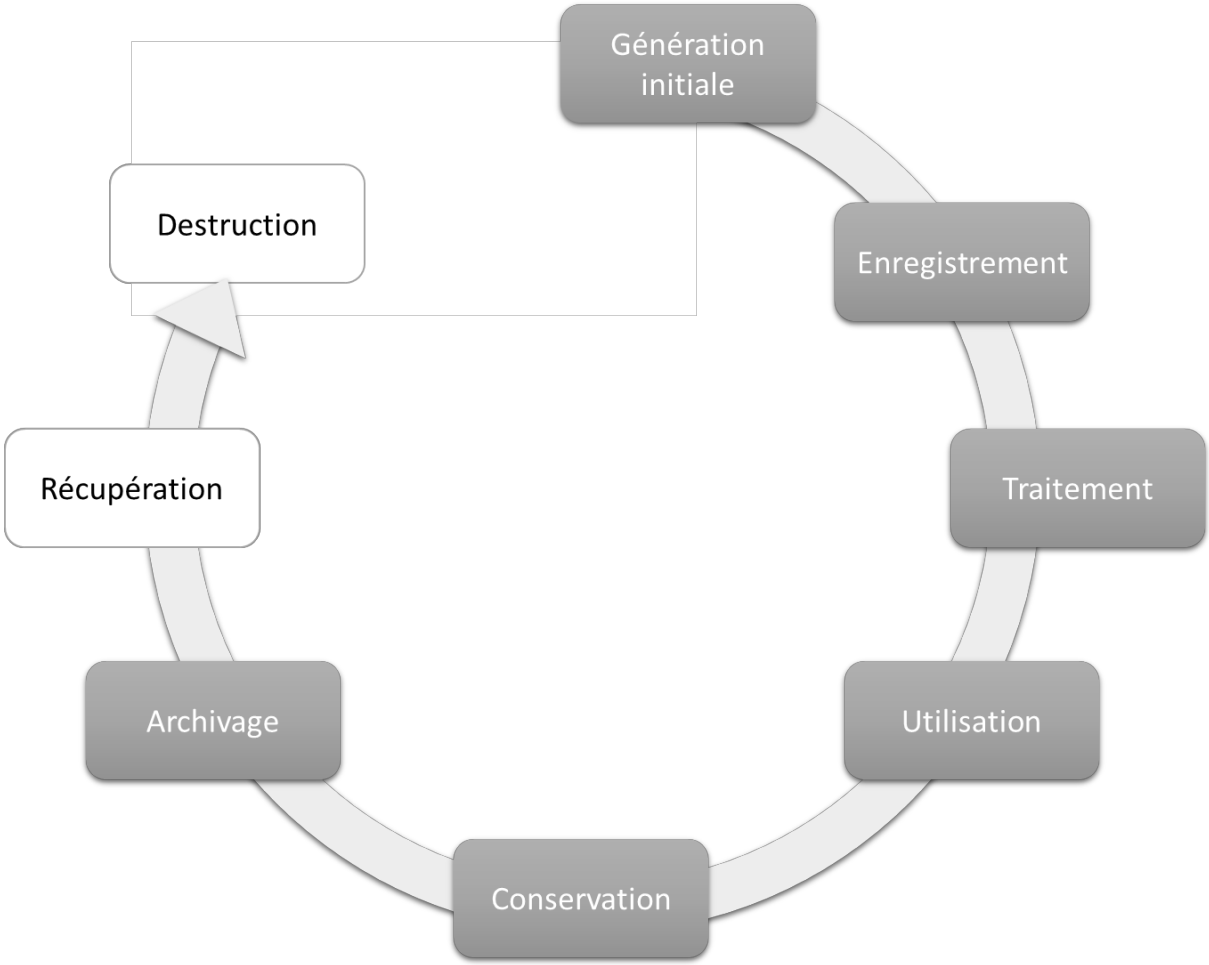


Figure 3 Cycle de vie d'une donnée

Dans les BPF, "*l'ensemble des informations ayant trait à des décisions qualité doivent être considérées comme des données brutes*" [3]. Une donnée brute est définie comme l'enregistrement original. Ce qui peut être décrit comme la première capture de l'information, sur papier ou électroniquement. Dans le cycle de vie de la donnée, les étapes "Génération initiale" et "Enregistrement" doivent donc s'effectuer concomitamment. L'enregistrement correspond à une première phase de stockage de la donnée brute.

Le traitement des données correspond au fait d'appliquer une formule à une donnée chiffrée par exemple. Ce traitement des données est réalisé selon des processus définis pour avoir des résultats répétables. Cette étape est aussi l'occasion de vérifier, de valider les données comme les métadonnées, et si nécessaire, de les compléter.

L'utilisation des données est réalisée lorsqu'une décision est prise grâce à cette donnée. Par exemple, les contrôles en cours de production sont réalisés au cours des étapes de production pour déterminer si le lot peut passer à l'étape suivante ou non. Lors d'une granulation, le contrôle de l'humidité est effectué pour déterminer la fin de la phase de mouillage. Ainsi, les données issues de ce contrôle en cours de production permettent une prise de décision.

La conservation des données et l'archivage des données sont des phases gérées par des procédures propres dans chaque industrie pharmaceutique. Pour les BPF, les documents et donc les données associées doivent être conservés pendant 10 ans après la commercialisation du lot. Il appartient aux industries de s'assurer que les données brutes soient toujours disponibles et lisibles au cours de la durée de conservation légale. Une fois archivées, les données peuvent être récupérées et pour cela, les industries pharmaceutiques doivent s'assurer régulièrement que la récupération soit possible. Selon des procédures et des critères bien définis, il peut être possible de détruire des données brutes, comme à la fin de la période de conservation légale ou si une copie certifiée conforme à l'originale a été effectuée.

Les métadonnées

Les données brutes numériques sont toujours associées à des métadonnées. Les métadonnées sont définies comme des données qui décrivent les attributs d'autres données, et fournissent un contexte, une signification aux données brutes. Les métadonnées sont donc toutes les informations qui gravitent autour de notre donnée.

La norme de l'organisation internationale de normalisation (ISO) 15836 :2009 « Information et documentation – L'ensemble des éléments de métadonnées Dublin Core » se base sur une ressource appelé « Dublin Core Metadata Element Set » dont la version 1.1 a été publiée en 2012 [17]. Les définitions de l'ensemble des 15 métadonnées existantes sont présentes dans cette ressource (Tableau 1).

Tableau 1 Tableau des 15 métadonnées existantes issu et traduite du « Dublin Core Metadata Element Set » [17]

	Nom	**Définition**
1	Contributeur	Une entité chargée d'apporter des contributions à la ressource
2	Créateur	Une entité principalement responsable de la fabrication de la ressource.
3	Date	Un point ou une période associée à un événement dans le cycle de vie de la ressource.
4	Description	Un compte rendu de la ressource.
5	Droits	Informations sur les droits détenus dans et sur la ressource.
6	Editeur	Une entité responsable de la mise à disposition de la ressource.
7	Format	Le format du fichier, le support physique ou les dimensions de la ressource.
8	Identifiant	Une référence non ambiguë à la ressource dans un contexte donné.
9	Langage	La langue de la ressource.
10	Localisation spatio-temporelle	Le sujet spatial ou temporel de la ressource, l'applicabilité spatiale de la ressource, ou la juridiction sous laquelle la ressource est pertinente.
11	Relation	Une ressource connexe.
12	Source	Une ressource connexe à partir de laquelle la ressource décrite est dérivée.
13	Sujet	Le sujet de la ressource.
14	Titre	Un nom donné à la ressource.
15	Type	La nature ou le genre de la ressource.

De plus, les données sont différenciées en données statiques et dynamiques. Une donnée statique correspond à une donnée, brute ou traitée, qui est enregistrée dans un format « fixe » comme le papier ou comme une image électronique tel que le format PDF protégé [6]. Par exemple, les données présentes sur un ticket de pesée ne nécessitent généralement pas de traitement par un utilisateur pour être exploitable. Il contient a priori l'ensemble des informations nécessaires à l'interprétation et l'utilisation des données.

Une donnée dynamique est enregistrée dans un format qui permet une interaction entre l'utilisateur et le contenu de l'enregistrement. Le format permet une interaction, un traitement par un utilisateur. Par exemple, un enregistrement chromatographique dynamique peut permettre à l'utilisateur de modifier la ligne de base et retraiter les données chromatographiques de sorte que le pic résultant puisse apparaître plus ou moins large. Les données brutes, avant traitement, sont inchangées et l'accès à ces données doit être maintenu. A propos des données dynamiques, le PIC/S ajoute que les informations qui sont initialement enregistrées dans un état dynamique doivent rester disponibles dans cet état [10].

II. Les critères d'intégrité des données

L'intégrité des données

La FDA a décrit 9 critères nécessaires pour qu'une donnée soit considérée intègre, ils ont été regroupés sous l'acronyme anglais ALCOA+ (Figure 4) qui signifie : « Attribuable, Lisible, Contemporain, Original, Précis (Accurate), « + » pour Complet, Cohérent, Disponible et Durable ». Chacun de ces mots correspond à une des facettes de l'intégrité de la donnée [18].

Figure 4 Explication de l'acronyme ALCOA+

« Attribuable » signifie qu'une donnée doit être associée à une personne, celle qui a généré une donnée. Elle peut aussi être associée à un équipement.

« Lisible » signifie que la donnée doit être compréhensible de tous et qu'elle ne doit pas laisser de place à l'interprétation. Une donnée manuscrite doit donc être déchiffrable par n'importe qui. Une donnée numérique doit avoir du contexte, ses métadonnées sont essentielles.

« Contemporain » signifie que la donnée doit être associée à un horodatage et que celui-ci correspond au moment de la création de la donnée. Pour une donnée manuscrite, chaque enregistrement est relié à l'heure qui doit être inscrite à la main.

« Original » signifie que la donnée brute correspond à la première donnée générée. Pour pouvoir exploiter une donnée brute, il faut qu'elle soit présente sur le premier enregistrement réalisé à la suite de sa génération ou sur une copie certifiée conforme à l'originale.

« Précis (Accurate) » signifie que la donnée est exacte, elle correspond à la réalité. Pour cela, l'équipement doit être qualifié, la donnée doit être associée à une unité. La donnée doit aussi être associée à ses métadonnées pour pouvoir lui donner du contexte et ainsi être la plus exacte possible.

« Complet » signifie que la donnée se doit d'avoir toutes les informations nécessaires pour être précise, et assurer qu'il n'y a aucune omission qui pourrait s'apparenter à de la falsification.

« Cohérent » signifie que la donnée doit être logique avec son environnement et avec les autres données présentes. Ce mot peut être associé à « Contemporain » car si chaque donnée est associée à un horodatage, tous les horodatages doivent suivre un ordre logique selon le moment de génération des données. Si une incohérence apparaît, une donnée n'est pas intègre, une investigation sera à mener.

« Disponible » signifie que la donnée doit être accessible pendant toute sa durée de vie, du moment de sa génération jusqu'à son archivage. Les conditions d'archivage doivent être maîtrisées, au niveau informatique comme au niveau papier.

« Durable » signifie que le format d'enregistrement de la donnée brute doit toujours pouvoir être lisible, et doit toujours pouvoir être accessible pendant toute sa durée de rétention. Si une donnée est enregistrée sur une disquette, l'entreprise se doit d'avoir un lecteur de disquette ou de copier ces données vers un support plus durable. Cette copie doit être certifiée conforme à l'originale pour pouvoir être considérée comme une donnée brute et le support original pourra être détruit si besoin.

Toutes les données doivent rassembler ces critères. Pour maintenir cette intégrité, différents outils sont à notre disposition. Nous avons l'horodatage qui peut être relié à un réseau commun. En reliant chaque équipement à ce même réseau et en le protégeant des changements, les données seront cohérentes et sécurisées de ce point de vue. Pour avoir une donnée précise, il est possible d'automatiser la demande d'information. Ainsi une information manquante rendra impossible l'exécution de la tâche suivante.

La qualité des données

Selon le guide GAMP « Records and Data integrity » [13] :

> *« La qualité des données concerne l'aptitude des données à servir l'objectif prévu dans un contexte donné au sein d'un processus commercial ou réglementaire spécifique. Les activités de gestion de la qualité des données portent sur des aspects tels que l'exactitude, l'exhaustivité, la pertinence, la cohérence, la fiabilité et l'accessibilité. »*

La gestion de la qualité des données englobe l'ensemble des critères pour la gestion de l'intégrité des données et prend en compte l'utilisation efficace de ces données. Pour cela, les données doivent :

- Être exactes : les données n'ont pas d'erreurs identifiables,
- Être accessibles : il faut définir la facilité nécessaire pour accéder aux données. Elles doivent être dans un environnement protégé et contrôlé,
- Être exhaustives : l'ensemble des données et des métadonnées requises sont réunies. Il est nécessaire de justifier chaque absence des métadonnées requises. Il est possible que des métadonnées soient disponibles mais non requises. Leur non-nécessité doit être justifiée, via une analyse de risque par exemple,
- Être cohérentes : les données sont fiables, identiques et reproductibles,
- Être actualisées : les données sont à jour ; elles sont à jour si elles sont le reflet de la réalité du présent. Elles ne sont plus à jour si elles sont le reflet d'un moment passé,
- Avoir une nomenclature : avoir une identification cohérente et précise des données et des métadonnées,
- Avoir un niveau de détail et de précision défini : définir les caractéristiques nécessaires pour la qualité des données pour répondre aux objectifs.

Les données doivent rassembler ces critères pour s'assurer de la qualité de leur génération, de leur traitement et de leur utilisation. Pour cela, l'objectif de l'utilisation de chaque donnée doit être défini en amont pour pouvoir établir la stratégie à adopter.

III. Evolution de l'intérêt pour l'intégrité des données

La gestion de l'intégrité des données est une problématique de plus en plus importante au sein des industries pharmaceutiques. En effet, cela se traduit au travers de différents éléments :

- Les textes réglementaires à ce sujet sont de plus en plus étoffés,
- Les recherches effectuées sur Google à ce sujet sont de plus en plus importantes,
- Le nombre de lettres d'injonction de non-conformités concernant l'intégrité des données émises par la FDA et celles émises par l'ANSM augmentent.

Evolutions réglementaires

Dans les BPF publié en 2007, la partie Système informatisé était comprise dans le Chapitre 3 « Gestion de la qualité et Documentation », l'intégrité des données y était mentionnée dans le paragraphe 3.2.5. Les éléments de pérennité, durabilité, intégrité, lisibilité, procédure de condition d'archivage sont eux aussi mentionnés. Les principes de l'ALCOA+ étaient présent avec une prise en compte du cycle de vie de la donnée [19].

Dans la version des BPF publiée en 2011, la partie Système informatisé a été séparé du Chapitre sur la documentation. La ligne directrice 11 lui est dédiée. Elle fait deux pages, dont une majeure partie sur la validation des systèmes. Le principe de l'intégrité des données n'est pas associé directement au système informatisé dans cette nouvelle version. Le principe de protection de l'intégrité des données n'est pas explicitement mentionné comme dans la version précédente [20].

Dans la version des BPF publiée en 2015, les informations à propos des systèmes informatiques et de la gestion de l'intégrité des données présentes dans le chapitre 3 Documentation est identique à la version précédente. A l'exception de la réapparition de la mention de la revue régulière nécessaire de « la précision, l'intégrité, la disponibilité et la lisibilité de documents ». La ligne directrice 11 « Système informatisé » a été étoffé. Par exemple, une vérification de l'intégrité des données archivés et une vérification régulière sur les enregistrements ont été ajoutées [21].

Depuis cette version des BPF de 2015, le texte sur les systèmes informatisé n'a pas évolué à propos de la gestion de l'intégrité des données. C'est au cours de cette même année, que le MHRA publie le guide « Data Integrity and Guidance ». L'ensemble des définitions nécessaires à la maîtrise de l'intégrité des données y sont présentes [6].

Pour compléter ses attentes rédigées dans le Code fédéral, la FDA a publié en 2018 « Data Integrity and Compliance With Drug CGMP, Questions and Answer, Guidance for Industry ». Ce document répond à 18 questions concernant la maîtrise de l'intégrité des données et regroupe les lignes directrices que les industriels doivent suivre [18]. L'ensemble de ces éléments est détaillé au sein de cette thèse, dans la Partie 2 : La gestion de l'intégrité des données et les outils de suivi des activités : la réglementation, leurs spécificités et leurs contraintes.

Evolution des préoccupations

L'outil « Trends » des services de l'entreprise Google, nous permet de connaître la proportion de recherches sur des mots clés. Le taux d'utilisation le plus élevé de ce mot clé a une valeur de 100. Une valeur de 50 signifie que le mot clé a été utilisé moitié moins souvent que le taux d'utilisation le plus élevé, et une valeur de 0 signifie que les données pour ce mot clé sont insuffisantes [22].

Le graphique ci-dessous (Figure 5) représente les moyennes sur chacun des taux d'utilisation mensuelle des mots clés « Data Integrity » soit intégrité des données en français. Le graphique recouvre la période de janvier 2012 à août 2022 et correspond aux utilisations faites à l'international. Le taux d'utilisation de ces termes est le plus élevé en mars 2022 et il augmente de 43 points en 10 ans.

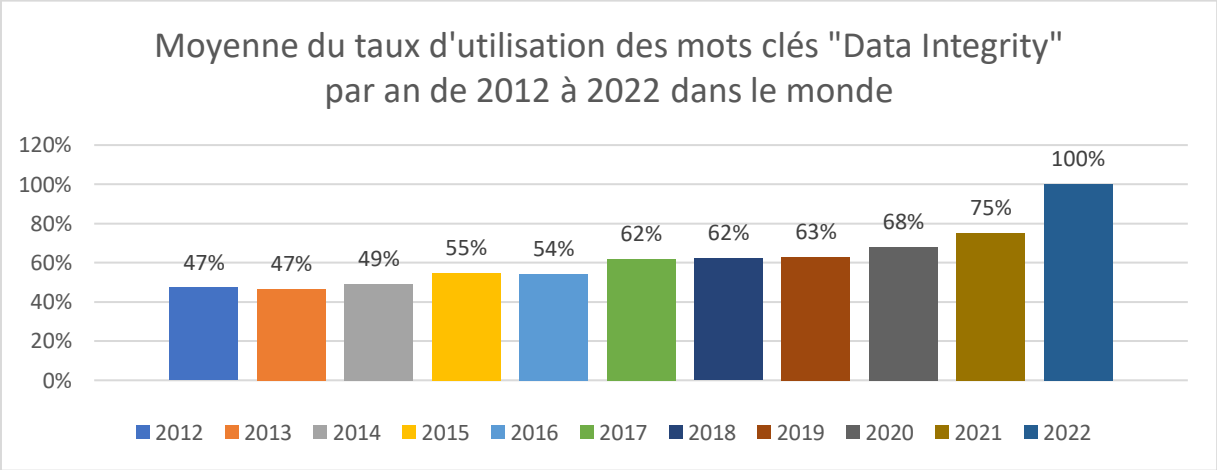


Figure 5 Représentation des moyennes du taux d'utilisation des mots clés "Data integrity" par an, de 2012 à 2022, dans le monde sur Google

L'intérêt pour la gestion de l'intégrité des données est devenu de plus en plus important au fil des années et plus particulièrement en 2022.

Les injonctions et lettres d'avertissements

Lorsque la FDA constate qu'un fabricant a enfreint, de manière significative, la réglementation, elle en informe le fabricant généralement sous le format des « Warning letters » [23]. Ce sont des lettres d'avertissements publiques. Contrairement à la FDA, l'ANSM ne publie pas tous les écarts détectés en inspection. Sur le site de l'ANSM, seules les injonctions sont publiées. L'ANSM peut prononcer une injonction si un de ces inspecteur constate un non-respect des lois et règlement lors d'une inspection. Ici, les injonctions comptabilisées sont celles publiées de janvier 2018 à août 2022. Comme le règlement 2017/745 relatif aux DM a été publié le 5 avril 2017 pour une mise en application le 26 mai 2021, uniquement les injonctions concernant les médicaments ont été prises en compte.

A propos du Data integrity, l'ANSM a publié 11 injonctions depuis 2018 portant notamment sur la maîtrise de l'intégrité des données au travers d'une validation des systèmes informatisés [24]. Les lettres d'avertissements de la FDA portent sur les mêmes sujets abordés par l'ANSM, cependant leur nombre est plus important du fait de leur fonctionnement. En effet, depuis 2018 jusqu'au mois d'août 2022, la FDA a publié 134 lettres d'avertissement concernant la maîtrise de l'intégrité des données.

Les injonctions de l'ANSM et les lettres d'avertissement de la FDA correspondent souvent à des insuffisances, des manquements voire des absences de « maîtrise de l'intégrité des données ». La plupart du temps, il est demandé de mettre en place un système informatisé validé et/ou des processus permettant de maîtriser l'intégrité des données.

La gestion de l'intégrité des données est une préoccupation de l'ANSM et de la FDA, elles attendent des industries que le cycle de vie des données, au complet, soit maîtrisé. Pour cela, les systèmes informatisés utilisés doivent être validés et des processus doivent être mis en place pour assurer la maîtrise de l'intégrité des données.

IV. Outil de suivi, ou « Audit trail »

Définition

L'outil de suivi des créations, modifications et suppression des données permet de couvrir plusieurs principes de l'ALCOA+ comme Attribuable, Précise, Cohérente et Complète. C'est un outil puissant permettant de nous assurer de l'intégrité de nos données et pour cela, il faut s'assurer qu'il est bien configuré, qu'il est revu régulièrement. Les textes réglementaires comme les BPF et la 21CFR part 11 ont commencé à encadrer l'utilisation de ces outils. Les référentiels comme les guides du PIC/S et les GAMP regroupent des recommandations pour faire une utilisation efficiente de cet outil au sein des industries pharmaceutiques. Un outil de suivi peut être sous un format papier ou électronique. Le risque majeur du format papier est l'oubli d'enregistrer une action. L'informatisation de l'outil de suivi permet d'enregistrer chaque action de façon exhaustive et automatique. Ainsi, cela permet de s'affranchir de ce premier risque.

Grâce à cet outil ou journal de suivi, les données peuvent être complètes. Pour chaque action de création, modification ou suppression, les éléments suivants doivent être présents :

- L'identification de l'auteur, généralement le système récupère les informations de la personne connectée au système : cela nous permet d'avoir une donnée attribuable,
- L'horodatage de l'action, l'idéal est que le système soit relié à un serveur commun aux autres systèmes pour que chaque horodatage ait la même source : cela nous permet d'avoir des données cohérentes entre elles,
- Pour une modification ou une suppression, la donnée précédent la correction ou la suppression doit être présente : cela nous permet d'assurer la disponibilité de toutes les données et tous leurs cycles de vie.

Dans l'exemple d'un système de données chromatographique d'un laboratoire de contrôle qualité, le journal de suivi peut intervenir à différentes phases comme indiqué dans la Figure 6 [25]. Il enregistre l'ensemble des actions réalisées tout au long du cycle de la donnée :

- La génération de la donnée brute,
- Le traitement de la donnée,
- L'utilisation de la donnée,
- Les rapports associés.

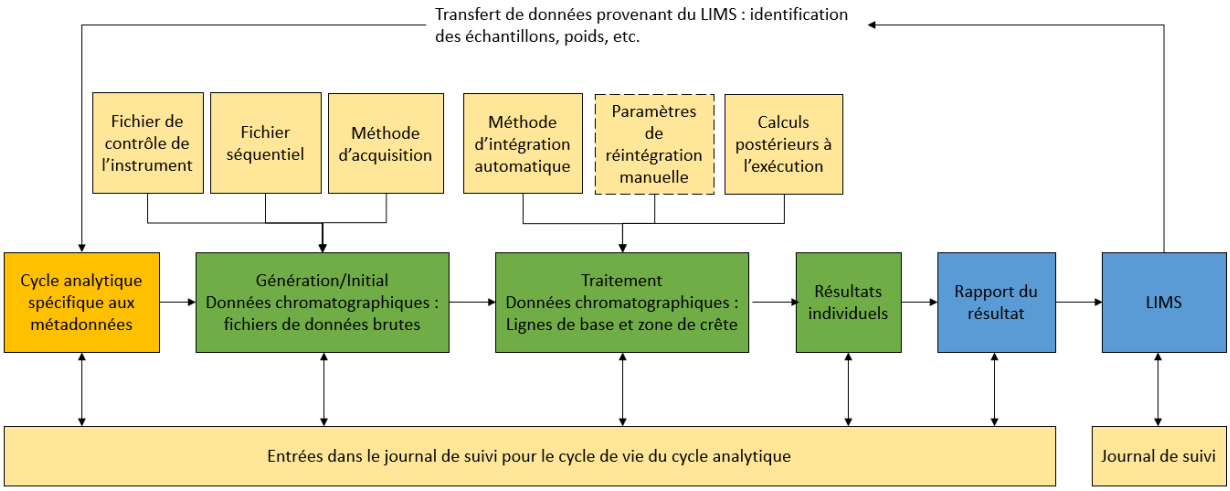


Figure 6 Journal de suivi quand un LIMS est interfacé avec un CDS (Chromatography Data System) traduit de l'article « The Why, What, and How CDS Audit trail Review » [25]

Cette figure montre les interfaces entre le système CDS (Chromatography Data System) et le LIMS, ce qui implique des problématiques propres :

- L'identification de l'auteur doit être issu de la même base de données pour ne pas avoir de risque d'erreur,
- L'horodatage doit avoir la même source pour les deux systèmes pour avoir une chronologie des événements cohérentes.

Ainsi, cela illustre qu'interfacer l'ensemble des systèmes facilitent l'accès à l'ensemble de l'historique de chaque produit. L'outil de suivi est utilisé dans la détection de potentielles fraudes [26]. En effet, ce journal permet de détecter des « signaux d'alarme », et de documenter les actions des utilisateurs. L'analyse de ces données statiques permet de faire une revue des changements d'accès, des changements de la sécurité, des contournements de la sécurité ou de la détection de fraude.

Evolution réglementaire

Dans les BPF publiées en 2007, la partie Système informatisé était comprise dans le Chapitre 3 « Gestion de la qualité et Documentation », il n'y avait pas de mention d'un journal de suivi des changements, appelé « audit trail ». Cependant, il était demandé d'avoir un suivi des changements ou suppression avec le nom de l'auteur et la date correspondante. Il n'était pas explicitement demandé de les revoir à fréquence régulière. S'il n'apparaissait pas clairement qu'une revue de l'historique des données étaient nécessaires, il était écrit explicitement que les personnes réalisant les modifications ou les suppressions doivent y être autorisées [19].

Dans la version des BPF publiée en 2011, dans la ligne directrice 11 « Système informatisé », cette partie sur les outils de suivi a été modifié. Il est toujours demandé d'avoir un suivi des modifications des données importantes avec l'identification de la personne et le motif du changement. Il est proposé d'avoir un outil permettant un enregistrement de toutes les entrées et de toutes les modifications. Dans cette version des BPF, la suppression des données n'est pas citée dans le cadre de cet outil [20].

Dans la version des BPF publiée en 2015, l'annexe 11 est plus détaillée. En effet, la mention de l'outil de suivi dit « Audit trail » dans le paragraphe 9 « traçabilité des modifications » apparaît. Il y est ajouté que la revue doit être faite à fréquence régulière [21]. Depuis cette version de 2015, le texte sur les outils de suivi n'a pas évolué. Les interactions entre les différentes parties des BPF, au sujet de la traçabilité et des journaux de suivi, est détaillée dans la Figure 7.

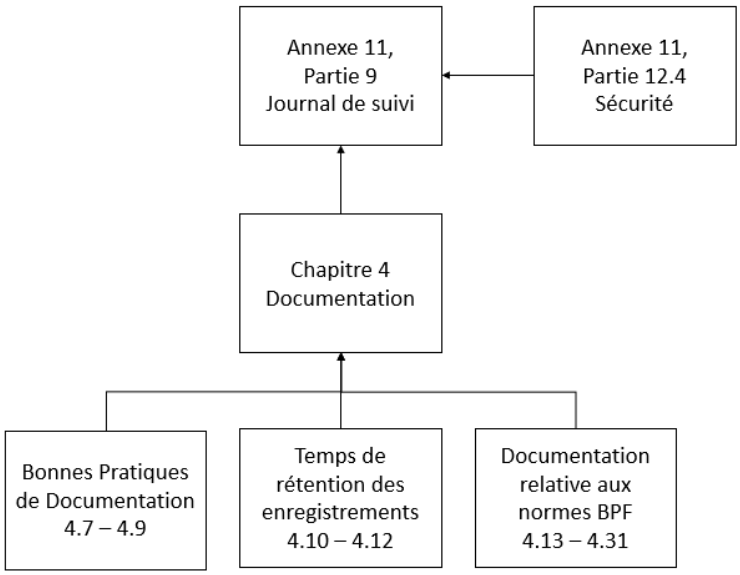


Figure 7 Relations entre le paragraphe 9 pour les journaux de suivis et les autres paragraphes des BPF traduit du livre « EU Annex 11 Guide to Computer Validation Compliance for the Worldwide Health Agency GMP » [27]

Dans « Data Integrity and Compliance With Drug CGMP, Questions and Answer, Guidance for Industry » publié en 2018, la FDA répond à des questions concernant la maîtrise de l'intégrité des données [18]. Deux questions parmi les 18 sont à propos des outils de suivi et de leur revue. Ces réponses constituent des lignes directrices pour déterminer qui doit faire la revue et la fréquence de ces revues. Ces éléments seront détaillés dans la Partie 2 : La gestion de l'intégrité des données et les outils de suivi des activités : la réglementation, leurs spécificités et leurs contraintes.

L'évolution des préoccupations

Comme pour le mot clé « Data integrity », l'analyse via l'outil « Trends » de l'entreprise Google, du mot clé « Audit trail », nous donne le graphique suivant (Figure 8). Nous pouvons voir que le pic du taux d'utilisation de ce mot clé apparaît en 2022 et qu'il y a une augmentation de 44 points entre 2012 et 2022. L'intérêt et les questionnements autour de ce sujet sont donc de plus en plus important [28].

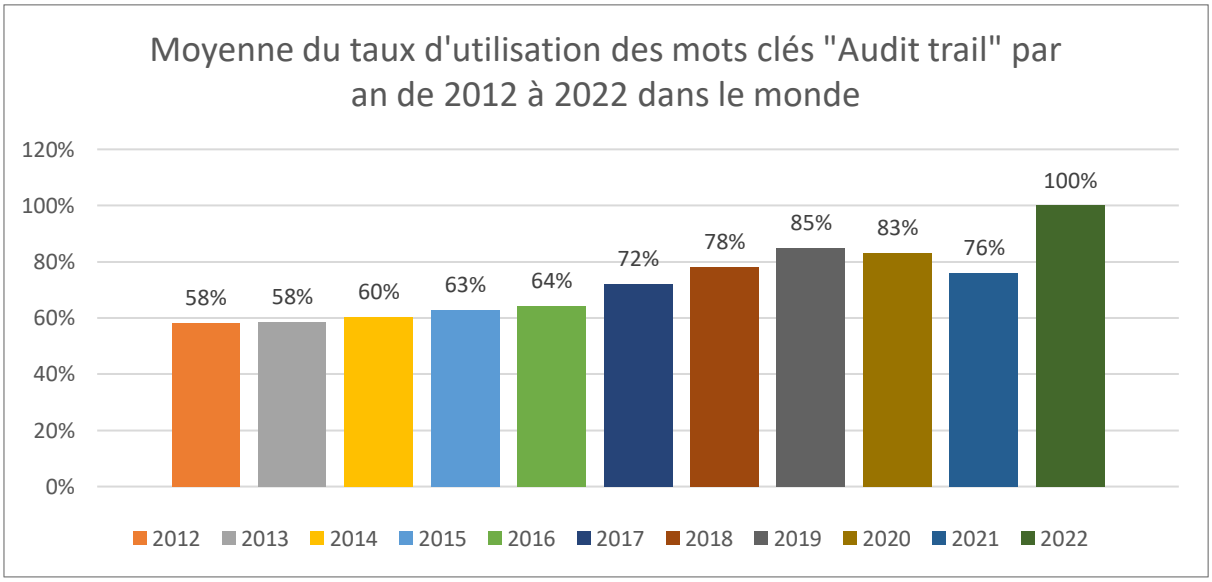


Figure 8 Représentation des moyennes du taux d'utilisation des mots clés "Audit trail" par an, de 2012 à 2022, dans le monde sur Google

Les injonctions et lettres d'avertissements

Aucune injonction publiée par l'ANSM ne porte sur les outils de suivi [24]. Le sujet n'a donc pas encore fait l'objet d'un écart critique selon les inspecteurs. Leurs attentes, auprès des industries pharmaceutiques, en matière de présence et d'exploitation des outils de suivi, semblent satisfaites. En revanche, de janvier 2018 à aout 2022, la FDA a publié 45 lettres d'avertissement portant sur les outils de suivi et leurs exploitations [23].

Dans ces lettres d'avertissement, la FDA demande que des outils de suivi soient présents, activés et configurés sur les systèmes. De plus, la FDA demande des procédures concernant la revue des outils de suivi.

Partie 2 : La gestion de l'intégrité des données et les outils de suivi des activités : la réglementation, leurs spécificités et leurs contraintes

L'ensemble des documents mentionnés dans cette thèse sont présents dans l'organigramme en Annexe 1 : Organigramme des réglementations et des référentiels en fonction de leurs domaines d'application. Ces documents soit font partie de réglementations françaises et américaines, soit sont des recommandations. Celles-ci peuvent être rédigés par des organismes étatiques comme l'ANSM, la FDA ou l'EMA, des organismes comme l'ISPE, le PIC/S ou l'ISO. Dans l'organigramme, les documents sont séparés en fonction de leur domaine d'application cela peut être les médicaments, les dispositifs médicaux/dispositifs in vitro (DM/DIV), la gestion des données patients, ou l'ensemble des produits.

I. La réglementation autour de l'intégrité des données

Les Bonnes pratiques de Fabrication

Les BPF abordent le sujet de la gestion de l'intégrité des données dans le chapitre 4 « Documentation » et dans l'annexe 11 « Système informatisé » [3]. Il y est mentionné quelques éléments composants l'ALCOA+ comme dans l'article 4.8 où il est demandé que les enregistrements soient « *effectués ou finalisés au moment où chaque action est réalisée* », ce qui correspond à la définition du mot « Contemporain ». Le but, selon les BPF, est d'éviter tout oubli de traçabilité. La précision, la disponibilité et la lisibilité des documents sont aussi mentionnées. Le principe de l'attribuabilité d'un enregistrement à un lieu/équipement et à une personne ainsi que l'horodatage sont aussi rappelés dans ce chapitre.

Pour garantir leur respect, les BPF demandent que des processus de contrôles soient mis en place. Or le mot « contrôle » peut être compris de deux façons différentes en français. Il y a des stratégies de contrôles qui s'apparentent à de la maîtrise du processus, une stratégie de maîtrise du risque liés à la gestion de l'intégrité des données. D'autres stratégies de contrôle correspondent à des vérifications régulières de ce qui a été réalisés pour s'assurer que tout a été effectué comme prévu. Si un contrôle est automatisé, cette fonction doit être validée et maintenue en condition opérationnelle. Ce contrôle doit être maintenu pendant tout le cycle

de vie de chaque données dites BPF, c'est-à-dire celles qui se rapportent aux « *activités qui influent – directement ou indirectement – sur tous les aspects de la qualité des médicaments* ».

La même exigence est demandée pour les documents papier ou électronique, avec des moyens de la satisfaire différents. Les processus à maîtriser pour assurer l'intégrité des données sont la gestion de la documentation (papier ou numérique), la gestion des copies certifiées conformes à l'original, la gestion du cycle de vie des données et le respect des principes de l'ALCOA+.

L'annexe 11 « Systèmes Informatisés » insiste sur l'application de la maîtrise de ces processus en passant par la maîtrise du risque. Pour cela, un des moyens sur lequel s'appuie particulièrement les BPF est la validation des systèmes utilisés pour assurer la qualité des processus réalisés. Par exemple, pour assurer l'intégrité des données sauvegardées, les BPF demandent que les processus de sauvegarde et de restauration soient « *vérifiés pendant la validation et contrôlées périodiquement.* ». La validation d'un système consiste à vérifier que l'ensemble des fonctions donnent les résultats voulus sans altérer les données au travers de la réalisation de tests. La validation est clôturée par un rapport contenant la conclusion, les tests effectués ainsi que les preuves.

Pour déterminer quels systèmes doivent être validés et ce qu'il est nécessaire de valider dans chaque système, les BPF demandent que ces décisions soient basées sur une notion de maîtrise du risque. Cette dernière correspond à l'identification et la qualification de l'ensemble des risques, ainsi qu'à la prise de décisions pour diminuer et/ou accepter ces risques. Cette notion est développée dans l'ICH (International Council for Harmonisation of Technical) Q9 « Gestion du Risque Qualité ». L'ICH Q9 est une norme qui a été intégré aux BPF dans la partie 3 « Documents relatifs aux Bonnes Pratiques de Fabrication ».

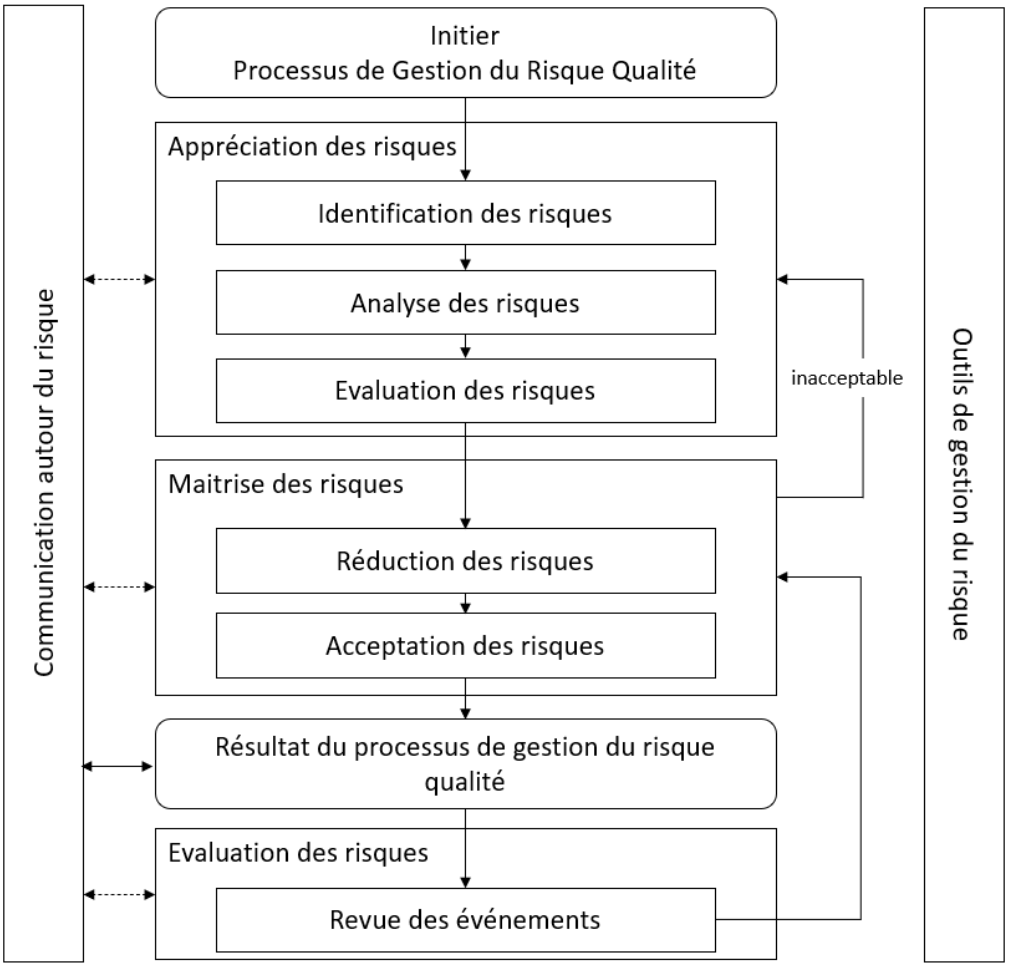


Figure 9 Aperçu d'un procédé de gestion du risque qualité classique traduit des Bonnes Pratiques de Fabrication, Gestion du risque Qualité (ICH Q9) [3]

Comme indiqué dans la Figure 9, la gestion du risque qualité est composée de quatre grandes étapes : « *Appréciation du risque* », « *Maîtrise du risque* », « *Communication relative au risque* » et « *Revue du risque* ». L'appréciation du risque est composée de l'identification, de l'analyse et de l'évaluation du risque. Les critères à prendre en compte sont la sécurité du patient, l'intégrité des données et la qualité du produit. Ensuite lors de la maîtrise du risque, il y a une première étape de réduction du risque puis une phase d'acceptation ou non du risque résiduel.

Tableau 2 Analyse de risque issus de l'ISPE GAMP 5 : « A risk-based approach to compliant GxP computerized system » [12]]

			Evaluation du risque						Gestion du risque restant	
Référence du risque	Fonctionnalité du système	Scénario à risque	Gravité de l' impact	Probabilité d' occurrence	Classe de risque	Probabilité de détection	Priorité du risque	Mesure de mitigation	Risque résiduel	Actions
			Elevé/ Moyen /Faible	Elevé/ Moyen /Faible	Elevé/ Moyen /Faible	Elevé/ Moyen /Faible	Elevé/ Moyen /Faible		Elevé / Moyen/ Faible	

L'l'ISPE GAMP 5 : « A Risk Based Approach to compliant GxP computerized systems » propose d'effectuer l'analyse de risque comme indiqué dans le Tableau 2 [12]. A chaque mode de défaillance appelé ici « Risque » est assigné une référence pour permettre une meilleure communication au sein de l'entreprise. Chaque risque est associé à une fonctionnalité du système. Une même fonctionnalité peut avoir différents scénarios à risque. Ces scénarios autrement appelés « Worst case scenario » correspondent à ce qui pourrait arriver de plus grave en cas de défaillance, de mauvaise utilisation ou pour une autre raison. Pour chaque scénario, il faut évaluer la classe puis la priorité du risque. La première étape est l'évaluation de la gravité c'est-à-dire l'évaluation des conséquences possibles d'un danger. Une gravité peut être :

- Elevée : Le risque a un impact direct sur la sécurité du patient et/ou la qualité du produit,
- Moyenne : Le risque a un impact indirect sur la sécurité du patient et/ou la qualité du produit,
- Faible : Le risque n'a pas d'impact sur la sécurité du patient et/ou la qualité du produit.

La probabilité d'occurrence est ensuite évaluée, cela consiste à évaluer la possible récurrence d'un risque. Par exemple, il est possible de se baser sur la fréquence d'utilisation d'une fonction du système : plus une fonction est utilisée plus le risque associé à une probabilité d'occurrence élevée. Cette probabilité peut être élevée, moyenne ou faible selon les critères définis et propres à chaque entreprise et/ou système.

Ces deux éléments nous permettent d'évaluer la classe du risque selon le Tableau 3 à double entrée suivant :

Tableau 3 Tableau d'évaluation de la classe du risque en fonction de la gravité et de la probabilité d'occurrence de ce risque traduit de l'ISPE GAMP 5 : « A Risk Based Approach to compliant GxP computerized systems » [12]

		Probabilité d'occurrence		
		Faible	Moyenne	Elevée
Gravité	Elevée	Classe de risque 2	Classe de risque 1	Classe de risque 1
	Moyenne	Classe de risque 3	Classe de risque 2	Classe de risque 1
	Faible	Classe de risque 3	Classe de risque 3	Classe de risque 2

Enfin, il y a l'évaluation de la probabilité de détection. La détectabilité correspond à la capacité à mettre en évidence ou identifier ce risque. Cette probabilité peut être élevée, moyenne ou faible selon les critères définis et propres à chaque entreprise et/ou système.

La classe du risque et la probabilité de détection nous permettent de définir la priorité du risque selon le Tableau 4 à double entrée suivant :

Tableau 4 Tableau d'évaluation de la priorité du risque en fonction de la classe du risque et de la probabilité de détection de ce risque traduit de l'ISPE GAMP 5 : « A Risk Based Approach to compliant GxP computerized systems » [12]

		Probabilité de détection		
		Elevée	Moyenne	Faible
Classe de risque	1	Risque Moyen	Risque Elevé	Risque Elevé
	2	Risque Faible	Risque Moyen	Risque Elevé
	3	Risque Faible	Risque Faible	Risque Moyen

A la suite de cette évaluation, vient l'étape de maîtrise et d'acceptation du risque. Pour cela, une ou plusieurs mesures de mitigation sont mises en place. Ces mesures peuvent correspondre à la réalisation de tests pour la validation d'une fonctionnalité du système, à la mise en place d'un processus, etc. A la suite de l'application de ces mesures de mitigations, le risque est réévalué. Pour pouvoir conclure que l'ensemble des risques sont maîtrisés, les risques résiduels doivent être tous au niveau « faible ». Si ce n'est pas le cas, de nouvelles mesures de mitigation sont mises en place pour maîtriser le risque en routine. Cette méthodologie d'analyse et de maîtrise de risque doit être menée en groupe pluridisciplinaire où chaque personne apporte son expertise et où les mesures et les conclusions sont prises de façon collégiale.

Comme indiqué sur la Figure 9, la dernière étape de la gestion du risque est un examen du risque qui consiste en une surveillance de l'ensemble des données provenant de ce processus et tenant compte des nouvelles connaissances scientifiques et de l'expérience liée à ce risque. Cette étape est répétée selon une fréquence définie en amont. Le choix de cette fréquence doit être justifié, il est propre à chaque entreprise et/ou système. Cette étape est aussi appelée « l'évaluation périodique ». Elle est aussi nécessaire pour assurer que l'ensemble des systèmes concernés sont toujours dans un état validé et qu'ils sont conformes aux BPF [3].

De plus, des sujets complémentaires au chapitre 4 sont abordés dans l'annexe 11 comme la gestion des interactions entre les systèmes pour lesquels les BPF proposent une nouvelle fois, de mettre en place des moyens de contrôles pour éviter la perte de l'intégrité des données. Il en est de même pour la maîtrise du risque autour de l'ajout manuel de données dans un système. Ces mesures permettent d'assurer que les données soient toujours exactes.

Il est rappelé que les éléments stockés doivent être protégés dans le but de répondre à des critères de l'ALCOA+ tels que l'accessibilité, la lisibilité et l'exactitude. Il est aussi indiqué que les fonctionnalités susceptibles d'interagir tout au long du cycle des données BPF, doivent être validées et les activités doivent être contrôlées.

La maîtrise de l'intégrité des données est aussi un sujet développé dans les cGMP où les principes de l'ALCOA+ sont détaillés [8]. De façon similaire aux BPF, la FDA demande que les équipements électroniques, mécaniques ou automatiques aient une gestion des accès, une validation de l'exactitude des données d'entrées ou de sortie. De plus, la FDA propose de prendre en compte la complexité et la fiabilité du système pour déterminer les contrôles à effectuer.

La conception et la production de chaque DM sont évaluées par un organisme notifié [29]. Il évalue l'aptitude à atteindre la qualité voulue, sur la base de la documentation technique du produit dont la documentation décrivant les méthodes de contrôle de la gestion de la qualité. Si l'évaluation est conforme aux attentes, l'organisme notifié certifie que le fabricant a la capacité de fournir un marquage CE pour le DM concerné. L'ensemble des étapes du circuit pour la demande et la décision de certification d'un fabricant par un organisme notifié est illustré par la Figure 10.

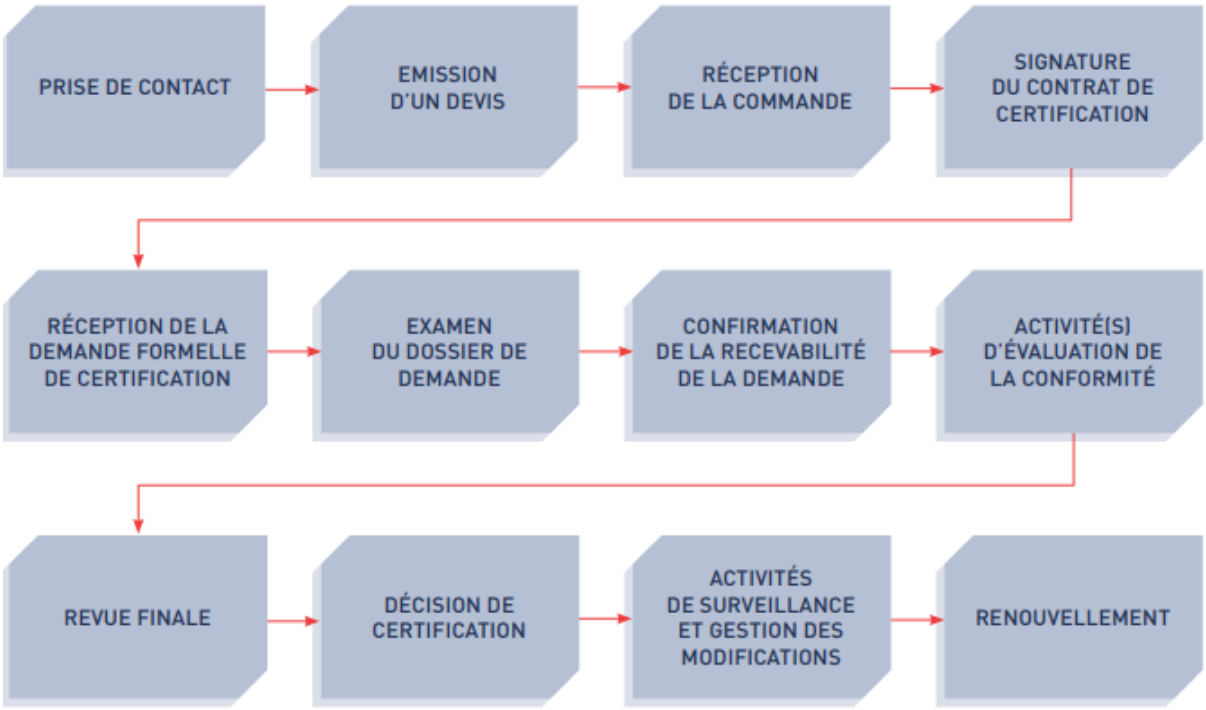


Figure 10 Processus de certification selon le règlement (UE) 2017/745 présent dans le guide « Demande de certification en vue de marquage CE Règlement (UE) 2017/745 » du groupe GMED [29]

Comme indiqué dans l'annexe XI « Evaluation de la conformité sur la base de la vérification de la conformité du produit » du règlement sur les DM [4], les organismes notifiés doivent baser leur décision sur les documents techniques, c'est-à-dire sur le Manuel d'assurance qualité qui doit contenir tous les éléments détaillés dans l'annexe IX « Evaluation de la conformité sur la base d'un système de gestion de la qualité et de l'évaluation de la documentation technique ». La vérification du produit est ensuite réalisée par le fabricant ou par l'organisme notifié pour délivrer une déclaration de conformité UE. L'ensemble des processus effectués doivent correspondre à la documentation technique vérifiée par l'organisme notifié. Les éléments composant cette documentation technique sont détaillés dans les annexes II et III du règlement sur les DM. Les éléments suivants y sont présents :

- La description et les spécifications du dispositif, y compris les variantes et les accessoires,
- Les informations sur la conception et la fabrication,
- Les exigences générales en matière de sécurité et de performances,
- L'analyse bénéfice/risque et gestion des risques,
- La vérification et la validation du produit,
- Les informations relatives à la surveillance après commercialisation.

Le principe général que doivent appliquer les fabricants en matière de maîtrise de la sécurité et de la performance de leur DM est le principe de gestion du risque. Selon l'article 17 « Système électroniques programmables » de l'annexe I du règlement DM/DIV, pour les mesures de maîtrises des risques, les fabricants doivent prendre leur décision en fonction de l'état de l'art généralement admis. Les principes de validation du système et de protection contre les accès non autorisés, de gestion documentaire sont inscrits dans ce règlement. Ces principes sont communs aux BPF. L'ensemble des procédures permettant la maîtrise de l'intégrité des données font partie des documents devant être audités par l'organisme notifié.

Dans ses recommandations concernant la cybersécurité des Dispositifs Médicaux Intégrant du Logiciel (DMIL) [30], l'ANSM demande que le DM satisfasse les exigences d'un système de management de la qualité « classique » et que des objectifs de sécurité soient définis pour des bien critiques à protéger. Ces biens sont, a minima :

- Le firmware, autrement appelé micrologiciel, c'est un programme intégré dans un équipement pour qu'il puisse fonctionner,
- Le paramétrage médical, comme la gestion des accès, le paramétrage du système en générale,
- Les clés cryptographiques, ce sont des éléments permettant de transformer un message clair en un message incompréhensible sans disposer de la clé de déchiffrement,
- Le journal des événements, autrement appelé outil de suivi ou « audit trail »,
- Les données relatives aux patients, comme l'identité, la maladie, les traitements du patient.

Le but est d'assurer la confidentialité et l'intégrité des données via le journal des événements et le paramétrage médical. Ce dernier permet, par exemple les fonctions de traitement de données brutes.

La FDA a aussi émis des recommandations concernant la cybersécurité des DM [31]. Lors du développement et de la conception du dispositif, l'identification et l'évaluation de l'impact des menaces et vulnérabilités doit être réalisée, ainsi que l'évaluation du risque résiduel présent après la mise en place des mesures de mitigation. La FDA est plus précise que l'ANSM sur le traitement des menaces. Elles peuvent être d'ordre général et peuvent concerner l'intégrité des données. Pour ces dernières, la FDA demande que :

- L'intégrité des données entrantes soit vérifiée,
- Le transfert de données puisse se faire en toute sécurité, en utilisant des méthodes de cryptage ou d'authentification par exemple,
- L'intégrité des données soit protégée pour assurer la sécurité et les performances essentielles du dispositif,
- L'ensemble des normes actuelles recommandées soient mises en application, comme l'utilisation d'une protection cryptographique pour les moyens de communication.

La réglementation pour les matières premières à usage pharmaceutique, les médicaments à usage vétérinaire, les cosmétiques et la pharmacovigilance

Pour les matières premières à usage pharmaceutique et les médicaments à usage vétérinaire, la réglementation insiste sur le management de la qualité et la gestion des risques. Les exigences présentent dans ces réglementations sont similaires à celles des médicaments à usage humain.

Il en est de même pour les produits cosmétique pour lesquels, il est noté dans l'article 8 du règlement Cosmétique n°1223/2009 CE [5] que la fabrication de ces produits doit être réalisée en conformité avec les BPF présent dans la norme harmonisée NF EN ISO 22716 « Cosmétiques – Bonnes Pratiques de Fabrication (BPF) – Lignes directrices relatives aux Bonnes Pratique de Fabrication » [32]. Les grands principes de la maîtrise de l'intégrité des données sont présents dans la partie 17-Documentation. Le but de ces principes est d'avoir des documents lisibles, compréhensibles, rédigés et complétés par des personnes autorisées. Les documents doivent avoir l'historique des activités au complet pour éviter toute perte d'information ou mauvaise interprétation.

Selon les Bonnes Pratiques de Pharmacovigilance (BPPV), il est essentiel d'avoir confiance dans les données de pharmacovigilance [33]. Pour cela, l'exploitant a la charge de la traçabilité des données enregistrées. Il doit mettre en place un système d'assurance et de contrôle de la qualité des données enregistrées. Ces données doivent être complètes, exactes et intègres car

elles peuvent être compilées dans un rapport d'enquête de pharmacovigilance, le cas échéant. Cependant, en termes de gestion de l'intégrité des données, les BPPV ne sont pas aussi détaillées que les BPF.

Les normes

Les normes internationales sont utilisées par les industriels comme des référentiels pour définir l'état de l'art à appliquer et ainsi, s'assurer de répondre aux attentes implicites de leurs clients et des autorités. Dans le cadre de la gestion de l'intégrité des données, des normes généralistes tels que la NF EN ISO 9001 – 2015 : « Système de management de la qualité » [34] et la NF EN ISO 14001 – 2015 : « Système de management environnementale » s'appliquent [35]. Pour l'approche processus, recommandée par la première norme, dans le cadre d'un système de management de la qualité, il faut 4 éléments. L'un de ces éléments est « l'amélioration des processus sur la base d'une évaluation de données et d'informations ». Ainsi, pour pouvoir exploiter ces informations, il est nécessaire d'avoir confiance en nos données et donc que les principes de l'ALCOA+ soient respectés. Pour le principe de la maîtrise des informations développé dans la seconde norme, il est nécessaire de mettre en place un processus de maîtrise des modifications complété par un processus de revue des modifications effectuées. L'ensemble des informations et modifications revues doivent être en accord avec l'ensemble de la pyramide documentaire. Cependant, la norme ne détaille ni comment cette revue doit être mise en place ni les éléments qui doivent être revus.

La norme NF EN ISO 27001 : 2023 : « Sécurité de l'information, cybersécurité et protection de la vie privée – Systèmes de management de la sécurité de l'information » [36], détaille le processus de maîtrise du risque nécessaire pour préserver la confidentialité, l'intégrité et la disponibilité des informations. Ce processus est nécessaire pour assurer que les risques soient gérés de façon adéquate. Comme présenté dans la Figure 11, le processus de maîtrise du risque est un enchaînement de cinq étapes identiques quelques soit les risques concernés.

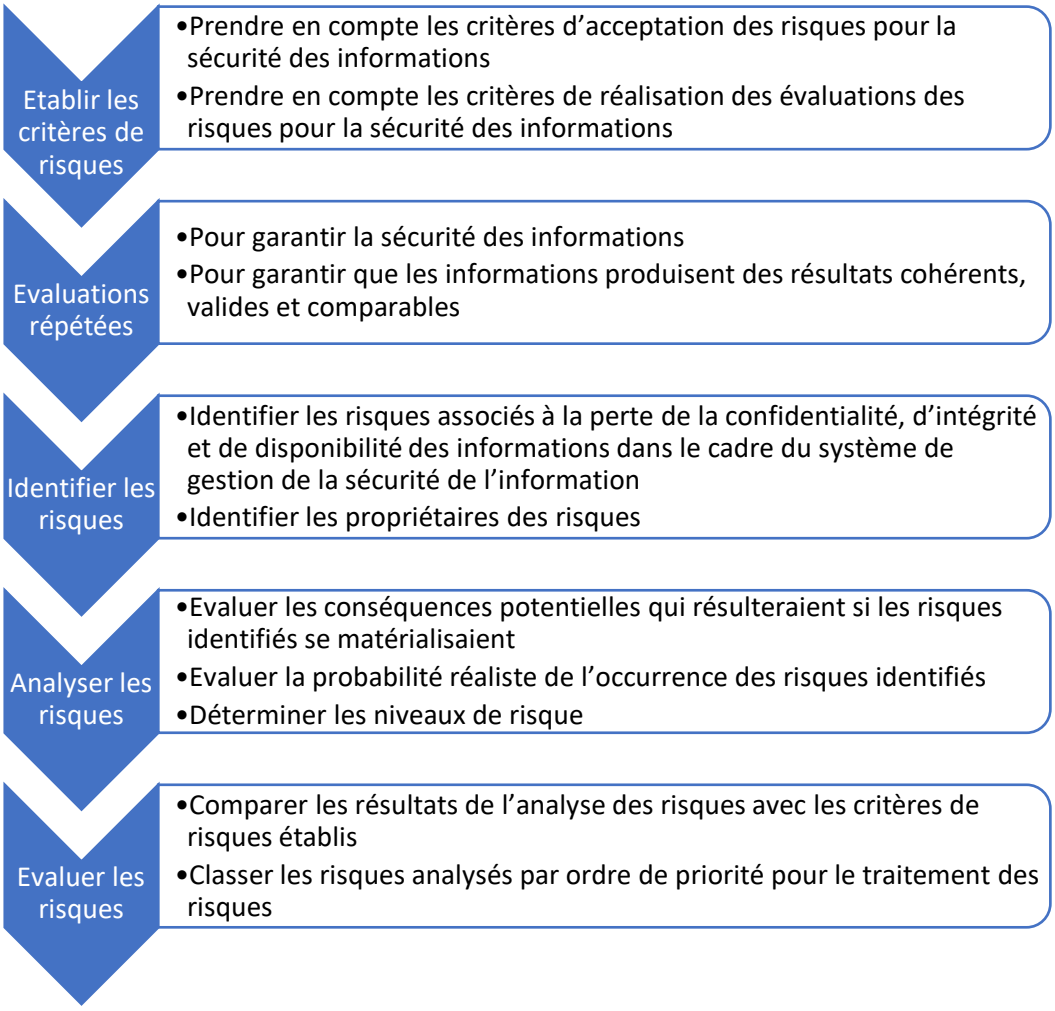


Figure 11 Logigramme d'un processus de gestion de la maîtrise de risque

La première étape, détaillée dans la Figure 11 consiste à définir les critères à prendre en compte pour l'acceptation du risque et l'ensemble du système d'évaluation des risques. Il est nécessaire de définir les critères, la grille d'évaluation, les critères d'acceptation du risque en amont du déploiement de ce processus. Ces définitions permettent de déployer ce processus de façon reproductible quel que soit le risque et le personnel impliqués. La deuxième étape consiste à définir la périodicité de la réévaluation des risques. Cette période doit être défini dans le but de toujours pouvoir garantir la sécurité des informations et que les résultats issus de celles-ci soient cohérents, valides et comparables. La troisième étape consiste à identifier les risques présents sur un système ou un processus. Les risques concernent la perte de confidentialité, d'intégrité et de disponibilité des informations. Dans cette étape, il peut être intéressant d'identifier les personnes associées à ces risques pour avoir leurs expertises sur les moyens de maîtrise de risque à mettre en place. La quatrième étape consiste à analyser les risques, c'est-à-dire évaluer les conséquences potentielles résultant de ce risque, évaluer

leur gravité, fréquence, probabilité d'occurrence et de détection. La dernière étape consiste à évaluer les risques. Grâce à l'ensemble de ces critères, il est possible de définir le niveau de chaque risque et ainsi, déterminer s'ils sont maitrisés ou si une action est à mettre en place. L'ensemble de ces étapes sont aussi présentes dans l'ICH Q9 « Gestion du risque qualité » développé dans la Partie 2 : La gestion de l'intégrité des données et les outils de suivi des activités : la réglementation, leurs spécificités et leurs contraintes, I-La réglementation autour de l'intégrité des données, Les Bonnes pratiques de Fabrication.

La norme NF EN ISO 60601-1 : « Appareils électromédicaux – Partie 1 Exigences générales pour la sécurité de base et les performances essentielles » [37] explicite les conséquences des risques devant être pris en compte dans une analyse de risque. Pour la sécurité de l'informations les situations dangereuses sont :

- La perte de données,
- L'échange inapproprié de données,
- Des données corrompues,
- La synchronisation inappropriée des données,
- La réception inattendue de données,
- L'accès non autorisé aux données,
- Les données indisponibles,
- Le manque d'intégrité des données,
- Les données incorrectes,
- Le manque de sécurité des données et ses effets sur la confidentialité des données, en particulier la vulnérabilité aux falsifications,
- Les interactions non désirées avec d'autres programmes et virus,
- La défaillance du réseau informatique à fournir les caractéristiques nécessaires pour attendre la sécurité de base ou les performances essentielles.

A ce propos, la norme NF EN ISO 62443-4-1 : « Sécurité des automatismes industriels et des systèmes de commande - Exigences relatives au cycle de vie de développement de produit sécurisé » [38] ajoute que lors du développement des produits, des éléments de l'architecture du logiciel peuvent être utilisés pour permettre la maîtrise des risques. Ces éléments sont :

- Les bases de données,
- Les fichiers de configurations,
- Les magasins de clés cryptographiques,
- Les listes de contrôle d'accès,
- Les clés de registres,
- Les pages web,
- Les journaux d'audit,
- Les supports de réseau,
- Les moyens de communications entre processus,
- Les autres fichiers et répertoire.

L'ensemble des éléments détaillées dans ces normes définissent l'état de l'art autour de la maîtrise des risques pour la gestion de l'intégrité des données. Elles donnent la démarche complète pour avoir un processus efficient.

II. La réglementation autour de l'outil de suivi

Les Bonnes pratiques de Fabrication

Dans les BPF, Annexe 11 "Système informatisé" [3], à propos de la traçabilité des modifications, il est inscrit :

> *"Il doit être envisagé, sur la base d'une analyse de risques, l'inclusion au sein du système informatisé d'un journal (dit « audit trail ») permettant de conserver la trace de toute modification ou suppression survenue sur les données ayant un impact BPF. Toute modification ou suppression d'une donnée ayant un impact BPF doit être justifiée et documentée. L'« audit trail » doit être disponible, convertible dans un format compréhensible et revu à fréquence régulière."*

Ce paragraphe permet d'avoir un premier aperçu de ce qui est attendu. Les BPF parlent d'un "journal" qui doit être informatisé. Cependant il n'est pas dit clairement ce qui est attendu en cas d'absence d'un outil semblable. A ce propos, la FDA [8] et le guide ISPE GAMP : « Records and Data Integrity » [13] préconisent de mettre un outil semblable pour maîtriser le risque résiduel. Les outils peuvent être des mesures physiques comme l'impossibilité de modifier ou de supprimer des données, un double contrôle ou via des procédures administratives spécifiques. Il est aussi possible de suivre les modifications et suppressions par un document papier.

Les journaux de suivis tracent les actions de modifications et de suppressions faites sur les données dites BPF. Contrairement aux BPF, la FDA et les autres référentiels, mentionnent aussi le suivi des créations de données. Il semblerait que pour les BPF, ce n'est pas au moment de la création qu'il y a un risque au niveau de l'intégrité de la donnée mais que le risque apparaît lorsqu'il y a une volonté de la modifier ou de la supprimer. Cependant, les BPF demande que les systèmes permettant la *« gestion des données et des documents doivent être conçus pour enregistrer l'identité des utilisateurs impliqués dans la saisie, la modification, la confirmation ou la suppression de données, y compris la date et l'heure* » [3]. Pour satisfaire à cette exigence, l'utilisation d'un outil de suivi est le plus adapté mais ici, les BPF demande que les données « saisies », c'est-à-dire les données créées, soit aussi suivies. Les BPF ajoutent à ce sujet, que chaque modification doit être datée, signée, la mention précédente doit toujours être lisible et qu'il peut être nécessaire d'avoir une justification documentée pour chaque modification ou suppression.

A différents endroits des BPF [3], il est mentionné des éléments pour lesquels un suivi est nécessaire. Par exemple, dans l'annexe 11, si des impressions papiers sont générées et utilisées pour la libération des lots, il doit être indiqué quelles modifications ont été réalisées. Dans le cadre de cet exemple, un outil de suivi permet de remplir cette fonction et de satisfaire à l'ensemble des critères de l'ALCOA+. Un autre exemple d'utilisation des outils de suivi est pour la gestion des accès informatique. En effet, chaque création, modification et annulation des autorisations d'accès informatique doivent être enregistrées. Les outils de suivi permettent de répondre à cette exigence. De plus, il est ainsi possible de contrôler qu'aucun changement non autorisé n'a été effectué. Pour aller plus loin, un outil de suivi permet aussi de tracer l'ensemble des tentatives de connexions effectuées, ainsi il est possible de voir s'il y a eu une intrusion dans le système. Dans le cadre d'un changement de configuration, à la suite de la réalisation d'un processus de maîtrise des risques, et de la réalisation de ce changement, l'outil de suivi permet de produire des preuves de la réalisation de ce changement. Dans l'ensemble de ces cas, l'utilisation d'un outil de suivi semble adaptée mais n'est pas explicitement demandée par les BPF.

A propos l'outil de suivi, il est mentionné dans les BPF, que cette métadonnée, doit répondre aux principes de l'ALCOA+ et que celui-ci doit être revu à fréquence régulière. Les BPF ne détaillent pas la méthodologie à adopter pour la réalisation de ces revues. Selon la FDA [8], il existe différents types de revues en fonction des données concernées. Les revues peuvent être "lot par lot" pour les données nécessaires à la libération des lots. Cette revue est réalisée pour s'assurer que l'ensemble des activités ont été réalisées comme décrites dans les procédures. En effet, il est essentiel que les métadonnées soient examinées conjointement avec leurs données associées afin de fournir le contexte et la signification des données. Pour les autres données dites BPF mais non nécessaire à la libération des lots, la fréquence doit être définie à l'aide des connaissances du processus et d'outils d'évaluation des risques. L'évaluation de la criticité doit prendre en compte les mécanismes de contrôle et l'impact sur la qualité du produit. La revue du journal de suivi réalisée selon ce processus permet d'atténuer le risque et de garantir l'intégrité des enregistrements. Cette maîtrise du risque permet de rendre la revue périodique plus efficiente, en effet, il n'est pas nécessaire d'être exhaustif pour ce type de revue. La FDA recommande d'avoir un système standard qui définit clairement quelles données devraient être soumises aux bonnes pratiques liées au journal de suivi [39]. De plus, il est nécessaire d'établir des procédures pour fournir les informations autour de l'utilisation et de la gestion des journaux de suivi et pour maintenir un état de conformité.

Contrairement à la FDA [7], les BPF ne nous guide pas sur le personnel qui doit avoir la charge de ces revues. Pour la FDA, Les personnes en charge de ces revues doivent être le même personnel que celui qui est chargé de l'examen des enregistrements dans le cadre GMP. Il est important que la revue soit effectuée par des experts métier car ce sont les personnes qui ont les connaissances les plus approfondies du système et du processus. Ils seront les plus à même d'identifier les problèmes, leurs sources et la gravité de leur conséquence.

La réglementation DM/DIV

Comme dit précédemment dans la partie « I : La réglementation autour de l'intégrité des données -

Le règlement des Dispositifs Médicaux/Dispositifs In V », cette dernière demande que les DM et leur production correspondent à l'état de l'art actuel. Pour définir cet état de l'art et donc les éléments sur lesquels se baser pour l'évaluation, les organismes notifiés utilisent les recommandations de l'ANSM et de l'EMA, les documents d'orientation des organismes notifiés dont ceux de GMED et les normes ISO.

Pour le maintien de la cybersécurité des DMIL [30], l'ANSM recommande d'enregistrer une trace des accès au dispositif et de chaque événement sous forme d'une fonction de journalisation locale. L'utilisation d'un outil de suivi permet ainsi de contrôler à posteriori tout ce qui s'est passé sur le dispositif et pouvoir mener des investigations le cas échéant. Le journal de suivi permet de détecter à posteriori les atteintes potentielles à la cybersécurité du dispositif. Dans ces recommandations, l'ANSM évoque qu'il faut notamment enregistrer les événements ayant un impact critique sur le fonctionnement du dispositif. Cela signifie qu'il est possible de mener une analyse de risque pour diminuer le nombre d'événement suivi. Ainsi, cela peut permettre la diminution de la quantité d'information enregistrée et d'accéder uniquement à des informations pertinentes lors d'investigation. Ces journaux sont considérés comme un bien à protéger dans les DM. Le fabricant doit s'assurer que la capacité de stockage est suffisante pour ne pas mettre en péril la sauvegarde des enregistrements des outils de suivi. L'ANSM recommande aussi d'établir le processus d'exploitation des journaux. Cependant ces recommandations ne détaillent pas dans quel but ces enregistrements doivent être exploités. De plus, l'ANSM recommande d'utiliser ces outils de suivi lors de la conception des DM disposant d'un logiciel pour permettre d'assurer l'intégrité du code source développé et de pouvoir réaliser la traçabilité de l'ensemble des modifications effectuées.

Dans ce même document sont présents des recommandations pour la gestion des accès dans un système informatique. Elles ont pour but de maintenir un niveau de cybersécurité satisfaisant :

- Définition claire des rôles et privilèges des acteurs/utilisateurs et des droits associés,
- Réduction au minimum des privilèges attribués aux utilisateurs,
- Organisation des droits possibles selon des rôles/profils,
- Limitation des accès aux fonctions sensibles pour la sécurité/la qualité du produit aux personnes habilitées,
- Authentification des utilisateurs sur la base de comptes nominatifs,
- Sécurisation de l'authentification : le mot de passe associé doit être robuste ou il est possible d'utiliser une authentification matérielle ou multi-facteur.

Les journaux de suivi permettent d'avoir la trace de l'ensemble des modifications apportés aux paramètres concernés par la gestion des accès ainsi que l'ensemble des actions effectuées pour chaque utilisateur. La revue de ce document permet de s'assurer que l'ensemble des actions effectuées correspondent aux processus en vigueur et qu'aucune falsification ou tentative de falsification n'a été effectuée.

L'EMA met à disposition des organismes notifiés un ensemble de recommandations pour mettre en application le nouveau règlement de façon efficace et harmonisé. Ces recommandations sont approuvées par le groupe de coordination des DM (MDCG) [40]. Un premier guide à propos de la qualification et de la classification des logiciels détaille comment déterminer si un logiciel ou une fonction de logiciel doit, ou non, appliqué la réglementation à l'aide d'un logigramme [41]. Un deuxième guide détaille les recommandations à appliquer pour la cybersécurité des DM [42]. La stratégie principale à mettre en place est celle de la maitrise du risque. Elle se base sur l'état de l'art actuel et sur la vérification et la validation des mesures de maitrise de risque. Ces mesures ne doivent ni être trop faible (exemple : un contrôle d'accès faible entraine un risque de modification malveillante) ni trop restrictive (exemple : un contrôle d'accès restreint risque d'empêcher l'accès en cas d'urgence médical). L'application de l'état de l'art doit être démontrée en justifiant les décisions sur la base des normes applicables, des recommandations, des informations scientifiques et des connaissances du fabricant. L'ensemble de ces éléments sont demandés dans la réglementation DM/DIV. Les sections détaillant ces éléments ont été regroupés dans la Figure 12, ainsi que la méthodologie a appliqué.

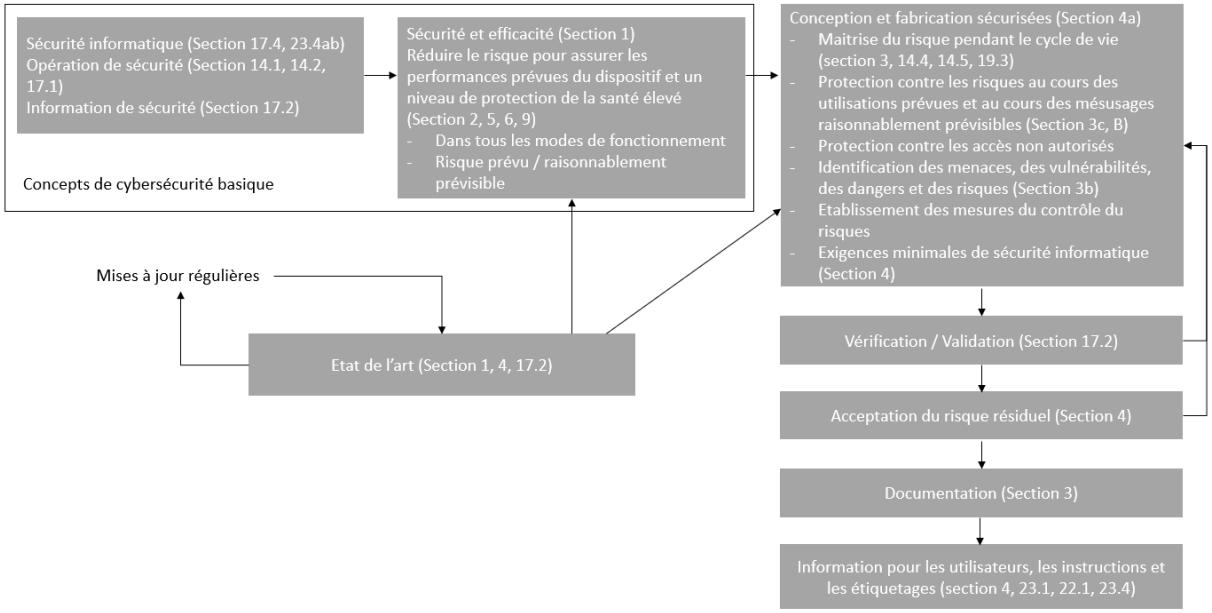


Figure 12 Représentation des exigences de sécurité et de performances contenues dans l'Annexe 1 du règlement DM/DIV 2017/745, illustration traduite du Medical Device Coordination Group Document "Guidance on Cybersecurity for medical devices" 2019-16 [42]

Selon ce document, pour assurer la cybersécurité des DM, il faut assurer trois éléments clés : la confidentialité des informations, l'intégrité des données (leur authenticité, leur exactitude) et la disponibilité des données, des processus, des dispositifs et des systèmes connectées. Pour cela, différentes mesures sont proposées comme la gestion des accès, la formation des utilisateurs sur les bonnes pratiques à adopter, valider les systèmes, avoir un processus de maitrise des changements, la mise en place d'un outil de suivi, etc.

Ce document met aussi en avant la méthodologie complète, détaillée dans la Figure 13, que la réglementation propose d'utiliser. Cette méthodologie correspond à celle de l'ICH Q9 « Gestion du risque qualité ». Les grandes étapes pour ce processus selon ce document sont :

- La planification de la gestion de risque,
- L'évaluation des risques,
- La maitrise des risques,
- Le risque résiduel,
- L'examen de la gestion des risques,
- La surveillance et vigilance après la mise sur le marché.

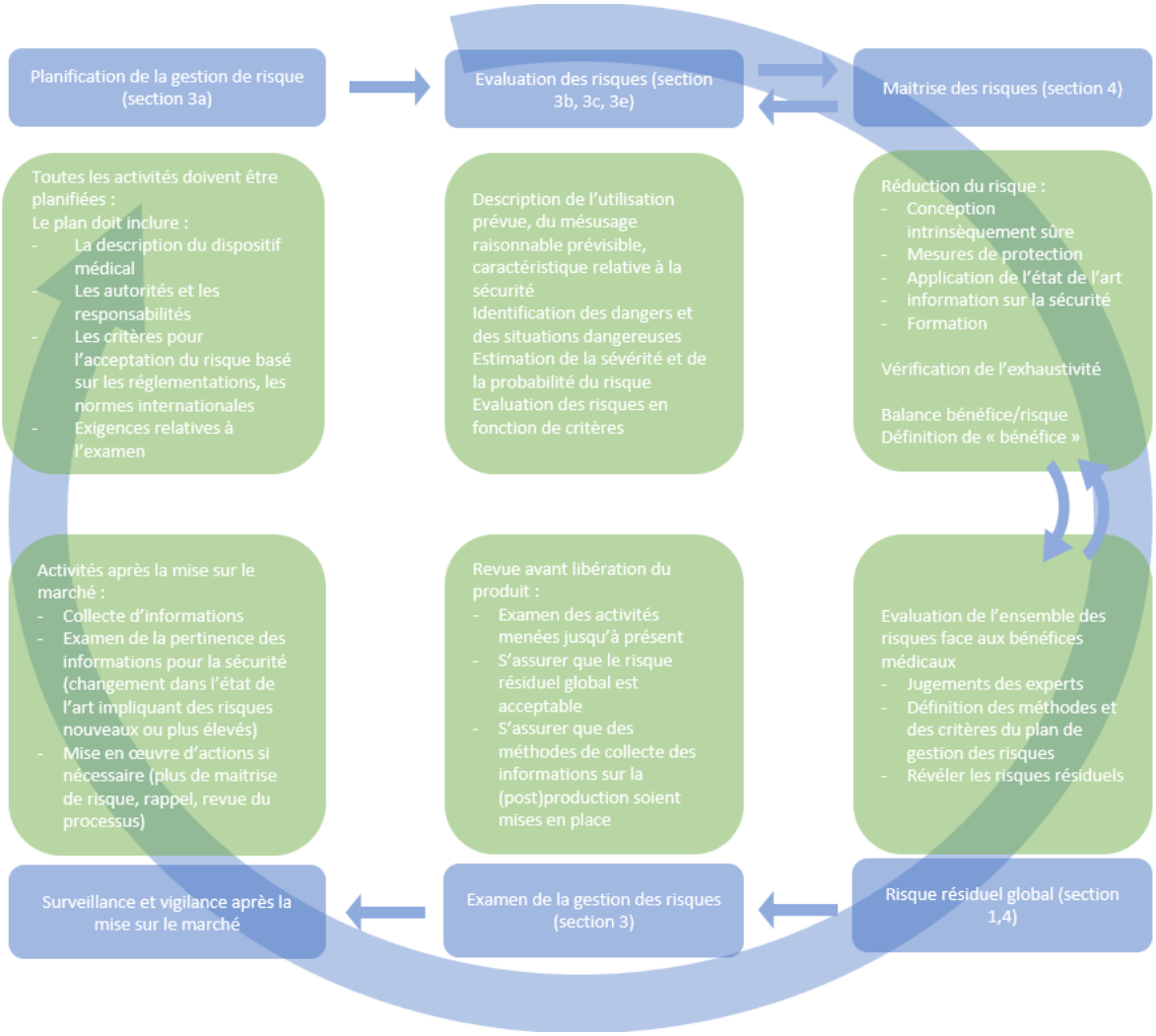


Figure 13 Flux d'informations pour la gestion des risques pour les dispositifs médicaux, illustration traduite du Medical Device Coordination Group Document "Guidance on Cybersecurity for medical devices" 2019-16 [42]

L'utilisation d'un outil de suivi assure la capacité à déterminer de manière fiable qui a apporté quelles modifications au système et à quel moment. Si nécessaire, cet outil permet de faciliter l'analyse en cas d'investigation.

Les normes

Dans les différentes normes développées précédemment, les outils de suivi sont régulièrement mentionnés mais leur exploitation est rarement développée. Cependant dans la norme EN NF IEC 62443-4-2 : « Sécurité des systèmes d'automatisation et de commande industrielles, exigences de sécurité techniques des composants IACS (Système d'Automatisation et de Commande Industrielles) » [43], ce sujet est plus détaillé. Cette norme s'adresse aux propriétaires, aux intégrateurs et aux fournisseurs des systèmes d'automatisation et de commande industrielles, ainsi qu'aux organismes de réglementation.

Selon cette norme, il existe sept exigences fondamentales pour définir le niveau de capacité de sécurité des systèmes. Ces exigences sont les suivantes :

- Contrôle de l'identification et l'authentification des utilisateurs,
- Contrôle de l'utilisation,
- Intégrité du système,
- Confidentialité des données,
- Transfert des données limitées,
- Réponse appropriée aux événements,
- Disponibilité des ressources.

Pour chacune de ces exigences, 4 niveaux de sécurisation sont définis avec des moyens de sécurisation correspondants.

Pour l'exigence « Contrôle d'utilisation », le système doit avoir une gestion des accès pour exécuter des actions demandées et une surveillance de l'utilisation de ces droits d'accès. Il y a quatre niveaux de sécurisation possible. Le niveau le plus faible correspond à une « *protection contre les mauvaises utilisations fortuites ou occasionnelles* ». Le quatrième niveau de sécurité, le plus important, correspond à une « *protection contre les contournements par des entités utilisant des moyens sophistiqués avec des ressources étendues, des compétences spécifiques au système et une motivation élevée.* ». Un des moyens de sécurisation préconisé par cette norme, pour chaque niveau de sécurisation, correspond à l'utilisation d'un outil de suivi permettant de générer des enregistrements des événements en rapport avec le contrôle des accès, les erreurs de demande, le système de commande, les sauvegardes et restaurations, la configuration et l'outil de suivi lui-même.

Pour chaque événement enregistré par cet outil de suivi, la norme demande qu'il y ait l'ensemble des éléments suivants :

- L'horodatage,
- La source (appareil d'origine, processus logiciel ou compte d'utilisateur),
- La catégorie,
- Le type,
- L'identification de l'événement,
- Le résultat de l'événement.

Pour ces enregistrements, la norme exige que les composants aient une capacité de stockage suffisante pour les conserver pendant la durée exigée par les politiques et les règlements applicables. De plus, il doit y avoir des mécanismes de protection lorsque la limite de capacité de stockage est atteinte ou dépassée. Dans ce cas, il y a un risque pour l'intégrité des données car les données enregistrées peuvent être écrasées ou modifiées. Pour cela, il est possible de mettre en place un avertissement lorsque le seuil de capacité de stockage est atteint. En cas de défaillances des mécanismes de capture et de traitement des enregistrements de suivi, la norme demande que des réponses adaptées soient mises en place. Il est donc nécessaire d'appliquer un processus de maitrise des risques et d'élaborer un plan de continuité des activités.

Pour répondre à l'exigence « intégrité du système », il est nécessaire d'avoir une protection contre les manipulations ou les modifications non autorisées tout au long de son cycle de vie. Il y a quatre niveaux de sécurisation possibles. Le premier niveau, le plus faible, correspond à une protection de l'intégrité du système « *face aux manipulations fortuites ou occasionnelles* ». Le quatrième niveau, le plus important, correspond à une protection de l'intégrité du système « *contre toute manipulation par des personnes utilisant des moyens sophistiqués avec des ressources étendues, des compétences spécifiques et une motivation élevée* ». Un des moyens de sécurisation est le contrôle de l'intégrité, de la configuration et de toute autre information pertinente. L'ensemble des contrôles des informations enregistrées via un outil de suivi sont réalisés pour détecter les potentiels manipulations frauduleuse effectuées. Ces contrôles doivent être enregistrés et consignés. Il est possible d'automatiser ces vérifications, mais un système d'alerte doit être présent pour avertir les utilisateurs le cas échéant. De plus, il est nécessaire que les informations enregistrées via un outil de suivi soient protégées contre les accès, les modifications et les suppressions non autorisés.

Pour répondre à l'exigence « Réponse appropriée aux événements », il est nécessaire de pouvoir recueillir les preuves des événements c'est-à-dire, ici, les violations de la sécurité, ainsi que les actions correctives réalisées en réponse à ces incidents. Il y a quatre niveaux de sécurisation. Pour le premier niveau, le plus faible, il faut « s*urveiller le fonctionnement des composants du système et répondre aux incidents détectés en rassemblant et en apportant les preuves demandées* ». Pour le quatrième niveau, le plus important, il faut « *surveiller le fonctionnement des composants du système et répondre aux incidents détectés en rassemblant activement les preuves et les transmettant aux autorités compétentes* ». Les outils de suivi sont des outils appropriés pour rassembler l'ensemble des preuves mentionnées. Selon la norme, il convient que ces outils n'aient pas d'impact négatif sur les performances opérationnelles du système et qu'ils permettent de rassembler, consigner, préserver et corréler automatiquement les preuves. Ces enregistrements doivent être accessible en lecture seule aux personnes autorisées, le but est de pouvoir mener des investigations sans mettre en péril l'intégrité des données. De plus, il est possible de suivre les connexions et les déconnexions réussies et non valides. Ainsi, si une personne non autorisée tente d'accéder aux systèmes, il est possible de mettre en place une notification de tentative de violation. Ces notifications doivent être consignées et peuvent être contrôlée. C'est un moyen complémentaire de sécurisation.

Les outils de suivi sont aussi utilisés dans le cadre du processus de gestion des changements. Comme indiqué dans les BPF, ce processus est une approche systématique pour proposer, évaluer, approuver, mettre en œuvre et réviser les changements [3]. Le journal de suivi, dans ce processus, permet de fournir une preuve nécessaire à la traçabilité liée à la mise en œuvre de ce changement. Il peut aussi être utilisé, après analyse spécifique pour fournir des indicateurs pour la révision des changements.

Exemple des systèmes informatiques de santé et des essais cliniques

L'implémentation et l'utilisation des outils de suivi sont particulièrement important dans les essais cliniques et dans les outils utilisant des données liées aux patients pour pouvoir, assurer la confidentialité, et l'exploitation des données [44]. Pour la confidentialité, l'outil de suivi permet de documenter l'identité de chaque utilisateur ayant accédé aux données. Pour l'exploitation des données, l'outil de suivi permet de documenter chacune des actions réalisées. Ainsi, les données brutes sont conservées et il est possible de justifier chaque traitement réalisé. Pour pouvoir assurer l'intégrité de ces informations, il doit y avoir une configuration pertinente et à jour, des droits d'accès et de ce qui est suivi par l'outil de traçabilité.

Dans le cadre d'un essai clinique, une donnée peut être interprétée et utilisée de diverses manières [45]. L'outil de suivi permet de tracer les éléments de synthèse, d'interprétation et d'utilisation de chaque donnée. Cet outil permet de faciliter la revue par les pairs et de mener des investigations si deux analyses différentes des mêmes données brutes ne donnent pas les mêmes résultats. Il faut alors s'assurer que les enregistrements de l'outil de suivi soient conservés conjointement à la donnée brute pour ne pas dépouiller cette dernière de son contexte. Cet outil fournit des preuves documentaires permettant à des experts d'examiner et de vérifier le chemin suivi par le chercheur. Cela permet d'examiner le processus de l'étude et d'établir sa fiabilité. L'utilisation d'un outil de suivi permet de fournir des preuves de la rigueur de l'étude et de documenter les stratégies analytiques des chercheurs. C'est un moyen pour démontrer la qualité et la fiabilité d'une étude.

Dans le cadre d'un système de gestion d'un réseau d'informations des soins de santé, un outil de suivi peut être mis en place pour enregistrer l'ensemble des connexions et des actions de chaque utilisateur [46]. Un outil de recherche des enregistrements a été ajouté pour pouvoir retrouver les informations pertinentes rapidement. Cela permet de s'assurer de la confidentialité des données. Par exemple, il est possible d'interroger la base de données avec le nom d'un patient, pour avoir comme résultat l'ensemble des utilisateurs ayant accédés à son dossier ainsi que l'ensemble de l'historique des changements de données (ajout, modification et/ou suppression). De plus, il peut être ajouté une signature électronique, un élément de sécurité certifiant l'intégrité des données à un instant défini, pour l'archivage des enregistrements des outils de suivi.

La norme ISO 18308 : « Informatique de santé - Exigences relatives à une architecture de l'enregistrement électronique en matière de santé » [47] et la norme ISO 27789 : « Informatique de santé – Historique d'expertise des dossiers de santé informatisés » [48] et ses différentes parties donnent des pistes sur la mise en place et la gestion d'un outil de suivi pour les dossiers de santé informatisés. Selon cette dernière norme, un enregistrement doit être fait quand « *un utilisateur crée des informations personnelles de santé, qu'il les lit, qu'il les met à jour ou qu'il les archive par le biais du système* ». Aucune information personnelle ne doit être enregistrée avec l'outil de suivi pour assurer la confidentialité mais il peut contenir des liens menant aux informations correspondantes. La norme insiste sur le fait que ces enregistrements démontrent la conformité du respect de la confidentialité des données des patients mais ils ne sont pas suffisants pour évaluer l'exhaustivité d'un dossier de santé informatisé. Comme indiqué précédemment, il est essentiel d'avoir un système avec une gestion des accès adaptée pour pouvoir utiliser un outil de suivi à bon escient. Il faut que chaque utilisateur puisse s'identifier individuellement dans le système et qu'ils aient des droits limités selon leurs besoins professionnels et leurs formations. Il en est de même pour les enregistrements réalisés avec l'outil de suivi, personne ne doit pouvoir le modifier, et l'accès doit y être limité et défini en amont de l'utilisation. Pour chaque enregistrement réalisé avec l'outil de suivi, les éléments suivants doivent être identifiés :

- L'identité de chaque utilisateur accédant aux informations,
- Le rôle de ces utilisateurs (chaque rôle correspond à un profil ayant des droits définis connus et déterminés en amont par l'organisation en charge du système),
- Le dossier concerné par l'action,
- L'action réalisée sur les informations personnelles : lecture, création, modification, traitement, utilisation, archivage, suppression,
- L'horodatage de l'action (jour mois année, heure minute seconde + fuseau horaire).

Ces enregistrements sont à la disposition des patients. Ils peuvent demander à consulter cet historique pour connaitre les personnes ayant accédées à leurs informations personnelles pour leur permettre de déterminer si leurs directives concernant l'accès à leurs données, ont été respectées. De plus, la conservation de ces données doit être régit par une politique déterminée par l'organisation responsable de ce système. La durée de conservation doit être suffisante pour couvrir le cycle de vie des documents associées.

Pour protéger contre la falsification de ces enregistrements, le système doit être strictement contrôler. Pour cela, il faut :

- Sécuriser et protéger l'accès à ces enregistrements,
- Tracer l'ensemble des actions réaliser sur la configuration de l'outil de suivi (notamment la désactivation de ce système) avec les mêmes informations que pour les éléments précédents,
- Avoir la possibilité de produire des rapports de l'ensemble des activités.

Ces rapports produits par l'outil de suivi peuvent être utilisé pour repérer des tendances ou pour alimenter des indicateurs. Il peut permettre de détecter un nombre inhabituel d'échec de connexions pouvant s'apparenter à des tentatives frauduleuses d'introduction dans le système. Ces rapports peuvent être un outil d'amélioration continue du système en rapportant les échecs récurrents. Ils sont aussi utilisés lors des investigations liées à un incident patient. Dans ce cas, le rapport contient l'ensemble de l'historique des activités réalisées sur un dossier et permet de détecter les comportements anormaux et les falsifications de données, le cas échéant. A propos des outils de suivi, la partie cybersécurité de la norme « Informatique de santé » ajoute que « *si, sur la base de l'évaluation de la vulnérabilité, la piste d'audit doit être immuable, la commande doit être signée numériquement, et les informations relatives à la signature numérique sont également stockées* » [49]. Il faudra donc réaliser une analyse des risques sur le système pour déterminer la nécessité d'un outil de suivi non modifiable. Le cas échéant, les enregistrements issus de cet outil doivent être certifié par un utilisateur via une signature numérique. Les informations concernées par ces protections de la confidentialité et de l'intégrité dans les systèmes informatiques de santé sont :

- Les informations personnelles de santé,
- Les données pseudonymisées,
- Les données statistiques de recherche,
- Les connaissances cliniques/médicales pouvant aider à la prise de décision clinique,
- Les données sur l'ensemble du personnel de santé,
- Les informations liées à la surveillance de la santé publique,
- Les données des systèmes de traçabilité produites par les systèmes d'information de santé comprenant des informations correspondant à cette liste,
- Les données de sécurité pour les systèmes d'information de santé (gestion des accès, configuration).

Dans cette partie de la norme est ajouté sur les outils de suivi, que les systèmes de messagerie utilisé pour transmettre des informations personnelles de santé garde la trace de tout ce qui a été émis. Les mêmes conditions de conservation et d'exploitation s'applique sur ces données que pour les autres enregistrements issus de l'outil de suivi. Cet outil permet de détecter les mauvais usages des systèmes et les enregistrements peuvent être utilisé dans des enquêtes réalisées par des experts médico-légaux, pour des fautes professionnelles médicales ou dans d'autres procédures judiciaires. Le degré de sécurisation des données de l'outil de suivi doit être au moins équivalent à celui des données sous-jacente et/ou des activités suivies. Une validation de l'outil de suivi est nécessaire pour garantir que l'ensemble des actions sont enregistrées, avec le niveau de détail suffisant pour la constitution des preuves. Si le système d'information est partagé entre différents ordinateurs, un service de synchronisation du temps doit être fournit afin d'aider au suivi et à la reconstitution de la chronologie de certaines activités. La revue des enregistrements issus de l'outil de suivi est mentionnée dans la Partie 1 « Vue d'ensemble et gestion des politiques » de la norme « Informatique de santé » [50]. Cependant les conditions de revue à appliquer ne sont pas développées.

III. Les référentiels

Dans les réglementations et les normes détaillées précédemment, les attentes à propos de la revue des enregistrements des outils de suivi sont abordées. L'ensemble des référentiels suivants proposent des méthodologies à adopter :

- PIC/S Guideline : « Good Practices for Data Management and Integrity in Regulated GMP/GDP environnements » (Draft) November 2018 [11],
- ISPE GAMP Guide : « Records and Data Integrity » – 2017 [13],
- ISPE GAMP Guide : « Data Integrity by design » – 2020 [14].

Comme pour les réglementations, selon les référentiels, les éléments attendus pour chaque création, modification ou suppression d'une donnée sont les suivants :

- Identité de la personne réalisant l'action,
- Détail de l'action, comme la nouvelle et l'ancienne valeur pour une modification,
- Date et lieu de l'action,
- Justification de l'action.

Selon le guide de l'ISPE GAMP : « Records and Data Integrity », il y a 3 principaux types de revues des enregistrements réalisés avec un outil de suivi :

- Revue en routine qui concerne les données opérationnelles,
- Revue pour la vérification périodique qui concerne la fonctionnalité de l'outil de suivi et de sa configuration au cours de la période concernée,
- Revue pour l'investigation qui concerne l'ensemble des données, selon les besoins.

En routine, un ensemble de données définies par les organisations sont revues pour permettre la certification et la libération des lots. Ces données ont un impact direct sur la prise des décisions pour la qualité du produit ou la sécurité du patient. La FDA et le référentiel précédent propose que l'ensemble des métadonnées associées à ces données définies doivent être revues conjointement. Ainsi cela concerne les enregistrements des outils de suivi. Cette vérification permet de s'assurer que l'ensemble des données sont intègres. Dans cette revue, il est vérifié qu'aucune donnée n'est supprimée, que les créations et les modifications sont réalisées par des personnes autorisée. De plus, ce référentiel conseille d'éviter les revues non ciblées pour optimiser les ressources mobilisées. Cette revue réalisée en routine est aussi appelée revue lot par lot.

La vérification périodique consiste à vérifier périodiquement un ensemble d'éléments pour un système. La périodicité est définie par la politique organisationnelle de l'entreprise. La périodicité sera plus régulière pour un système dit « critique » que pour un système avec une criticité faible. Ce classement est réalisé grâce à une analyse de risque ou selon des critères définis dans cette même politique organisationnelle. Les éléments à vérifier périodiquement sont déterminés de la même façon. Le référentiel de l'ISPE GAMP : « Records and Data Integrity » recommande de réaliser la revue de la configuration de la fonctionnalité de l'outil de suivi, ainsi que les événements associés, au cours de la période concernée. Selon ce référentiel, il est nécessaire de vérifier si le système limite les modifications et les suppressions possibles. Si le système ne permet pas ces actions, il n'est pas nécessaire de faire des revues périodiques ou lot par lot car l'intégrité des données n'est pas mise en cause. En revanche, il faut garder la fonctionnalité de l'outil de suivi car elle peut être utile en cas d'investigation. De plus, en fonction des systèmes, la configuration et l'activation de l'outil de suivi peuvent être modifiables. Il faudra, dans ce cas, vérifier périodiquement que la fonctionnalité n'a pas été modifiée ou désactivée. Les utilisateurs disposant des droits de modifications de cette configuration doivent être restreints pour limiter ce risque au maximum.

Pour les investigations, comme les réglementations, les référentiels proposent d'utiliser ces enregistrements comme preuves. Les revues, dans ce cas, sont exhaustives. En effet, il n'est pas pertinent d'appliquer une analyse de risque pour déterminer quelles données seront revues ou non. En cas d'investigation, aucune piste ne peut être éliminée avant d'être analysée. En revanche, dans certains cas, une analyse de risque est réalisée pour déterminer quelles fonctions sont tracées par l'outil de suivi. Lors de cette analyse, la possibilité d'une investigation doit être prise en compte pour assurer la récupération de l'ensemble des preuves nécessaires. De plus, les enregistrements des outils de suivi sont généralement des rapports lourds avec des éléments non nécessaires ce qui rend l'identification d'informations spécifiques difficiles. Il est nécessaire de bénéficier d'une fonction « recherche » ou « filtre » pour effectuer les revues et pour mener des investigations efficacement.

Avant de pouvoir exploiter cet outil, la fonction doit être validée. En effet, il faut s'assurer que les rapports générés répondent aux réglementations. Pour cela, l'ensemble des éléments suivants doivent être validés :

- Les rapports ne sont pas modifiables,
- Les rapports représentent l'ensemble des données nécessaires,
- L'heure associée ne peut pas être modifiée, elle doit être précise et sécurisée,
- La gestion des utilisateurs est conforme, un dossier de paramétrage permet de séparer efficacement les taches et assure la sécurité en fonction des rôles. La configuration de la gestion des accès est conforme aux droits de chacun.

De plus, une procédure doit être mise en place pour guider la détermination des données nécessaires dans l'outil de suivi et celles revues. Une instruction détaillée pour expliciter le mode d'exécution des revues en fonction des systèmes peut être utile. Cette instruction contient une explication type pas-à-pas pour accéder aux enregistrements de l'outil de suivi ainsi que le déroulement de la revue au complet. Ces processus sont détaillés pour l'exemple de la mise en place d'une revue périodique sur un système dans la Partie 3 : Présentation d'un cas concret de mise en place de la revue d'un outil de suivi.

Partie 3 : Présentation d'un cas concret de mise en place de la revue d'un outil de suivi

Contexte

Ce cas concret a été sélectionné dans une industrie pharmaceutique produisant des médicaments de formes sèches (comprimés, gélule, poudre). Le système choisit est utilisé dans le laboratoire de contrôle de la qualité. Ce dernier fournit des données essentielles à la libération des lots. Ce système permet de suivre les réactifs nécessaires aux contrôles, au niveau de leur volumétrie, et de leur péremption. L'ensemble des actions réalisables avec ce système informatique sont listés sur la Figure 14.

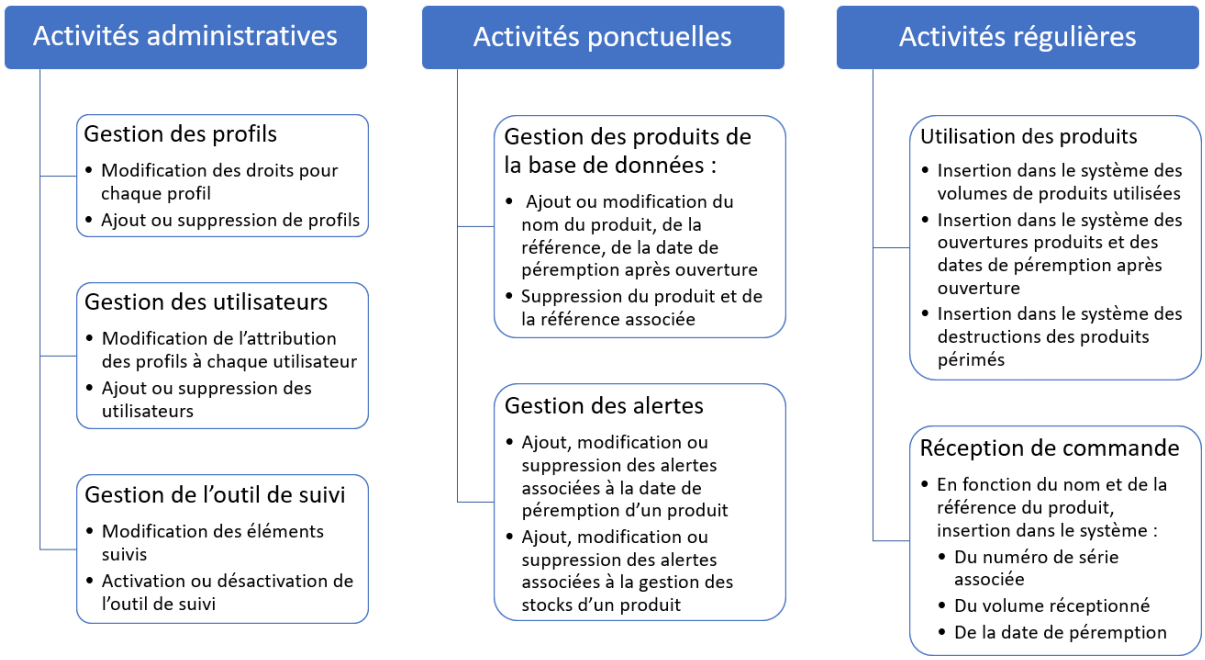


Figure 14 Liste des actions réalisables avec le système informatique de suivi des réactifs

Ce système est déjà validé et utilisé en routine au sein du laboratoire, cependant l'outil de suivi n'était pas exploité à son plein potentiel. Pour cela, un processus complet a été créé pouvant être appliqué à l'ensemble des systèmes de l'industrie existant et ainsi que pour les futurs systèmes. Ce nouveau processus a aussi impliqué le fait de mettre à jour d'autres documents telles que les critères des futurs cahiers des charges et les critères de validation périodique qui seront développés par la suite.

Pour des raisons de confidentialité, les informations présentes dans cette partie, sont inspirées de la réalité.

Conception et validation d'un système contenant un outil de suivi

L'implémentation d'un nouveau système est un projet à part entière pour lequel, comme indiqué dans la Figure 15, il faut commencer par l'élaboration d'un planning pour définir les éléments du projet (le temps et le personnel nécessaire, les objectifs principaux de ce projet). Pour déterminer le niveau requis de sécurisation, il faut déterminer si le système doit être soumis au BPF ou non, c'est-à-dire, si le système a un impact direct ou indirect sur la qualité du produit ou sur la sécurité du patient. Pour pouvoir rédiger le cahier des charges de ce système, il faut commencer par collecter l'ensemble des Spécifications des Besoins Utilisateurs (SBU) qui seront traduits en spécifications fonctionnelles puis en spécifications techniques et matériels en collaboration avec le fournisseur de la solution et l'entreprise. Ce cahier des charges doit contenir l'ensemble des éléments permettant d'assurer le niveau requis pour la sécurisation de l'intégrité des données demandé par la réglementation. Comme détaillé précédemment, ces fonctions de sécurisation peuvent être des fonctions de gestions des accès, d'outil de suivi, de sauvegardes et de restaurations, de signature électronique, etc. Après la définition des spécifications, un protocole de validation doit être rédigé pour s'assurer que le système réponde à nos attentes, aux regards des SBU et des spécifications fonctionnelles. Chaque item du cahier des charges doit faire l'objet d'au moins une ligne dans le protocole de test. Ce protocole doit être approuvé avant d'être appliqué. Il sera déployé pendant les différentes phases de validation du système. La méthodologie de validation utilisé ici, est celle détaillé sous forme de diagramme en V, détaillée dans la Figure 155. Celle-ci est la plus couramment utilisé dans l'industrie pharmaceutique.

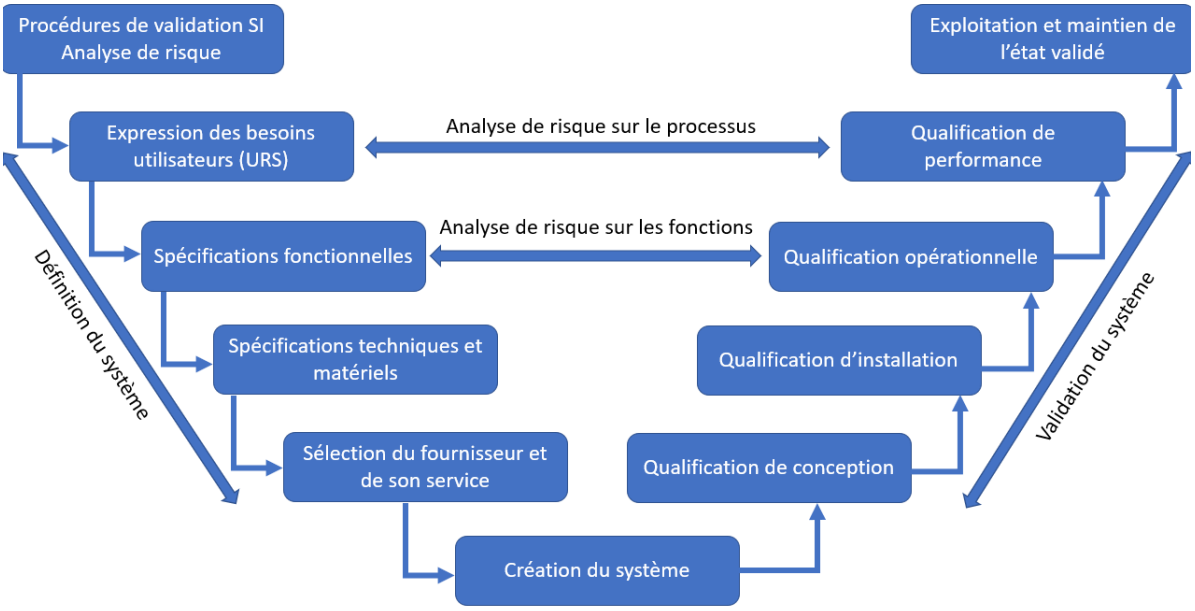


Figure 15 Etapes du cycle de vie d'un système sous forme de diagramme en V

Pour répondre à la réglementation et être en accord avec les référentiels, un système, soumis aux BPF, doit comprendre un outil de suivi dont chaque enregistrement sont composés à minima, de l'ensemble des informations suivantes :

- identité de l'utilisateur à l'origine de l'action,
- identification de l'action réalisée,
- horodatage de l'action,
- une justification de l'action le cas échéant.

Cette volonté est appuyée par la FDA, dans le paragraphe sur l'outil de suivi (« Audit trail ») du 21 CFR part 11 [9] et dans les deux questions/réponses associées, issues de la « FDA Questions and Answers session Data Integrity and Compliance with Drug CGMP » [18].

A la suite de l'appel d'offre, il faudra choisir le système le plus adapté aux critères définis. Les systèmes peuvent être de différents types, il peut être peu configurable, très configurable voire fait sur mesure. Cela correspond à l'étape de « Création du système » indiqué dans la Figure 15. Pour l'outil de suivi, l'étape de configuration consiste à décider quelles activités seront suivies par l'outil. Pour cela, il faut réaliser une première analyse de risque dans laquelle il faut prendre en compte les pires scénarios possibles (« worst case scenario ») pour chaque action possible. Comme expliqué précédemment, la gravité de ce scénario doit prendre en compte l'impact de l'action sur la qualité du produit, sur la sécurité du patient et /ou sur l'intégrité des données. Un des moyens de mitigation est l'utilisation d'un outil de suivi pour tracer l'ensemble des actions et la revue périodique de ces enregistrements. L'analyse de

risque permet de définir quelles actions du système doivent être tracées par l'outil de suivi et ainsi la configuration à adopter. Une fois la configuration réalisée, vient l'étape de validation du système. Cela correspond à l'exécution des scripts de tests rédigés. Lors de cette validation, il faut s'assurer :

- pour chaque activité, que l'outil de suivi trace l'ensemble des éléments demandées,
- qu'il n'est pas possible de modifier ou supprimer tout ou partie de l'enregistrement de l'outil de suivi,
- que la configuration de l'outil de suivi n'est modifiable que par les personnes autorisées.

Quand la validation du système est conforme et approuvée, le projet se clôture par une phase de compte rendu. C'est un rapport rédigé à l'issu du projet pour s'assurer que l'ensemble des objectifs définis dans la phase de planification sont atteints. Enfin, le système est prêt à l'utilisation en routine.

Dans le cas présenté ici, un exemple de cahier des charges est disponible dans l'Annexe 2. Ce cahier des charges reprend les objectifs du système, les éléments généraux nécessaires à son bon fonctionnement au sein de l'entreprise ainsi que l'ensemble des fonctionnalités nécessaire à son utilisation. Ici, une des fonctionnalités nécessaires est d'avoir un interfaçage avec le serveur de l'entreprise pour avoir le même horodatage que l'ensemble des autres systèmes. Le cahier des charges contient les descriptions des fonctionnalités nécessaires pour la gestion des profils, des utilisateurs, des profils, de l'outil de suivi, des alertes, et des produits. Lors de la qualification du système, chaque élément présent dans le cahier des charges est testé. Par exemple, les éléments nécessaires, dans le cahier des charges, pour la gestion de l'outil de suivi sont :

- « Avec le profil adéquate, il est possible de modifier les éléments suivis.
- La désactivation de l'outil de suivi est impossible.
- Chaque ajout, modification, suppression, archivage, actions sont suivi par cet outil.
- Les actions tracées par l'outil de suivi doivent contenir : l'identité de l'utilisateur, le/s profil/s accordé/s à l'utilisateur, l'action réalisée, les éléments présents avant l'action et les éléments présents après l'action, l'horodatage, la justification. »

Pour qualifier ces éléments, il faut :

- modifier les éléments suivis avec un profil n'ayant pas les droits et vérifier qu'il n'est pas possible de réaliser cette action. Modifier les éléments suivis avec un profil ayant les droits et vérifier qu'il est possible d'effectuer cette action.
- désactiver l'outil de suivi et vérifier que ce n'est pas possible d'effectuer cette action.

- effectuer un exemplaire de chaque action possible et vérifier l'enregistrement dans l'outil de suivi.
- pour chaque action tracée, vérifier que l'ensemble des informations sont présentes.

Exploitation de l'outil de suivi

Comme détaillé par le référentiel ISPE GAMP Guide : « Records and Data Integrity », les enregistrements issus des outils de suivi sont utilisés lors d'investigation, en routine et périodiquement [13]. A ces différents moments, ils sont revus et vérifiés soient exhaustivement soit de façon ciblée. Le but de ces revues est d'identifier les problèmes potentiels qui peuvent entraîner une perte de l'intégrité des données :

- la saisie erronée de données,
- les modifications par des personnes non autorisées,
- les données saisies extemporanément,
- la falsification de données.

Le processus mis en place pour ces revues est représenté sous la forme d'un diagramme FIPEC (Fournisseurs, Intrants, Processus, Extrants, Clients) présent sur la Figure 16. Les fournisseurs correspondent à « ceux qui fournissent la matière pour faire fonctionner le processus », c'est-à-dire les propriétaires du système de suivi informatisé soumis aux BPF. Dans notre cas, les fournisseurs sont :

- le laboratoire de contrôle qualité, ce service fournit la demande de revue sur son système de suivi des réactifs. Il fournit aussi l'ensemble des connaissances du système (expert système) et de l'environnement d'utilisation du système (expert métier).
- l'assurance qualité, ce service fournit les outils et la méthodologie nécessaire à la mise en place des revues.

Les intrants correspondent aux informations et/ou aux événements provoquant le besoin du déploiement du processus. Les intrants peuvent être :

- implémentation d'un nouveau système validé,
- changement impliquant le système validé et le suivi des modifications,
- implémentation d'une nouvelle version d'un système validé,
- mise à niveau d'un système validé existant. Ce dernier est l'intrant de notre cas concret.

Figure 16 FIPEC pour la revue des outils de suivi

Le processus de réalisation correspond à l'analyse de risque (Figure 15). Sa méthodologie est celle décrite dans l'ICH Q9 [3] dans la Partie 2 : La gestion de l'intégrité des données et les outils de suivi des activités : la réglementation, leurs spécificités et leurs contraintes. Cette analyse de risque permet de définir les éléments à suivre et donc la configuration de la fonction outil de suivi, les éléments à revoir et la périodicité de revue de l'ensemble de ces éléments. La périodicité peut être lot par lot, à fréquence définie ou uniquement en cas d'investigation. L'ensemble de ces éléments définit sont le résultat de l'application du processus, ils correspondent aux extrants. Pour finir, les clients, c'est-à-dire ceux pour qui est réalisé ce processus, sont :

- le service qui utilise ce système dit « BPF », ici, le laboratoire de contrôle de la qualité pour assurer l'intégrité des données fournit par leur système,
- les autorités de santé. Ce processus est nécessaire pour répondre à leurs exigences pour assurer la sécurité du patient et la qualité des produits.

Comme détaillé dans le FIPEC en Figure 16, le processus de réalisation commence par la formation d'un groupe pluridisciplinaire composé d'expert métier, système et des représentants de l'assurance qualité. Ces personnes vont mener ensemble l'analyse de risque et l'ensemble des prises de décisions. Ce processus de maitrise des risques commence par la définition des scénarios à risques. Pour chaque fonction d'un système informatique qui génère des données et qui influence la génération de ces données, il faut déterminer le ou les scénarios les plus à risques qui peuvent apparaitre lors de la création, modification ou

suppression de données. Cette étape est l'étape 2 « Définition des scénarios à risques » et correspond aux 3 premières colonnes du Tableau 5.

Tableau 5 Tableau récapitulatif de l'analyse de risques pour les revues d'outil de suivi

Etape 2 : Définition des scénarios à risque			*Etape 3 : Définition de la classe du risque*					*Etape 4 : Définition des mesures de mitigation hors revue de l' outil de suivi*	*Etape 5 : Définition des éléments présents dans la revue, du type et de la fréquence de revue*	
			Evaluation du risque						Gestion du risque restant	
Référence du risque	Fonction du système	Scénario à risque	Gravité	Probabilité d' occurrence	Classe de risque	Probabilité de détection	Priorité du risque	Mesure de mitigation	Risque résiduel	Actions
			Elevé/ Moyen / Faible	Elevé/ Moyen/ Faible	Elevé/ Moyen/ Faible	Elevé/ Moyen/ Faible	Elevé/ Moyen/ Faible		Elevé/ Moyen/ Faible	
2 Gestion des paramètres										
2.01	Création, modification des profils de droits	Insertion d' un mauvais paramétrage Risque : Accorder des droits à une personne non habilitée	Moyen	Moyen	Moyen	Faible	Elevé	Limiter la modification de ces paramètres à des personnes autorisées dans le système →Diminution de la probabilité d' occurrence	Moyen	Vérification périodique de l' outil de suivi : vérifier que les actions ont été réalisées par des utilisateurs ayant les droits, et que chaque action est conforme. Périodicité fixée à 3 mois pour un risque résiduel moyen. →Augmentation de la probabilité de détection
2.02	Suppression de profils de droits	Suppression fortuite de profils de droits Risque : Perte de l' historique des actions liés à cet utilisateur	Moyen	Moyen	Moyen	Moyen	Moyen	L' action de « suppression » est impossible dans le système. Il n' existe que la fonction « Archivage ». →Diminution de la probabilité d' occurrence	Faible	

Chaque scénario est ensuite évalué en fonction de sa gravité et de sa probabilité d'occurrence pour définir la classe du risque. Cette classe du risque peut être définit selon le Tableau 3 Tableau d'évaluation de la classe du risque en fonction de la gravité et de la probabilité d'occurrence de ce risque traduit de l'ISPE GAMP 5 : « A Risk Based Approach to compliant GxP computerized systems ». Puis la classe de risque et l'évaluation de la probabilité de détection servent à définir la priorité du risque. Elle peut être classée selon le Tableau 4 Tableau d'évaluation de la priorité du risque en fonction de la classe du risque et de la probabilité de détection de ce risque traduit de l'ISPE GAMP 5 : « A Risk Based Approach to compliant GxP computerized systems ». Dans notre cas, les critères pour définir la gravité, la probabilité d'occurrence et la probabilité de détection sont présents dans le Tableau 6 suivant.

Tableau 6 Définition générale des critères pour la gravité, la probabilité d'occurrence et la probabilité de détection

	Faible	Moyen	Elevé
Gravité	Sans impact sur la sécurité du patient et/ou la qualité du produit	Impact indirect sur la sécurité du patient et/ou la qualité du produit	Impact direct sur la sécurité du patient et/ou la qualité du produit
Probabilité d'occurrence	Il est très peu probable que ce scénario se réalise	Ce scénario peut se réaliser	Ce scénario a de fortes probabilités de se réaliser
Probabilité de détection	La détection est fortuite	Un système de détection ponctuel est mis en place	Un système de détection automatique est mis en place

Pour chaque scénario, ces critères sont appliqués. Ceci est l'étape 3 « Définition de la classe du risque » correspondant aux colonnes pour l'évaluation du risque dans le Tableau 5. Un point d'attention doit être porté sur le fait de ne pas prendre en compte la revue des outils de suivi dans l'évaluation de la probabilité de détection car c'est ce qui sera définit grâce à ce processus.

En quatrième étape, pour les risques élevé ou moyen, des mesures de mitigation doivent être mises en place comme la configuration, ou la sécurisation par un autre moyen. Le risque est ensuite réévalué à la suite du déploiement de ces mesures. La revue de l'outil de suivi ne doit pas être utilisée comme un moyen de mitigation à ce stade.

Pour les risques résiduels élevé ou moyen, des revues de l'outil de suivi doivent être réalisés. Cette étape correspond à l'étape 5 présente dans le Tableau 5. Pour maitriser au mieux les risques, l'équipe pluridisciplinaire doit se mettre d'accord sur le type de revue à effectuer, la fréquence ainsi que les personnes en charge. L'ensemble de ces informations sont rassemblées dans le Tableau 5.

Le Tableau 5 contient deux exemples issus de l'Annexe 3. Ces exemples se rapportent à des activités administratives, et sur la gestion des paramètres. Pour la fonction du système « Création, modification des profils de droits », le scénario le plus à risque correspond à l'insertion de données erronées lors du paramétrage. Le risque associé est d'accorder des droits à une personne non habilitée. L'impact de ce risque est indirect sur la sécurité du patient et/ou la qualité du produit, la gravité est évaluée « moyenne ». La probabilité d'occurrence est évaluée « moyenne ». Ainsi, la classe de ce risque est « moyenne ». La probabilité de détection est évaluée « Faible » car en l'état, la découverte de ce paramétrage erroné serait fortuite. A l'issue de l'analyse, la priorité du risque de ce scénario est évaluée « élevée ». Une ou plusieurs mesures de mitigation sont nécessaire. L'équipe pluridisciplinaire a décidé de « limiter la modification de ces paramètres à des personnes autorisées dans le système ». Cette action permet d'évaluer la probabilité d'occurrence comme « faible » et de réduire la priorité du risque à « moyenne ». La mesure de mitigation n'est pas suffisante pour maitriser le risque résiduel, il est nécessaire de mettre en place une nouvelle action. Ici, il a été décidé de réaliser une « vérification périodique de l'outil de suivi : vérifier que les actions ont été réalisées et vérifiées par des utilisateurs ayant les droits, et que chaque action est conforme. » à une périodicité de 3 mois car le risque résiduel est « moyen ». Cette action permet l'augmentation de la probabilité de détection et ainsi de maitriser le risque.

Pour la fonction du système « Suppression de profils de droits », le scénario le plus à risque est la suppression fortuite de profils de droits. Le risque associé est de perdre l'ensemble de l'historique des actions liés à cet utilisateur. Comme pour le scénario précédent, la gravité, la probabilité d'occurrence et la classe de risque sont évaluées « moyennes ». En revanche, la probabilité de détection est évaluée « moyenne » car dans ce cas, les utilisateurs sont bloqués dans leurs actions s'ils n'ont plus les droits associés à un profil. Ainsi, l'alerte est donnée plus rapidement que dans le cas précédent. Ainsi la priorité du risque est « moyenne », ce qui nécessite une ou plusieurs mesures de mitigation. Pour ce scénario, le système rend impossible la suppression des profils, il n'est possible que d'archiver. Ceci diminue la probabilité d'occurrence à « faible » et permet de maitriser le risque de perte de données.

L'analyse de risque complète appliquée pour notre cas concret est présente dans l'Annexe 3 : Analyse de risque de l'utilisation du système de suivi des réactifs du laboratoire. A l'issu de cette analyse, sept éléments de l'outil de suivi sont à revoir lors d'une revue périodique :

- Création, modification des références de réactifs,
- Suppression des références de réactifs,
- À la suite de l'ouverture d'un produit, modification de la date de péremption,
- Gestion des alertes des produits bientôt à péremption,
- Création, modification des profils de droits,
- Création, modification des droits d'utilisateur,
- Création, modification et suppression des éléments suivi par l'outil de suivi.

La fréquence définie est de 3 mois. Cette fréquence a été choisie par l'équipe pluridisciplinaire pour réaliser un contrôle efficient de ces événements.

Une fois chaque revue réalisée, un rapport doit être rédigé et compléter par des preuves pour assurer la traçabilité nécessaire [27]. Le formulaire utilisé pour réaliser la revue périodique de notre exemple, est présent dans l'Annexe 4 : Formulaire pour la revue de l'outil de suivi du système de suivi des réactifs du laboratoire de contrôle qualité.

Validation périodique

La validation périodique d'un système est réalisée pour s'assurer que le système répond toujours à son cahier des charges et pour s'assurer qu'il ne dévie pas de ses spécifications. Ainsi, le rapport de revue périodique de validation du système permet d'assurer le maintien en condition opération vis-à-vis de la réglementation. La fréquence de revue de l'outil de suivi est généralement plus importante que la fréquence de la validation périodique du système. Ces deux périodicités sont déterminées en prenant en compte la criticité du système. L'ensemble des revues de l'outil de suivi ayant été effectué sur la période de la validation périodique du système sont regroupés. A ce moment-là, il y a une vérification que les revues de l'outil de suivi ont été faites selon ce qui a été déterminé (périodicité et éléments). De plus, il faut s'assurer qu'elles sont conformes à l'attendues, et que l'ensemble des événements indésirables détectées ont été pris en charge et tracés.

Procédure associée au déploiement de la revue de l'outil de suivi

Pour s'assurer que ce processus sera suivi de façon uniforme pour l'ensemble des systèmes de l'entreprise, une procédure a été rédigé. Elle suit les recommandations de la procédure dite « Corporate ». Cette dernière est à destination de l'ensemble des différents sites du groupe. Ces recommandations suivent les éléments présents dans les réglementations et les référentiels décrits précédemment. La procédure dite « Corporate » a été rédigé par un groupe de travail auquel j'ai participé pour la finaliser et pouvoir la rendre effective. Je suis intervenu plus particulièrement sur le déploiement de cette procédure sur un des sites français du groupe. La procédure du site français en question se concentre sur la détermination des revues périodiques, c'est-à-dire pour vérifier les données opérationnelles classiques et pour vérifier la fonctionnalité de l'outil de suivi si besoin. Elle contient :

- la description des outils de suivi,
- les définitions des différents types de revu possible, comme décrit par le GAMP 5,
- la composition du groupe pluridisciplinaire,
- le processus à réaliser comme indiqué dans le FIPEC Figure 16,
- le personnel en charge des revus.

Cette procédure ajoute que si un outil de suivi informatique ne peut pas être mis en place, une solution de remplacement doit être choisie. Cela peut consister en une sécurisation du système, une sécurisation par double contrôle ou via d'autres procédures. Il est aussi possible de mettre en place un log book papier. Cette solution reste risquée d'un point de vue de l'intégrité des données car ce n'est pas automatisé, les omissions sont donc fortement possibles.

Le personnel chargé de la revue doit recevoir une formation adéquate pour s'assurer qu'il ait une bonne compréhension du système. Il faut qu'il puisse mener des investigations et prendre des décisions si besoin. De plus, chaque utilisateur du système doit être sensibilisé sur le fait que l'usage de l'outil de suivi est réalisé et ce qu'il implique [49]. En effet, son but n'est pas de surveiller les faits et gestes des utilisateurs mais bien d'avoir l'ensemble des informations nécessaires pour pouvoir prendre des décisions neutres. Pour comprendre tous les enjeux liés à l'intégrité des données, le personnel doit être aussi formé et sensibilisé à ce sujet. En effet, il faut que chaque contributeur ait conscience du risque engendrée par une simple modification, une lacune d'information ou l'utilisation du compte d'un autre utilisateur que le sien. Le chapitre 2 « Personnel » des BPF insiste sur la formation de l'ensemble du personnel et que cette formation soit appropriée aux taches attribuées à chacun [3]. Chaque personne

en contact avec des données dites BPF doivent être sensibilisée à la maitrise de l'intégrité des données.

Amélioration continue

Pour chaque système, il est nécessaire de mettre en place des indicateurs pour le bon suivi de ces revues. Ces indicateurs permettent d'assurer le bon suivi et de mettre en place des actions préventives ou correctives rapidement si besoin. Ils peuvent couvrir différentes facettes des revues :

- La clôture dans les temps des revues,
- Le nombre d'erreur détecté par revue,
- La gravité des erreurs détecté par revue.

Si aucune erreur n'est détectée à plusieurs reprises, il peut être intéressant de revoir l'analyse de risque pour diminuer la fréquence car le risque semble maîtrisé. Dans le cas contraire, c'est-à-dire si des erreurs sont souvent détectées, la fréquence pourra être revue à la hausse car la maitrise du risque semble moins robuste. Ceci est détaillé dans une roue de Deming (PDCA : Plan, Do, Check, Act) illustrée par la Figure 177.

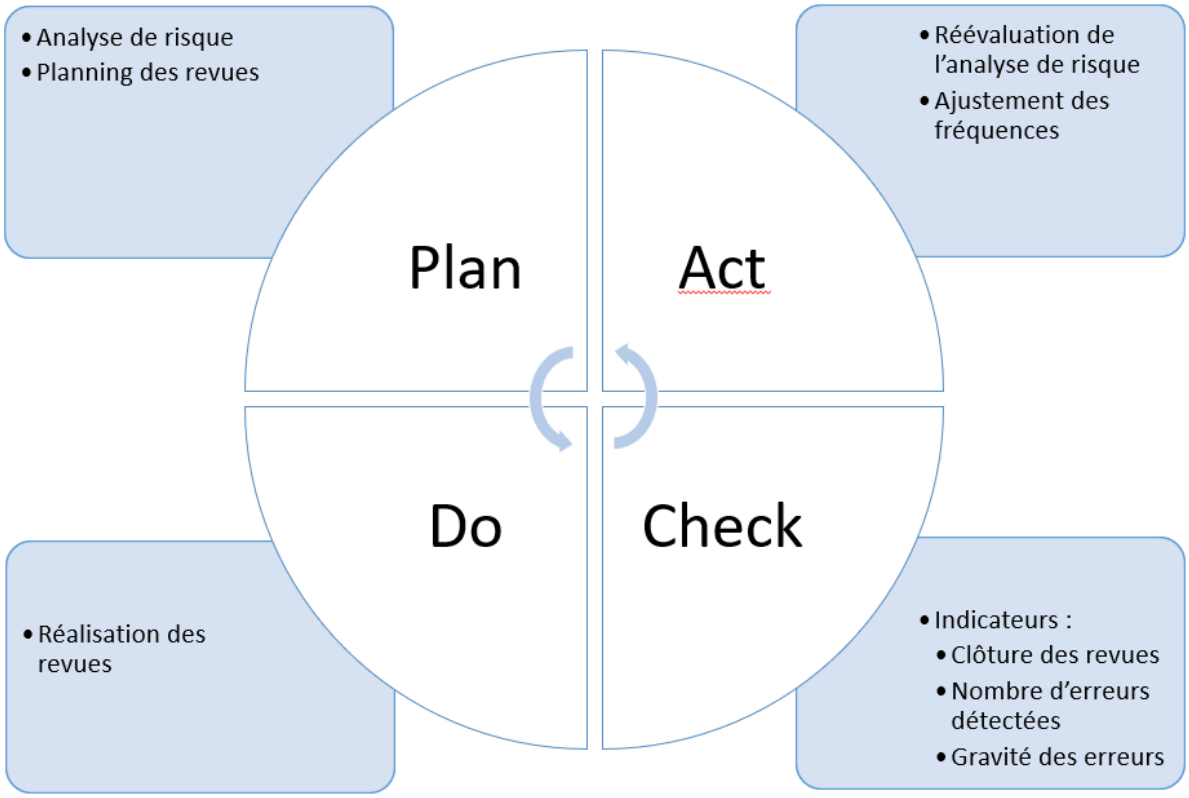


Figure 17 PDCA pour les revues des outils de suivi

La roue de Deming ou PDCA est un outil d'amélioration continue de la qualité. La première étape d'un PDCA est le « Plan », la partie planification. Ici, elle correspond à l'application du FIPEC détaillé en Figure 16. La deuxième étape, le « Do » correspond à la réalisation de ces revues en routine. La troisième étape est le « Check ». Elle correspond au suivi via des indicateurs pour détecter si des améliorations de notre processus sont à mettre en place. Cette dernière étape de mise en place de différentes améliorations, correspond au « Act ».

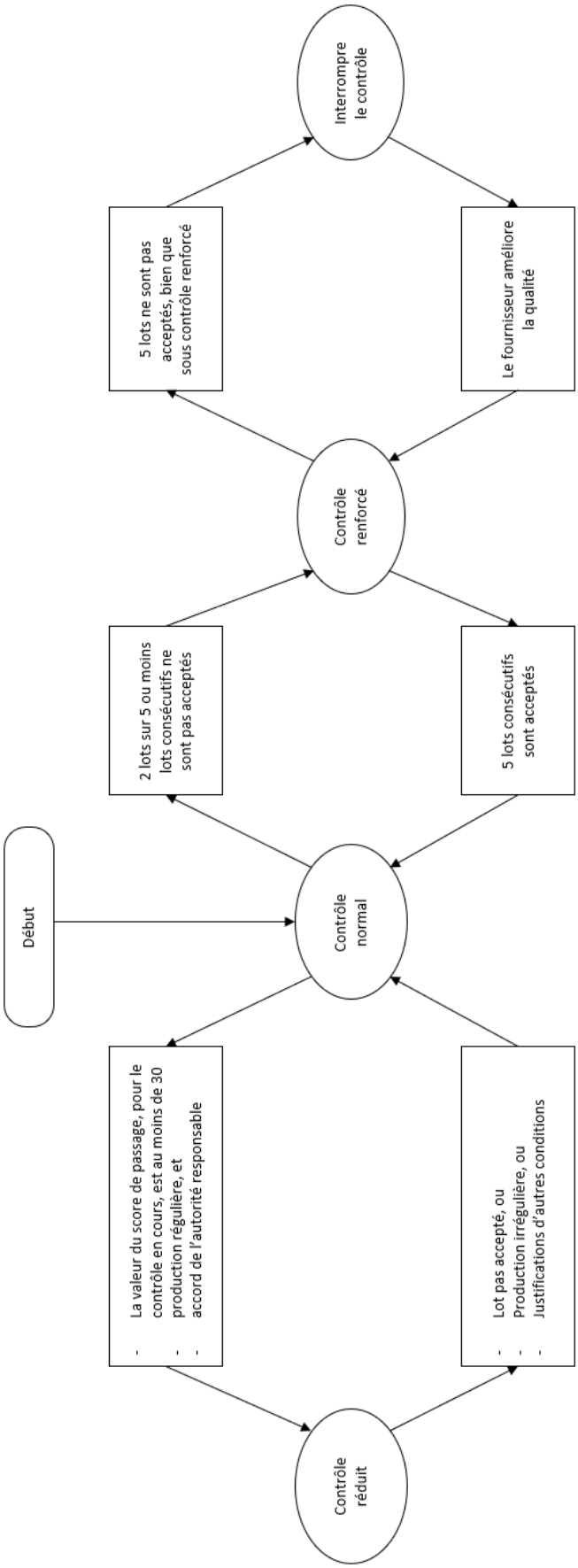


Figure 18 Schéma des règles de passage du contrôle issu de la norme ISO 2859 "Règles d'échantillonnage pour les contrôles par attributs" [51]

Pour cette dernière étape, il est possible d'adopter les règles de modification du contrôle issue de la norme ISO 2859 « Règles d'échantillonnage pour les contrôles par attributs » Partie 1 « Procédures d'échantillonnage pour les contrôles lot par lot, indexés d'après le niveau de qualité acceptable NQA » détaillée dans la Figure 188 [51]. Dans notre cas, un « lot » correspond à une revue de l'outil de suivi d'un système défini. Le contrôle normal est réalisé lors de la mise en place de ce processus. Si 2 revues consécutives sur 5 ne sont pas conformes, il est nécessaire de passer à un contrôle renforcé. Ensuite, si 5 revues ne sont pas conformes, le fournisseur, ici les personnes en charge de ce processus devront mettre en place des éléments de sécurisation ou revoir l'analyse de risque.

Dans le cadre de notre exemple du système informatique de gestion des réactifs, il existe la fonction « modification de la date de péremption à la suite de l'ouverture d'un produit ». Un des scénario à risque (1.10) est l'« insertion de données erronées : date de péremption postérieur à la date de péremption réelle » ayant pour risque l'utilisation d'un réactif périmé. Pour maitriser le risque, il a été décidé de :

- programmer automatiquement la date de péremption à la suite de l'ouverture,
- de réaliser une double vérification si l'insertion de la date est faite manuellement,
- de réaliser une vérification périodique de l'outil de suivi : vérifier que les actions ont été réalisées et vérifiées par des utilisateurs ayant les droits, et que chaque action est conforme. La périodicité de la vérification est fixée à 3 mois.

Si 2 revues consécutives sur 5 contiennent des erreurs détectées lors de la revue, le risque d'utiliser des réactifs périmés est trop important. Le risque résiduel évalué « moyen » est réévalué « élevé » car l'une des mesures de mitigation n'est pas suffisante. Dans notre, il est probable que la cause de ces erreurs soit l'insertion manuelle des dates de péremption et une mauvaise pratique lors de la double vérification. En l'absence d'une mesure de mitigation automatique efficace, la périodicité de la vérification de l'outil est fixée à 1 mois, ce qui correspond à un contrôle renforcé. Différentes mesures peuvent être prise pour diminuer le nombre d'erreur comme l'amélioration de la programmation automatique de la date de péremption. Si 5 revues périodiques sont réalisées conformes, la périodicité peut de nouveau être à 3 mois.

La revue par exception pour les revues en routine

Le déploiement d'un outil de revue par exception est une optimisation pour la revue des outils de suivi mais aussi des accès. Ce type d'outil est détaillé dans le Guide de l'ISPE GAMP : « Data

Integrity by design » [14]. C'est un système offrant des fonctionnalités, telles que des outils de rapports automatisés et des rapports d'alarme ou d'exception. Il est particulièrement adapté pour la revue des outils de suivi en lot par lot. En effet, cet outil permettrait de réduire les contrôles nécessaires à un réviseur humain tout en améliorant le taux global de détection des problèmes d'intégrité des données et des erreurs. La revue par exception est une approche plus efficace en matière d'examen des données [3]. Elle consiste à utiliser des ordinateurs et des logiciels pour un examen général de tous les résultats afin d'identifier les données suspectes. Ensuite, des personnes examinent en détails ces données signalées par le système afin de décider s'il existe un problème d'intégrité des données. Pour cela, il est nécessaire d'avoir :

- un système informatisé permettant de générer un rapport d'exception avec la possibilité de configurer les limites et les spécifications du rapport,
- une compréhension détaillée du produit et du processus alimentant une évaluation détaillée du risque d'intégrité des données afin d'identifier ce qui doit être automatiquement évalué dans un rapport d'exception,
- une vérification robuste de tout outil de rapport d'exception, y compris des tests de cas positifs et négatifs,
- une gestion de la configuration des limites et des spécifications du rapport d'exception.

Des exemples de systèmes de revue par exception utilisent un système de drapeau d'avertissement. Si aucun drapeau n'est présent, aucune revue n'est à réaliser, dans le cas inverse, une revue est à réaliser. Une fois la revue faite, les documents sont validés pour pouvoir passer à l'étape suivante [27].

Conclusion

Un outil de suivi, autrement appelé « Audit trail » est un outil permettant d'avoir une traçabilité complète et fiable. Pour chaque système et chaque activité définie, il permet de tracer l'ensemble des éléments suivants :

- Identité de l'utilisateur,
- Rôle de l'utilisateur dans le système,
- Identification de l'action réalisée,
- Horodatage de l'action,
- La justification de l'action. Cette dernière est facultative mais fortement conseillée.

Un outil de suivi permet de satisfaire plusieurs critères de l'ALCOA+ demandés par les réglementations :

- Il permet de rendre les données Attribuable,
- Il permet de garder la lisibilité pour les données brutes potentiellement modifiées,
- Il permet de garder associé un horodatage à chaque action. Cela assure le caractère contemporain de chaque activité,
- Il permet de s'assurer que les données brutes soient toujours Originale et Disponible,
- Comme l'ensemble des activités sont concernées par l'outil de suivi, l'enregistrement associé permet d'avoir des informations Cohérentes Complètes et Précises.

De plus, pour la mise en place des processus autour des outils de suivi, il est nécessaire d'utiliser le principe de gestion du risque, comme détaillé dans les BPF. Pour répondre à la réglementation et pour exploiter l'outil de suivi de façon efficiente, trois types de revues sont réalisés :

- Revue des données opérationnelles, dites « Lot par lot ». Cela correspond à la revue de l'ensemble des métadonnées associées aux données nécessaires pour la certification et la libération de chaque lot. Pour être efficient, il est possible de réaliser une revue par exception,
- Revue des données administratives. C'est une revue de l'ensemble des données définies par analyse de risque selon une périodicité définie,
- Revue des données lors d'une investigation. C'est une revue de l'ensemble des données pertinentes pour réaliser une enquête et trouver la cause d'une erreur.

Chaque revue a sa méthodologie propre qui doit être décrite dans des procédures et/ou des instructions. Les instructions sont propres à chaque système pour s'assurer que la

méthodologie appliquée soit la même selon les personnes qui l'exécutent. Pour compléter cela, la formation et la sensibilisation à la gestion de l'intégrité des données et à son intérêt sont essentielles. Elles permettent de s'assurer que chaque personne comprenne les enjeux de leurs activités et qu'ils puissent avoir l'ensemble des informations pour détecter des défaillances possibles dans les processus.

Les outils de suivi à l'heure de l'intelligence artificielle et des chaînes de blocs (*Blockchain*)

Les prochaines générations de systèmes pourraient intégrer l'apprentissage automatique pour faciliter la prise de décision. L'apprentissage automatique est une forme d'intelligence artificielle où le système informatique est dans la capacité d'améliorer ses performances en se basant sur l'analyse de jeux de données. La pharmacopée européenne a proposé une fiche pour l'utilisation d'apprentissage automatique et d'intelligence artificielle : « Méthodes chimiométriques appliquées aux données analytiques » [52]. Il est indiqué dans ce chapitre que la chimiométrie correspond à « *la discipline qui utilise des méthodes mathématiques et statistiques pour (a) concevoir ou sélectionner des procédures de mesure et des expériences optimales et (b) extraire des données analysées le maximum d'informations chimiques.* ». Il y est expliqué l'ensemble des étapes pour arriver à un système fonctionnel ainsi que les méthodes de validation nécessaire à l'utilisation d'un tel système. Selon la pharmacopée européenne, il y a un ensemble d'étapes « *généralement valable pour l'analyse d'ensemble de données non organisées :*

- *Définir l'objectif précis de la collecte de données et les résultats attendus de l'analyse, pour la formulation du problème ;*
- *Vérifier l'origine et la disponibilité des données. S'assurer que les données collectées couvrent le domaine de variation des variable(s) ou attribut(s) explorés ;*
- *Si les données disponibles ne couvrent pas le domaine de variation attendu, procéder à la préparation et à l'analyse d'échantillons permettant d'obtenir les données expérimentales requises ;*
- *Choisir soigneusement les variables, l'utilisation de variables pertinentes pouvant apporter davantage de robustesse au modèle et en améliorer l'exactitude ;*
- *Si nécessaire, appliquer aux données brutes des transformations et prétraitements mathématiques ;*
- *Elaborer le modèle, par étalonnage et validation ;*

- *Mettre le modèle à l'épreuve et en vérifier les performances sur de nouveaux échantillons ou données ;*
- *Valider la méthode conformément aux usages et exigences pharmaceutiques en vigueur*. »

Dans ce type de système, la traçabilité est essentielle. En effet, l'ensemble des données servant à élaborer le modèle de prise de décision doivent être connu. Il est essentiel de savoir si c'est un humain qui a pris la décision ou si c'est un système d'intelligence artificielle. De plus, si le système s'améliore en continue, il faut s'assurer qu'une traçabilité suffisante soit mise en œuvre. En effet, dans ce type d'apprentissage, il est possible que les tendances dérivent et que le système ne prenne plus les décisions qu'il devrait. Il est donc intéressant de tracer sur quoi se base l'intelligence artificielle pour prendre ses décisions. En cas d'investigation, si cette traçabilité est réalisée par un outil de suivi, il sera plus simple de connaitre la raison de l'écart constaté et de pouvoir établir quels produits sont impactés.

Ce type de système peut être complété par les technologies relatives aux chaines de blocs. Cette technologie est particulièrement développée dans le secteur financier [53]. La chaine de blocs permet de faciliter l'analyse des documents financiers et d'assurer la traçabilité de l'ensemble des transactions effectuées. Elle permet d'augmenter l'efficacité de la surveillance et l'auditabilité de l'ensemble des transactions. Le principe de chaine de blocs correspond à l'assemblage de plusieurs blocs où chaque bloc contient un ensemble des données sur un événement qui a été réalisé sur le produit [54].

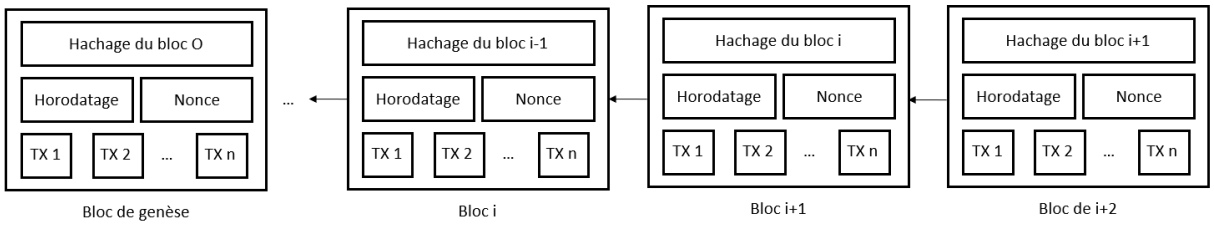


Figure 19 Exemple d'une chaine de blocs qui consiste en une séquence continue de blocs, traduit du document "Blockchain in audit trails - An investigation how blockchain can help auditors to implement audit trails" [53]

Comme indiqué dans l'illustration de la Figure 19, le premier bloc de la chaine est appelé « bloc de genèse » et tous les blocs précédents sont appelés « blocs parents » [53]. Chaque bloc est constitué d'une liste complète (TX n) des enregistrements de transactions, d'un horodatage, d'un nonce (clé de cryptographie) correspondant, ainsi que le hachage cryptographique du bloc parent. Cette suite de hachage permet de reconstituer l'historique complet, en créant une chaine de bloc, d'où le nom « Blockchain ». La chaine de blocs peut être comparé à un

grand livre public où il est possible de créer et de partager des informations numériques par et pour différents utilisateurs.

La Figure 20 illustre le processus de transactions utilisant la chaine de bloc [53]. Lorsqu'une transaction est effectuée par un employé d'une compagnie A, elle est validée par un employé d'une compagnie B. Cette transaction est ensuite transférée vers un réseau nodal qui valide la transaction. Un bloc est ensuite créé avec la transaction, l'horodatage, la clé de cryptographie et le hachage du précédent bloc pour l'ajouter à la chaine.

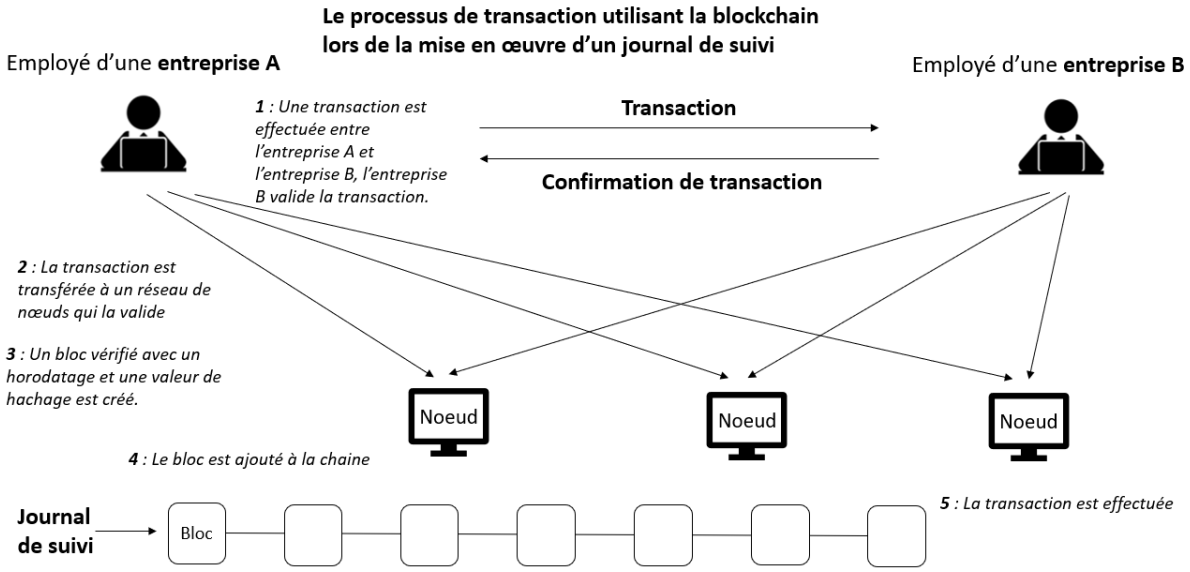


Figure 20 Illustration du processus de transaction utilisant la chaine de bloc lors de la mise en œuvre d'un outil de suivi, traduite du document "Blockchain in audit trails - An investigation how blockchain can help auditors to implement audit trails" [53]

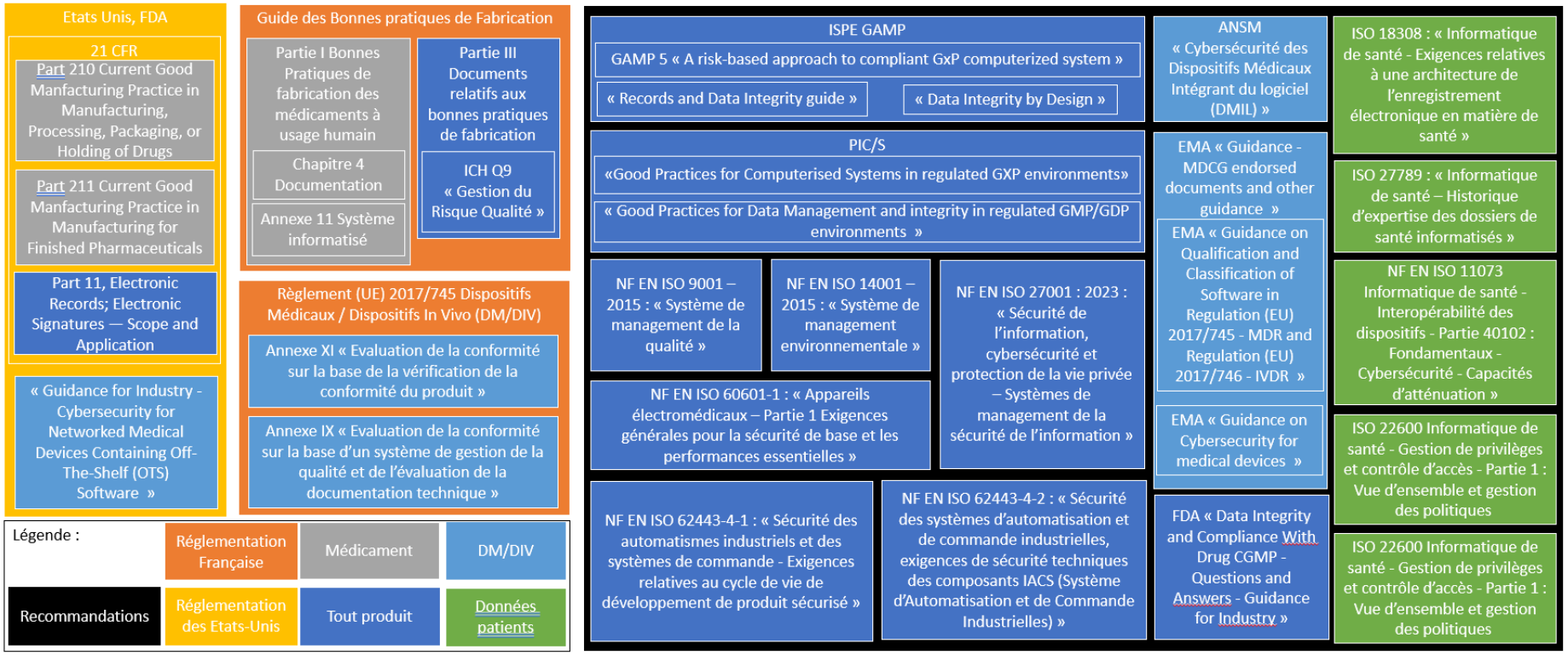
C'est une technologie intéressante car elle permet de regrouper l'ensemble de l'historique d'un produit. De plus, la chaine de bloc est dans la capacité d'assurer la sécurité, l'intégrité, la disponibilité et la non-répudiation des données. Grâce à cette technologie, et à la sérialisation présente sur chaque étui de médicament, il serait possible de retracer le cycle de production complet ainsi que l'ensemble du parcours logistique. La chaine de bloc n'est pas seulement intéressante pour l'industrie pharmaceutique, elle peut être utilisée dans l'ensemble du secteur de la santé comme pour améliorer la tenue décentralisée des dossiers pour les données de santé, pour les réclamations ou la gestion de l'approvisionnement [55].

Cette technologie peut être utilisée pour la gestion des outils de suivi informatisés et ainsi réduire la fraude systématique. La chaine de blocs permet de répondre à des problématiques du secteur médical et de soins de santé au travers de différents points. Elle permet de décentraliser le lieu de stockage des données et de pouvoir les échanger entre différentes entités, pour le suivi des essais cliniques par exemple. La chaine de blocs permet aussi

d’assurer la sécurité informatique et la confidentialité des données car elle rend difficile de retrouver les données associées à un patient pour un utilisateur qui n’aurait pas les clés cryptographiques. L’ensemble des transactions sont ainsi enregistrées et la traçabilité associée répond aux critères ALCOA+. Cependant, comme ce sont des données sensibles, les contributeurs devront être formés à la bonne utilisation de ces outils pour ne pas briser la confidentialité associée aux données. Cette technologie n’est pour le moment pas appliquée dans le secteur de la santé mais pourrait être indispensable à l’avenir.

Annexe

Annexe 1 : Organigramme des réglementations et des référentiels en fonction de leurs domaines d'application



Organigramme des réglementations et des référentiels en fonction de leurs domaines d'application

Annexe 2 : Cahier des charges pour un système informatique de suivi des réactifs

Objectifs du système

Suivi des réactifs en termes de volumétrie (stock) et de péremption au laboratoire de Contrôle Qualité. Le but est de s'assurer d'avoir les réactifs en quantité suffisante pour pouvoir réaliser les contrôles des produits, de l'environnement de routine et les contrôles exceptionnels.

Généralités

Le système doit être en interface avec notre système de commande de consommable.

Le système doit être en interface avec notre serveur pour la définition de l'horodatage.

Le système peut utiliser notre annuaire informatique interne pour définir les utilisateurs.

Le système doit répondre à l'ensemble des exigences des documents réglementaires 21CFR part 11 et Bonnes Pratiques de Fabrication

La maintenance du système doit être géré par la société propriétaire du système sous contrat de prestation.

Spécifications fonctionnelles :

1. Fonctionnalités administratives
    a. Gestion des profils

Des profils peuvent être définis à la demande. Avec le profil adéquate, il est possible de créer, modifier ou archiver l'ensemble des profils présents sur le système.

Aucun profil ne peut avoir l'ensemble des droits en même temps.

    b. Gestion des utilisateurs

Avec le profil adéquate, il est possible de créer, modifier ou archiver l'ensemble des utilisateurs et leurs profils associés.

Il est possible d'attribuer un ou plusieurs profils à un utilisateur.

Si plusieurs profils lui sont accordés, aucun utilisateur ne peut avoir l'ensemble des droits en même temps.

Chaque utilisateur peut accéder à la consultation des informations présentes dans le système.

c. Gestion de l'outil de suivi

Avec le profil adéquate, il est possible de modifier les éléments suivis.

La désactivation de l'outil de suivi est impossible.

Chaque ajout, modification, suppression, archivage, actions sont suivi par cet outil.

Les actions tracées par l'outil de suivi doivent contenir : l'identité de l'utilisateur, le/s profil/s accordé/s à l'utilisateur, l'action réalisée, les éléments présents avant l'action et les éléments présents après l'action, l'horodatage, la justification.

2. Activités ponctuelles
    a. Gestion des produits de la base de données :

Avec le profil adéquate, il est possible d'ajouter ou modifier le nom du produit, la référence et la date de péremption après ouverture.

Avec le profil adéquate, il est possible d'archiver les produits et les références associées.

b. Gestion des alertes

Avec le profil adéquate, il possible d'ajouter, modifier ou supprimer des alertes associées à la date de péremption d'un produit.

Avec le profil adéquate, il possible d'ajouter, modifier ou supprimer des alertes associées à la gestion des stocks d'un produit.

3. Activités régulières
    a. Utilisation des produits

Une douchette permet de scanner les produits. Via ce scan, le système est capable de retrouver le produit, la référence, la date de péremption, la quantité restante et les alertes associées à ce produit.

Avec le profil adéquate, il est possible d'insérer les volumes de produits consommés. Le système met à jour automatiquement les quantités restantes disponibles.

Avec le profil adéquate, il est possible d'insérer les dates d'ouvertures de produits. Si possible, le système est capable d'appliquer sur le produit juste ouvert, la date de péremption après ouverture. Si impossible, avec le profil adéquate, il est possible d'insérer manuellement les dates de péremption après ouverture.

Avec le profil adéquate, il est possible d'insérer les destructions des produits périmés. Le système met à jour automatiquement les quantités restantes disponibles.

    b. Réception de commande

Une douchette permet de scanner les produits. À la suite de ce scan, avec le profil adéquate, il est possible d'affilier un produit, une référence, d'insérer le nombre de flacons réceptionnés, le volume des flacons et leurs dates de péremption. Le système met à jour automatiquement les quantités restantes disponibles.

Annexe 3 : Analyse de risque de l'utilisation du système de suivi des réactifs du laboratoire

Référence	Fonction du système	Scénario à risque	Evaluation du risque					Mesure de mitigation	Gestion du risque résiduel	
			Gravité	Probabilité d'occurrence	Classe de risque	Probabilité de détection	Priorité du risque		Risque résiduel	Action
	1- Fonctionnalités du système									
1.01	Création, modification des références de réactifs	Associer une référence à un réactif différent. Risque : Utilisation du mauvais réactif	Elevé	Elevé	Elevé	Faible	Elevé	Double vérification lors de la création et modification de référence →Augmentation de la probabilité de détection	Moyen	Vérification périodique de l'outil de suivi : vérifier que les actions ont été réalisées et vérifiées par des utilisateurs ayant les droits, et que chaque action est conforme. Périodicité fixée à 3 mois pour un risque résiduel moyen. →Augmentation de la probabilité de détection
1.02	Suppression des références de réactifs	Suppression fortuite de références. Risque : Ne pas pouvoir réaliser le contrôle	Moyen	Elevé	Elevé	Faible	Elevé	Double vérification lors de la suppression de référence → Augmentation de la probabilité de détection	Moyen	Vérification périodique de l'outil de suivi : vérifier que les actions ont été réalisées et vérifiées par des utilisateurs ayant les droits, et que chaque action est conforme. Périodicité fixée à 3 mois pour un risque résiduel moyen. →Augmentation de la probabilité de détection
1.03	À la suite d'une réception de produit, enregistrement des quantités, des dates de péremption	Insérer une quantité sur estimée Risque : Avoir une quantité trop faible de réactif	Moyen	Elevé	Elevé	Moyen	Elevé	Programmer un seuil d'alerte automatique →Augmentation de la probabilité de détection	Faible	
1.04		Insérer une quantité sous-estimée Risque : Avoir une quantité trop importante de réactif	Faible	Elevé	Moyen	Moyen	Moyen	Risque uniquement économique, non mitigé	Faible	

Référence	Fonction du système	Scénario à risque	Evaluation du risque					Mesure de mitigation	Gestion du risque résiduel	
			Gravité	Probabilité d'occurrence	Classe de risque	Probabilité de détection	Priorité du risque		Risque résiduel	Action
1.05		Insérer une date de péremption antérieur à la date de péremption réelle Risque : Détruire le réactif trop tôt	Faible	Elevé	Moyen	Faible	Elevé	Risque uniquement économique, non mitigé	Faible	
1.06		Insérer une date de péremption postérieur à la date de péremption réelle Risque : Utiliser un réactif périmé	Elevé	Elevé	Elevé	Faible	Elevé	Double vérification lors de l'insertion de la date de péremption → Augmentation de la probabilité de détection Vérification et inscription dans le dossier de la date de péremption présente sur le produit avant chaque utilisation →Augmentation de la probabilité de détection	Faible	
1.07	À la suite de l'utilisation de produit, mise à jour des quantités	Insertion de données erronées : quantité retirée sous-estimée Risque : Avoir une quantité trop importante de réactif	Faible	Elevé	Moyen	Moyen	Moyen	Risque uniquement économique, non mitigé	Faible	
1.08		Insertion de données erronées : quantité retirée surestimée Risque : Avoir une quantité trop faible de réactif	Moyen	Elevé	Elevé	Moyen	Elevé	Programmer un seuil d'alerte automatique →Augmentation de la probabilité de détection	Faible	

Référence	Fonction du système	Scénario à risque	Evaluation du risque					Mesure de mitigation	Gestion du risque résiduel	
			Gravité	Probabilité d'occurrence	Classe de risque	Probabilité de détection	Priorité du risque		Risque résiduel	Action
1.09	À la suite de l'ouverture d'un produit, modification de la date de péremption	Insertion de données erronées : date de péremption antérieur à la date de péremption réelle Risque : Détruire le réactif trop tôt	Faible	Elevé	Moyen	Faible	Elevé	Risque uniquement économique, non mitigé	Faible	
1.10		Insertion de données erronées : date de péremption postérieur à la date de péremption réelle Risque : Utiliser un réactif périmé	Elevé	Elevé	Elevé	Faible	Elevé	Programmation de la date de péremption automatique à la suite de l'ouverture. Si insertion manuelle : double vérification de l'insertion →Diminution de la probabilité d'occurrence	Moyen	Vérification périodique de l'outil de suivi : vérifier que les actions ont été réalisées et vérifiées par des utilisateurs ayant les droits, et que chaque action est conforme. Périodicité fixée à 3 mois pour un risque résiduel moyen. →Augmentation de la probabilité de détection
1.11	A la suite d'une mise au rebut d'un produit, mise à jour de la quantité d'un produit	Mise à jour des stocks du mauvais produit Risque : Utilisation d'un réactif périmé	Elevé	Faible	Moyen	Faible	Elevé	Double vérification par scan de la référence au moment de la destruction par un second utilisateur →Augmentation de la probabilité de détection	Faible	
1.12	Consultation des quantités et des natures de produits	Pas de risque car aucune action possible dans le système	NA	NA	NA	NA	NA	NA	NA	NA

Référence	Fonction du système	Scénario à risque	Evaluation du risque					Mesure de mitigation	Gestion du risque résiduel	
			Gravité	Probabilité d'occurrence	Classe de risque	Probabilité de détection	Priorité du risque		Risque résiduel	Action
1.13	Gestion des alertes des produits bientôt à péremption	Modification de la date d'alerte Risque : Avoir une quantité trop faible de réactif	Moyen	Elevé	Elevé	Faible	Elevé	Limiter la modification de ces paramètres à des personnes autorisées dans le système →Diminution de la probabilité d'occurrence	Moyen	Vérification périodique de l'outil de suivi : vérifier que les actions ont été réalisées par des utilisateurs ayant les droits, et que chaque action est conforme. Périodicité fixée à 3 mois pour un risque résiduel moyen. →Augmentation de la probabilité de détection
	2- Gestion des paramètres									
2.01	Création, modification des profils de droits	Insertion d'un mauvais paramétrage Risque : Accorder des droits à une personne non habilitée	Moyen	Moyen	Moyen	Faible	Elevé	Limiter la modification de ces paramètres à des personnes autorisées dans le système →Diminution de la probabilité d'occurrence	Moyen	Vérification périodique de l'outil de suivi : vérifier que les actions ont été réalisées par des utilisateurs ayant les droits, et que chaque action est conforme. Périodicité fixée à 3 mois pour un risque résiduel moyen. →Augmentation de la probabilité de détection
2.02	Suppression de profils de droits	Suppression fortuite de profils de droits Risque : Perte de l'historique des actions liés à cet utilisateur	Moyen	Moyen	Moyen	Moyen	Moyen	L'action de « suppression » est impossible dans le système. Il n'existe que la fonction « Archivage ». →Diminution de la probabilité d'occurrence	Faible	

Référence	Fonction du système	Scénario à risque	Evaluation du risque					Mesure de mitigation	Gestion du risque résiduel	
			Gravité	Probabilité d'occurrence	Classe de risque	Probabilité de détection	Priorité du risque		Risque résiduel	Action
2.03	Création, modification des droits d'utilisateur	Accorder trop de droit à un utilisateur Risque : un utilisateur n'est pas habilité aux actions réalisées	Moyen	Moyen	Moyen	Faible	Elevé	Limiter la modification de ces paramètres à des personnes autorisées dans le système →Diminution de la probabilité d'occurrence	Moyen	Vérification périodique de l'outil de suivi : vérifier que les actions ont été réalisées par des utilisateurs ayant les droits, et que chaque action est conforme. Périodicité fixée à 3 mois pour un risque résiduel moyen. →Augmentation de la probabilité de détection
2.04	Suppression des droits d'utilisateur	Suppression fortuite de droit d'utilisateur Risque : Perte de l'historique des actions liés à cet utilisateur	Moyen	Moyen	Moyen	Moyen	Moyen	L'action de « suppression » est impossible dans le système. Il n'existe que la fonction « Archivage ». →Diminution de la probabilité d'occurrence	Faible	
2.05	Création, modification et suppression des éléments suivi par l'outil de suivi	Insertion d'un mauvais paramétrage Risque : suivi d'éléments définis non réalisé	Moyen	Moyen	Moyen	Faible	Elevé	Limiter la modification de ces paramètres à des personnes autorisées dans le système →Diminution de la probabilité d'occurrence	Moyen	Vérification périodique de l'outil de suivi : vérifier que les actions ont été réalisées par des utilisateurs ayant les droits, et que chaque action est conforme. Périodicité fixée à 3 mois pour un risque résiduel moyen. →Augmentation de la probabilité de détection
2.06	Activation/ désactivation de l'outil de suivi	Pas de risque car le système n'autorise pas la désactivation de l'outil de suivi. Ceci a été testé lors de la validation du système	NA	NA	NA	NA	NA	NA	NA	NA

Annexe 4 : Formulaire pour la revue de l'outil de suivi du système de suivi des réactifs du laboratoire de contrôle qualité

Revue de l'outil de suivi du système de suivi des réactifs du laboratoire

Période concernée par la revue : Du _____ au _____

1- Lister chaque création, modification des références de réactifs

Référence de l'action réalisée	VISA de la personne qui a réalisé	Habilitation de la personne qui a réalisée	VISA de la personne qui a vérifiée	Habilitation de la personne qui a vérifiée	Action conforme à l'attendue

2- Lister chaque suppression des références de réactifs

Référence de l'action réalisée	VISA de la personne qui a réalisé	Habilitation de la personne qui a réalisée	VISA de la personne qui a vérifiée	Habilitation de la personne qui a vérifiée	Action conforme à l'attendue

3- Lister chaque insertion manuelle de changement de date de péremption après ouverture de produit

Référence de l'action réalisée	VISA de la personne qui a réalisé	Habilitation de la personne qui a réalisée	VISA de la personne qui a vérifiée	Habilitation de la personne qui a vérifiée	Action conforme à l'attendue

4- Lister chaque modification de la date d'alerte des produits arrivant à péremption

Référence de l'action réalisée	VISA de la personne qui a réalisé	Habilitation de la personne qui a réalisée	VISA de la personne qui a vérifiée	Habilitation de la personne qui a vérifiée	Action conforme à l'attendue

5- Lister chaque création, modification des profils de droits

Référence de l'action réalisée	VISA de la personne qui a réalisé	Habilitation de la personne qui a réalisée	VISA de la personne qui a vérifiée	Habilitation de la personne qui a vérifiée	Action conforme à l'attendue

6- Lister chaque création, modification des droits d'utilisateur

Référence de l'action réalisée	VISA de la personne qui a réalisé	Habilitation de la personne qui a réalisée	VISA de la personne qui a vérifiée	Habilitation de la personne qui a vérifiée	Action conforme à l'attendue

7- Lister chaque création, modification et suppression des éléments suivi par l'outil de suivi

Référence de l'action réalisée	VISA de la personne qui a réalisé	Habilitation de la personne qui a réalisée	VISA de la personne qui a vérifiée	Habilitation de la personne qui a vérifiée	Action conforme à l'attendue

	Rédacteur	Vérificateur	Approbateur
DATE			
VISA/Signature	Expert métier	Responsable CQ	Responsable AQ SI

Bibliographie

[1] A. V. Bogoviz, E. G. Popkova, et Y. V. Ragulina, Éd., *Industry 4.0 : Industrial Revolution of the 21st Century*, 1st ed. 2019. in Studies in Systems, Decision and Control, no. 169. Cham: Springer International Publishing : Imprint: Springer, 2019. doi: 10.1007/978-3-319-94310-7.

[2] « Traçabilité », *Larousse*. 2022.

[3] Agence Nationale du Médicament et des produits de santé, « Guide des Bonnes Pratiques de Fabrication 2019 ». 6 mai 2019.

[4] Parlement européen et conseil, « Règlement (UE) 2017/745 relatif aux dispositifs médicaux ». Journal Officiel de l'Union européenne, 5 avril 2017.

[5] Parlement européen et conseil, « Règlement (CE) no 1223/2009 relatif aux produits cosmétiques ». Journal Officiel de l'Union européenne, 30 novembre 2009.

[6] Medicines and Health products Regulatory Agency, « MHRA GMP Data Integrity Definitions and Guidance for Industry ». mars 2015.

[7] Food and Drug Administration, « Title 21 - Food and Drugs Chapter I - Food and Drug Administration, Department of Health and Human Services Chapter C - Drugs : General Part 211 Current Good Manfacturing Practice in Manufacturing for Finished Pharmaceuticals ». 11 mars 2022.

[8] Food and Drug Administration, « Title 21 - Food and Drugs Chapter I - Food and Drug Administration, Department of Health and Human Services Chapter C - Drugs : General Part 210 Current Good Manfacturing Practice in Manufacturing, Processing, Packaging, or Holding of Drugs;General ». 11 mars 2022.

[9] Food and Drug Administration, « Guidance for Industry - Part 11, Electronic Records; Electronic Signatures — Scope and Application », Aout 2003.

[10] Pharmaceutical Inspection Convention et Pharmaceutical Inspection Co-operation Scheme, « Good practices for computerised systems in regulated "GXP" environments ». 25 septembre 2007.

[11] Pharmaceutical Inspection Convention et Pharmaceutical Inspection Co-operation Scheme, « Good Practices for Data management and integrity in regulated GMP/GDP environments ». 1 juillet 2021.

[12] Good Automated Manufacturing Practice Forum et International Society for Pharmaceutical Engineering, Éd., *A risk-based approach to compliant GxP computerized systems*. in Gamp, no. 5. Tampa, Fl: ISPE, 2008.

[13] International Society for Pharmaceutical Engineering, « ISPE GAMP - Guide : Records and Data Integrity ». 2017.

[14] International Society for Pharmaceutical Engineering, « ISPE GAMP - Good Practice Guide: Data Integrity by Design ». 2020.

[15] C. Estrosi, N. Kosciusko-Morizet, et D. Potier, « Briques génériques du logiciel embarqué », oct. 2010.

[16] A. Telukdarie et M. N. Sishi, « Enterprise Definition for Industry 4.0 », in *2018 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, Bangkok: IEEE, déc. 2018, p. 849-853. doi: 10.1109/IEEM.2018.8607642.

[17] DCMI Usage Board, « Dublin Core™ Metadata Element Set ». 14 juin 2012. Consulté le: 25 octobre 2022. [En ligne]. Disponible sur: https://www.dublincore.org/specifications/dublin-core/dces/

[18] Food and Drug Administration, « Data Integrity and Compliance With Drug CGMP - Questions and Answers - Guidance for Industry », déc. 2018.

[19] Agence Nationale du Médicament et des produits de santé, « Guide des Bonnes Pratiques de Fabrication 2007 ». 2007.

[20] Agence Nationale du Médicament et des produits de santé, « Guide des Bonnes Pratiques de Fabrication 2011 ». 2011.
[21] Agence Nationale du Médicament et des produits de santé, « Guide des Bonnes Pratiques de Fabrication 2015 ». 2015.
[22] « Data Integrity », *Google Trends*, 4 septembre 2022. https://trends.google.fr/trends/explore?date=all&q=Data%20integrity
[23] Food and Drug Administration, « Warning Letters », 15 septembre 2022. https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/compliance-actions-and-activities/warning-letters
[24] Agence Nationale du Médicament et des produits de santé, « Listes des injonctions publiées par l'ANSM », 15 septembre 2022. https://ansm.sante.fr/actualites/?filter%5Bcategories%5D%5B%5D=19
[25] R.D. McDowall, « The Why, What, and How CDS Audit trail Review », p. 163, mars 2020.
[26] P. Best, P. Rikhardsson, et M. Toleman, « Continuous Fraud Detection in Enterprise Systems through Audit Trail Analysis », *J. Digit. Forensics Secur. Law*, 2009, doi: 10.15394/jdfsl.2009.1053.
[27] O. López, *EU Annex 11 Guide to Computer Validation Compliance for the Worldwide Health Agency GMP*. Boca Raton: CRC Press,Taylor & Francis Group, 2015.
[28] « Audit trail », *Google Trends*, 4 septembre 2022. https://trends.google.fr/trends/explore?date=all&q=Audit%20trail
[29] GMED, « Guide - Demande de certification en vue du Marquage CE - Règlement (UE) 2017/745 ». septembre 2021.
[30] Agence Nationale du Médicament et des produits de santé, « Cybersécurité des Dispositifs Médicaux Intégrant du Logiciel au cours de leur cycle de vie ». septembre 2022.
[31] Food and Drug Administration, « Guidance for Industry - Cybersecurity for Networked Medical Devices Containing Off-The-Shelf (OTS) Software », janv. 2005.
[32] Association française de normalisation, « Norme NF EN ISO 22716 Cosmétiques Bonnes Pratiques de Fabrication (BPF) ». 12 décembre 2007.
[33] Agence Nationale du Médicament et des produits de santé, « Bonnes pratiques de pharmacovigilance ». mai 2022. [En ligne]. Disponible sur: https://ansm.sante.fr/uploads/2022/06/02/20220602-bppv-mai-2022-3.pdf
[34] Association française de normalisation, « Norme NF EN ISO 9001 Systèmes de management de la qualité - Exigences ». 15 octobre 2015.
[35] Association française de normalisation, « Norme NF EN ISO 14001 Systèmes de management environnemental - Exigences et lignes directrices pour son utilisation ». 15 octobre 2015.
[36] Association française de normalisation, « Norme NF ISO/IEC 27001 Sécurité de l'information, cybersécurité et protection de la vie privée - Système de management de la sécurité de l'information - Exigences ». 25 janvier 2023.
[37] Association française de normalisation, « Norme NF EN 60601-1 Appareils électromédicaux Partie 1 : Exigences générales pour la sécurité de base et les performances essentielles ». 20 janvier 2007.
[38] Association française de normalisation, « Norme NF EN IEC 62443 Sécurité des automatismes industriels et des systèmes de commande. Partie 4-1 : Exigences relatives au cycle de développement de produit sécurisé ». mars 2018.
[39] A. Saxena, « Audit Trail in Pharma : A Review », *Asian J. Pharm. Res.*, nov. 2022, doi: 10.52711/2231-5691.2022.00056.
[40] European commission, « Guidance - MDCG endorsed documents and other guidance », 23 décembre 2022. https://health.ec.europa.eu/medical-devices-sector/new-regulations/guidance-mdcg-endorsed-documents-and-other-guidance_en (consulté le 23 décembre 2022).
[41] Medical Device Coordination Group Document, « Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 - MDR and Regulation (EU) 2017/746 - IVDR ». octobre 2019.

[42] Medical Device Coordination Group Document, « Guidance on Cybersecurity for medical devices ». décembre 2019.
[43] Association française de normalisation, « Norme NF EN IEC 62443 Sécurité des systèmes d'automatisation et de commande industrielles - Partie 4-2 : Exigences de sécurité technique des composants IACS ». avril 2019.
[44] K. Jiang et X. Cao, « Design and implementation of an audit trail in compliance with US regulations », *Clin. Trials*, vol. 8, n° 5, p. 624-633, 2011, doi: 10.1177/1740774511413943.
[45] Z. R. Wolf, « Exploring the Audit Trail for Qualitative Investigations », *Nurse Educ.*, vol. 28, n° 4, juill. 2003, doi: 10.1097/00006223-200307000-00008.
[46] N. Nakamura, M. Nakayama, J. Nakaya, T. Tominaga, et T. Suganuma, « Audit Trail Management System in Community Health Care Information Network », 2015, doi: 10.3233/978-1-61499-564-7-1080.
[47] Association française de normalisation, « Norme NF ISO 18308 Informatique de santé - Exigences relatives à une architecture de l'enregistrement électronique en matière de santé ». juin 2011.
[48] Association française de normalisation, « Norme ISO 27789 Informatique de santé - Historique d'expertise des dossiers de santé informatisés ». octobre 2021.
[49] Association française de normalisation, « Norme NF EN ISO 11073 Informatique de santé - Interopérabilité des dispositifs - Partie 40102 : Fondamentaux - Cybersécurité - Capacités d'atténuation ». mars 2022.
[50] Association française de normalisation, « Norme ISO 22600 Informatique de santé - Gestion de privilèges et contrôle d'accès - Partie 1 : Vue d'ensemble et gestion des politiques ». octobre 2014.
[51] Association française de normalisation, « Norme ISO 2859 Règles d'échantillonnage pour les contrôles par attributs - Partie 1 : Procédures d'échantillonnage pour les contrôles lot par lot, indexés d'après le niveau de qualité acceptable (NQA) ». novembre 1999.
[52] Direction européenne de la qualité du médicament & soins de santé, « 5.21. Méthodes chimiométriques appliquées aux données analytiques ». Pharmacopée Européenne 10.0, janvier 2020.
[53] A. Argyrou, « Blockchain in audit trails - An investigation of how blockchain can help auditors to implement audit trails », mai 2018.
[54] F. Leal *et al.*, « Smart Pharmaceutical Manufacturing : Ensuring End-to-End Traceability and Data Integrity in Medicine Production », *Big Data Res.*, vol. 24, p. 100172, mai 2021, doi: 10.1016/j.bdr.2020.100172.
[55] S. Yaqoob *et al.*, « Use of Blockchain in Healthcare : A Systematic Literature Review », *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, n° 5, 2019, doi: 10.14569/IJACSA.2019.0100581.

NANTES UNIVERSITE

Année de la soutenance

2023

Nom – Prénoms : Lauriot Adeline Régina Amélie

Titre de la thèse : Gestion de l'intégrité des données : contraintes dans l'industrie pharmaceutique et application d'un outil de suivi dit « audit trail »

Résumé de la thèse :

La gestion de l'intégrité des données est un sujet de plus en plus important pour les industries de santé. Les différentes réglementations demandent la mise en place d'une traçabilité complète et fiable. Pour cela, les outils de suivi sont utilisés pour tracer chaque action ainsi que l'identité de l'utilisateur, l'horodatage et la justification correspondantes.

MOTS CLES

INTEGRITE DES DONNEES

OUTIL DE SUIVI

REGLEMENTATION

INDUSTRIE DE SANTE

JURY

Présidente : Mr Jean-Michel Robert, PharmD, PhD, HDR, UFR Sciences Pharmaceutiques et Biologiques de Nantes

Assesseurs : Mr Samuel Bertrand, Maitre de conférence (Associate Professor),Ph.D. Chimie, M.Sc. Chimie (ENSCL), UFR Sciences Pharmaceutiques et Biologiques de Nantes

Mr Antoine Pierson, Responsable Assurance Qualité en Data integrity, Servier, Gidy

Mr Julien Wang, Consultant Pharmacien Qualité, Caduceum, Rouen