Année 2023 - 2024 **Thèse n° 119**

Académie d'Orléans – Tours

Université de Tours

Faculté de Pharmacie « Phillipe – MAUPAS

Thése d'exercice pour le diplôme de

Docteur en Pharmacie

par

M. SIMON Judickaël

La Data Integrity au sein de l'industrie Pharmaceutique : enjeux et mise en application au sein du laboratoire de Contrôle Qualité de Delpharm Tours

Présentée et soutenue publiquement le 22 Décembre 2023

Membres du Jury :

Mme Leslie BOUDESOCQUE, Pharmacien, Professeur, Faculté de Pharmacie de Tours

M. Fabien FRANTZ, Responsable Contrôle Qualité, Delpharm Tours

Mme Jackie VERGOTE, Pharmacien, Maitre de Conférence, Faculté de Pharmacie de Tours

Mme Christine MORER, Pharmacien, Responsable Assurance Qualité, Delpharm Tours

Mme Perrine MANDREUX, Pharmacien, Responsable Assurance Qualité produit , Sanofi Tours

Listes des enseignants

Année : 2023 - 2024

Directeur : **Pr Denys BRAND**
Directeur Adjoint : **M. Matthieu JUSTE**
Assesseurs : **M. Gildas PRIE, Mme Mélanie BOUVIN PLEY, Mme Emilie ALLARD-VANNIER, M. Bruno GIRAUDEAU, Mme Claire POUPLARD, Mme Audrey OUDIN**

ENSEIGNANTS

14 PROFESSEURS D'UNIVERSITÉ

ALLARD-VANNIER	**Emilie**	PHARMACIE GALENIQUE
ALLOUCHI	**Hassan**	CHIMIE PHYSIQUE
BOUDESOCQUE-DELAYE	**Leslie**	PHARMACOGNOSIE
BRAND	**Denys**	MICROBIOLOGIE
BRAIBANT	**Martine**	MICROBIOLOGIE
CHEVALIER	**Stéphane**	BIOCHIMIE GENERALE & BIOTHERAPIE
CHOURPA	**Igor**	CHIMIE ANALYTIQUE
CLASTRE	**Marc**	BIOLOGIE CELLULAIRE & BIOCHIMIE VEGETALE
DIMIER-POISSON	**Isabelle**	PARASITOLOGIE & MYCOLOGIE MEDICALES, IMMUNITE ANTI-INFECTIEUSE
ENGUEHARD-GUEIFFIER	**Cécile**	CHIMIE THERAPEUTIQUE
MAHEO	**Karine**	PHYSIOLOGIE
MAUPOIL-DAVID	**Véronique**	PHARMACOLOGIE
MUNNIER	**Émilie**	PHARMACIE GALENIQUE
VIAUD-MASSUARD	**Marie-Claude**	CHIMIE ORGANIQUE

6 PROFESSEURS D'UNIVERSITÉ ET PRATICIENS HOSPITALIERS

ANTIER	**Daniel**	PHARMACIE CLINIQUE
ARLICOT	**Nicolas**	BIOPHYSIQUE & BIOINFORMATIQUE
EMOND	**Patrick**	BIOPHYSIQUE & BIOINFORMATIQUE
GIRAUDEAU	**Bruno**	SANTÉ PUBLIQUE, BIOSTATISTIQUE & ÉPIDÉMIOLOGIE
LANOTTE	**Philippe**	MICROBIOLOGIE
POUPLARD	**Claire**	HEMATOLOGIE

2 PROFESSEURS ÉMERITE

BARIN	**Francis**	MICROBIOLOGIE
THIBAULT	**Gilles**	IMMUNOLOGIE

35 MAITRES DE CONFÉRENCES

AUBREY	**Nicolas**	BIOCHIMIE GENERALE & BIOTHERAPIE
BESSON	**Pierre**	PHYSIOLOGIE
BIRER-WILLIAMS	**Caroline**	BIOLOGIE CELLULAIRE & BIOCHIMIE VEGETALE
BONNIER	**Franck**	CHIMIE ANALYTIQUE
BORDY	**Romain**	PHARMACOLOGIE & TOXICOLOGIE
BOUVIN-PLEY	**Mélanie**	MICROBIOLOGIE
BREDELOUX	**Pierre**	PHARMACOLOGIE
DAVID	**Stéphanie**	PHARMACIE GALENIQUE
DEBIERRE-GROCKIEGO	**Françoise**	PARASITOLOGIE & MYCOLOGIE MEDICALES, IMMUNITE ANTI-INFECTIEUSE
DELAYE	**Pierre-Olivier**	CHIMIE THERAPEUTIQUE
DENEVAULT	**Caroline**	CHIMIE THERAPEUTIQUE
DOUZIECH-EYROLLES	**Laurence**	AFFAIRE REGLEMENTAIRE ET MANAGEMENT DE LA QUALITE
DUMAS	**Jean-François**	BIOCHIMIE GENERALE ET BIOTHERAPIE
GERMON	**Stéphanie**	PARASITOLOGIE & MYCOLOGIE MEDICALES, IMMUNITE ANTI-INFECTIEUSE
GLEVAREC	**Gaëlle**	BIOLOGIE CELLULAIRE & BIOCHIMIE VEGETALE
HERVE-AUBERT	**Katel**	CHIMIE ANALYTIQUE
JUSTE	**Matthieu**	PARASITOLOGIE & MYCOLOGIE MEDICALES, IMMUNITE ANTI-INFECTIEUSE
LAJOIE	**Laurie**	IMMUNOLOGIE
LANOUE	**Arnaud**	BIOLOGIE CELLULAIRE & BIOCHIMIE VEGETALE
MARC	**Jillian**	BIOMOLECULES ET BIOTECHNOLOGIES VEGETALES
MAVEL	**Sylvie**	CHIMIE THERAPEUTIQUE
OUDIN	**Audrey**	BIOLOGIE CELLULAIRE & BIOCHIMIE VEGETALE
POUPET	**Cyril**	BIOLOGIE CELLULAIRE & BIOCHIMIE VEGETALE
PASQUALIN	**Côme**	PHARMACOLOGIE
PRIE	**Gildas**	CHIMIE ORGANIQUE
SAHLI	**Ramla**	PHARMACOGNOSIE
SIEROCKI	**Pierre**	CHIMIE ORGANIQUE
SOUCE	**Martin**	CHIMIE ANALYTIQUE
TAUBER	**Clovis**	BIOPHYSIQUE & BIOINFORMATIQUE
VELGE-ROUSSEL	**Florence**	IMMUNOLOGIE PARASITAIRE
VERCOUILLIE	**Johnny**	BIOPHYSIQUE & BIOINFORMATIQUE
VERGER	**Alexis**	PHARMACIE GALENIQUE
VERGOTE	**Jackie**	AFFAIRE REGLEMENTAIRE ET MANAGEMENT DE LA QUALITE
VIERRON	**Emilie**	SANTÉ PUBLIQUE, BIOSTATISTIQUE & ÉPIDÉMIOLOGIE
ZHANG	**Bei-Li**	PHARMACOLOGIE

Serment de Galien

En présence des Maitres de la Faculté, je fais le serment :

D'honorer ceux qui m'ont instruit(e) dans les préceptes de mon art et de leur témoigner ma reconnaissance en restant fidèle aux principes qui m'ont été enseignés et d'actualiser mes connaissances ;

D'exercer, dans l'intérêt de la santé publique, ma profession avec conscience et de respecter non seulement la législation en vigueur, mais aussi les règles de Déontologie, de l'honneur, de la probité et du désintéressement ;

De ne jamais oublier ma responsabilité et mes devoirs envers la personne humaine et sa dignité ;

En aucun cas, je ne consentirai à utiliser mes connaissances et mon état pour corrompre les mœurs et favoriser des actes criminels ;

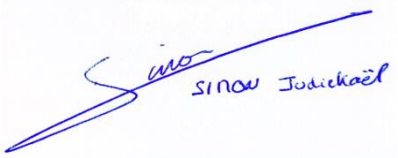
De ne dévoiler à personne les secrets qui m'auraient été confiés ou dont j'aurais eu connaissance dans l'exercice de ma profession ;

De faire preuve de loyauté et de solidarité envers mes collègues pharmaciens ;

De coopérer avec les autres professionnels de santé ;

Que les Hommes m'accordent leur estime si je suis fidèle à mes promesses. Que je sois couvert(e) d'opprobre et méprisé(e) de mes confrères si j'y manque

le 22/12/23 :



Remerciements

A Mme Leslie BOUDESOCQUE

Je tiens à vous remercier pour votre accompagnement tout au long de la rédaction de cette thèse en tant que Présidente du jury et co-Directrice, ainsi que pour votre réactivité lors des relectures et corrections de celle-ci. Je vous suis reconnaissant également pour les enseignements pratiques et théoriques que vous m'avez transmis tout au long de mon cursus universitaire, que ce soit en cours ou lors des différents stages effectués au sein du laboratoire SIMBA.

A M. Fabien FRANTZ

Je tiens à te remercier d'avoir accepté de co-diriger cette thèse portant sur un sujet que nous suivons depuis plusieurs années. Merci également de m'avoir offert l'opportunité d'intégrer le Laboratoire de Contrôle Qualité de Delpharm Tours en tant qu'alternant et de m'avoir fait confiance pour prendre la responsabilité du laboratoire de Physico-Chimie ces derniers mois. Ton soutien et tes conseils m'ont permis d'acquérir des compétences cruciales pour réussir mes études en Pharmacie pendant mon alternance, et qui me sont aujourd'hui bénéfiques dans ma vie professionnelle. J'espère pouvoir accompagner Ayoub et Amélie de la même manière, afin qu'eux aussi puissent réussir dans leur vie professionnelle.

A Mme Jackie VERGOTTE et à Mme Christine MORER

Je tiens à vous remercier de faire partie de ce jury de soutenance de thèse d'exercice marquant ainsi la fin de mes études en Pharmacie.

A ma famille,

Je tiens à remercier l'ensemble des membres de ma famille qui m'ont permis de devenir la personne que je suis aujourd'hui. Ils m'ont soutenu et accompagné pendant mes années de formation universitaire, et continuent de me soutenir dans ma vie personnelle et professionnelle. Je leur suis reconnaissant pour leur patience lors des moments les plus difficiles de mes études, ce qui m'a permis de continuer à avancer jusqu'à ce jour.

A mes amis,

Je tiens à vous remercier pour votre soutien depuis de nombreuses années. Depuis la première année de PACES pour la plupart d'entre vous (et pour d'autres, même bien avant), nous nous sommes toujours suivis et soutenus afin qu'aujourd'hui chacun d'entre nous ait réussi le pari de terminer nos études, nous permettant ainsi de réaliser un métier qui nous rende heureux et de concrétiser des projets professionnels et personnels. Un merci particulier à Perrine qui a accepté de faire partie de mon jury de soutenance de thèse, marquant symboliquement la fin d'une époque.

Je tiens à remercier également l'ensemble du corps enseignant de la Faculté de Pharmacie de Tours qui nous à enseigner les bases de notre métier de Pharmacien.

Table des matières

Table des illustrations

Tableaux

Figures

Glossaire

AC : Article de conditionnement

AMM : autorisation de mise sur le marché

ANSM : Agence nationale de sécurité du médicament et des produits de santé (France)

AR : analyse de risque

ATMP : Advanced Therapy Medicinal Products

Audit trail : piste d'enregistrement, il s'agit d'un enregistrement continu des actions menées sur un systèmes informatisés

BPF : Bonnes pratiques de Fabrication

CPG : Chromatographie en phase gazeuse

CQ : Contrôle Qualité

CSP : Code de Santé Publique

DMID : Data Managment and Data Integrity

EMA : European Medicines Agency

FDA : Food and Drugs Administration (USA)

GxP : Good x Practices

HPLC : High Performance Liquide Chromatography

ICH : International Concil for Harmonization

IR : Infra Rouge

ISPE : Internationnal Society for Phamaceutical Engenering

IT : Information Technology (désigne de service Informatique)

LAL : Lysat d'Amébocytes de Limules (test endotoxines bactériennes)

MHRA : Medicines and Healthcare products Regulatory Agency (Grande Bretagne)

MP : matière premiere

OMS : Organisation Mondiale de la Santé

OOS : Out of Specifications

PF : Produit fini

PIC/s : Pharmaceutical Inspection Co-operation Scheme

SAA : Spectroscopie d'Absorption Atomique

TGA ; Medicines and Healthcare products Regulatory Agency (Australie)

USP : United States Pharmacopeia

UV : Ultra Violet

WHO : World Health Organization

ZAC : Zone à atmosphère contrôlée

Résumé de la thèse

Aujourd'hui, les réglementations liées à la production des produits de santé sont plus strictes que celles qui étaient en place il y a encore une dizaine d'années. La réglementation se durcit dans un seul but avec un seul objectif : la sécurité du patient. La traçabilité des données liées aux médicaments est donc devenue, cette dernière décennie, un enjeu majeur de la santé publique mondiale, et les industries pharmaceutiques doivent s'adapter pour répondre au mieux aux autorités régulatrices de produits de santé.

La mise en place d'une traçabilité globale est résumée sous le terme « Data Integrity ». La demande liée à l'intégrité des données par les autorités doit être prise en considération, et des mesures correctrices doivent être mises en œuvre par les industries pharmaceutiques. La mise en place de protocoles et d'actions en lien avec l'intégrité des données doit se faire dans tous les domaines de l'industrie pharmaceutique. Un de ces domaines est le laboratoire de Contrôle Qualité, dont le rôle est d'analyser les produits de santé afin de pouvoir attester de leur qualité.

Le but de cette thèse est d'établir un résumé condensé des actions et des outils pouvant être mis en œuvre dans le but d'accroître la sécurisation des données fournies par les laboratoires de contrôle qualité.

Ce travail pourrait ainsi servir à des étudiants, des alternants, des chefs de projet qui seront en charge de travailler sur des projets d'amélioration continue en lien avec la Data Integrity au sein des laboratoires de contrôle qualité. Les outils et principes généraux qui y sont décrits sont des prérequis essentiels à la mise en place de protocoles d'intégrité des données au sein des laboratoires pharmaceutiques

Introduction Générale

Les industries pharmaceutiques ont la responsabilité de fournir aux patients des produits de qualité et de garantir la sécurité des médicaments qui seront prescrits ou administrés. La production de produits de santé doit donc se faire sous haute surveillance afin de garantir la qualité, la sécurité et l'efficacité des médicaments, dispositifs médicaux ou produits cosmétiques.

Les autorités régulatrices des médicaments de toutes les nations mondiales (l'ANSM, l'Agence Nationale de Sécurité du Médicament et des produits de santé, la FDA, Food and Drugs Administration, la MHRA, Medicines and Healthcare products Regulatory Agency, etc.) ainsi que des organismes tels que l'OMS (Organisation Mondiale de la Santé), le PIC/s (Pharmaceutical Inspection Co-operation Scheme), l'EMA (European Medicines Agency) travaillent à instaurer des règles, des normes et des recommandations visant à garantir une production fiable et sécurisée de produits de santé.

Il est aujourd'hui aberrant de penser qu'à partir des années 1980, les règles d'hygiène pour la production de produits destinés à être injectés autorisaient de fumer à proximité des cuves de fabrication des médicaments. Les normes d'hygiène ont évolué (en instaurant le principe des Zone à Atmosphère Contrôlée (ZAC), des zones blanches, des tenues désarticulées, …) afin de garantir une production sécurisée de produits de santé. Depuis une vingtaine d'années, la préoccupation majeure des différents organismes de régulation des produits de santé est la traçabilité des productions. Le concept d'intégrité des données a été évoqué pour la première fois par la FDA dans les années 1960 et s'est aujourd'hui démocratisé. La traçabilité des données liées à la production des médicaments vise à suivre la vie du produit de santé à tous les niveaux.

Suite à mon master, j'ai intégré le groupe Delpharm au sein du site de Tours. Le groupe Delpharm est l'un des leaders mondiaux de la production de médicaments. Il s'agit d'un sous-traitant travaillant pour des clients (d'autres entreprises pharmaceutiques ou cosmétiques) en produisant leurs produits de santé selon leurs recommandations et en accord avec les règles définies par les différents textes réglementaires. Les usines de sous-traitance Delpharm se doivent de garantir aux clients une qualité de production de leurs produits afin que ceux-ci puissent être utilisés sans craintes par les patients. Cette qualité de production se traduit par une traçabilité des données de production qui permet de justifier de la compétence de Delpharm à produire des produits de qualité.

Je travaille au sein du laboratoire de Contrôle Qualité du site de Delpharm Tours où le concept de Data Integrity est omniprésent. Les analyses réalisées au sein du laboratoire visent à contrôler la qualité de tout ce qui entre dans les produits de santé (matières premières, articles de conditionnement) ainsi qu'à contrôler la qualité des produits fabriqués et leur environnement de production. Les résultats d'analyses obtenus au laboratoire permettent de déterminer si un produit de santé est conforme en tous points aux spécifications exigées par les clients et les autorités du médicament, afin de permettre sa libération pour sa mise sur le marché et son administration à des patients.

Le but de cette thèse est de résumer le concept de Data Integrity au sein d'un laboratoire de contrôle qualité et de décrire des outils permettant de garantir l'intégrité des données obtenues. Cette thèse vise également à servir de support à des étudiants et des chefs de projets dont les missions seront associées à la mise en place de protocoles de gestion des données au sein d'une entreprise.

Partie 1 : Les principes fondamentaux de la Data Integrity

1. Histoire de l'intégrité des données au sein de l'industrie pharmaceutique

La Data Integrity est un terme relativement ancien mais très présent dans l'industrie pharmaceutique depuis les années 2010. L'intégrité des données dans l'industrie pharmaceutique était une préoccupation majeure à la fin du 20ème siècle. C'est la FDA qui a publié en 1963 [1] la première directive en termes de Data Integrity et depuis cette date, l'ensemble des agences de régulation des médicaments dans le monde travaillent à instaurer des règles en lien avec la gestion des données papier ou numériques.

Ces préoccupations sont au cœur des discussions aujourd'hui suite à plusieurs affaires où l'intégrité des données a été remise en cause. L'une de ces affaires concerne la Data Integrity au sein des laboratoires de contrôle qualité. Il s'agit du cas du laboratoire Able (USA). Ce laboratoire, fabricant de médicaments génériques, a été mis en cause pour des produits sous-dosés ou sur-dosés mis sur le marché sur la base de tests en laboratoire falsifiés. En 2005, suite à une dénonciation interne, le laboratoire Able [2], déjà sous surveillance étroite par la FDA pour des problèmes similaires dans les années 90, a fait l'objet d'une enquête pour la mise sur le marché de médicaments dont les dossiers ont été falsifiés. Les conclusions de l'enquête ont pu être obtenues suite à la vérification des enregistrements des équipements de laboratoire. Des données papier falsifiées (enregistrements modifiés, fausses impressions, …) ont été jointes aux dossiers de lots qui ont pu être libérés. En effet, il a été démontré que le laboratoire a retraité des résultats OOS (Out Of Specifications) afin d'en faire des résultats conformes. Il a également été démontré que certains tests n'ont pas été réalisés dans les bonnes conditions avec des méthodes inappropriées. L'analyse des enregistrements a permis de montrer que le retraitement de certains chromatogrammes a été effectué sans traçabilité.

Les problèmes de Data Integrity sont des problèmes de santé publique. Il doit être possible de tracer l'origine et la qualité des produits de santé qui sont administrés aux patients.

Les scandales liés à des problèmes de traçabilité des produits de santé sont aujourd'hui moins médiatisés que d'autres problèmes de santé publique de la fin du 20ème siècle ou du début du 21ème siècle (Talc Morhange, Thalidomide, Mediator, …) mais les conséquences d'un problème de traçabilité peuvent être aussi dramatiques : la mise sur le marché d'un produit ne respectant pas les dosages peut entraîner le décès de patients malgré un usage normal et prévu de celui-ci.

Les règles d'intégrité des données n'ont pas été durcies d'année en année uniquement suite à des séries d'incidents. Elles ont été renforcées afin de combler les lacunes dans la réglementation de la production des produits de santé pour sécuriser au maximum la prise des médicaments par les patients

2. La Data Integrity, Qu'est-ce que c'est ?

Depuis plusieurs années, l'une des préoccupations des industries des produits de santé est la protection et la conservation des données. Le terme « Data Integrity » est un terme générique regroupant les principes de gestion des données dans les domaines de l'archivage, de la sécurisation et de la traçabilité.

La Data Integrity peut être résumée par l'acronyme ALCOA + (Figure 1) :

- Attribuable (Attributable) : les auteurs et sources des données doivent être clairement identifiés. Il est possible de citer comme exemple le fait de dater et de signer systématiquement les documents afin de connaître leur origine ;
- Lisible (Legible) : les données doivent être visualisables sur le long terme. Ce point peut se traduire par l'utilisation d'une encre (ex : stylo bille) plutôt que du crayon à papier pour rédiger un document. Le crayon va s'effacer avec le temps tandis que l'encre restera ;
- Contemporain (Contemporaneous) : Une donnée doit être enregistrée au moment où elle est acquise. Une mesure doit être enregistrée ou archivée dès son acquisition. Il n'est pas acceptable de retrouver une donnée non liée à un processus. Il doit être possible de

savoir quand cette information a été obtenue (exemple : un ticket de pesée doit être horodaté) ;

- Originale (Original) : Il doit s'agir de la donnée issue du premier enregistrement ou d'une copie certifiée. Un document original doit être certifié et ses copies doivent être tracées dans le but d'éviter que des copies d'une procédure archivée, par exemple, soient encore utilisées à défaut de la procédure à jour ;
- Précis (Accurate) : la donnée doit être conforme à la réalité et traitée correctement. Il est possible de citer comme exemple les processus d'investigation en cas de défauts retrouvés. L'investigation doit être la plus complète possible afin de permettre de comprendre les aboutissants plusieurs mois ou années après sa rédaction ;
- + :
    - Complete : est-ce que toutes les informations sont disponibles ?
    - Consistent : est-ce que la donnée est correcte / vérifiée ?
    - Enduring : les données sont-elles stockées en toute sécurité pour une utilisation sur le long terme ?
    - Available : est-ce que les données sont accessibles immédiatement ?

Figure 1 : Principe ALCOA +

La « Data Integrity » n'est pas seulement associée à la gestion des systèmes informatiques. Il s'agit de la gestion des données sous tous les formats. Les données peuvent être classées en 3 domaines :

• *Paper data* : Il s'agit d'une donnée obtenue sans équipement électronique ou système informatisé. La donnée se trouve sur un document papier rédigé par une personne sans intervention de la machine. Concernant le laboratoire et les analyses, le cahier de laboratoire fait foi dans l'archivage de cette donnée. Au sein d'un laboratoire, il peut s'agir du résultat d'un comptage de colonies sur une boîte de Pétri. Cette mesure est obtenue via l'œil humain et retranscrite sur un document (cahier de laboratoire ou rapport informatique tel qu'un bulletin d'analyse). En Zone à Atmosphère Contrôlée (ZAC), il peut s'agir de la feuille d'émargement des techniciens présents lors d'une journée de production ou de la feuille de suivi de nettoyage d'une zone. Toutes ces données doivent être conservées sur des supports physiques et les principes de la Data Integrity s'y appliquent au même titre que pour les données archivées sur des serveurs informatiques.

• *Hybrid data* : Les données hybrides sont obtenues sur un appareil électronique possédant un logiciel interne utilisant un algorithme pour générer une donnée. Il peut s'agir d'un résultat d'analyse spectrométrique UV ou IR. Le logiciel interne réalise la mesure de pourcentage de lumière transmise et émet une donnée sous la forme de l'absorbance qui sera imprimée sur un rapport papier. Le stockage des données est partiellement possible sur cet appareil, mais de manière incomplète. L'appareil ne permet pas un archivage complet des données au format numérique ; le format papier via les cahiers de laboratoire est le support à long terme de conservation de ce type de données.

• *Computerized data* : Ces données peuvent être obtenues et archivées intégralement de façon numérique. Il peut s'agir de données obtenues à l'aide des systèmes informatiques tels que des résultats d'analyses sur des HPLC en réseau. Les données sont obtenues puis archivées automatiquement. L'archivage informatique fait foi dans la conservation de cette donnée. Il peut également s'agir de données obtenues via des logiciels de gestion (comme StarLIMS

permettant la gestion des données au sein du laboratoire ou SAP permettant la gestion des données associées à la production).

Deux types de données supplémentaires sont également décrites, les *Static data* et les *Dynamic data*. Les Données statiques sont figées dans le temps, elles n'évolueront pas et ne seront pas mises à jour. Par exemple, le résultat d'une analyse à un temps donné restera inchangé et la donnée brute ne doit pas être altérée, il s'agit de *Static data*. Par exemple, un ticket de mesure est une donnée statique, la valeur lue correspond à une donnée obtenue à un moment précis, elle est figée dans le temps. En revanche, la liste des personnes ayant accès à un équipement est une *Dynamic data*. Son contenu est en constante évolution et doit être régulièrement mis à jour. Un suivi de la température d'un réfrigérateur est un autre exemple de donnée dynamique, son enregistrement est continu et à chaque instant de nouvelles informations sont fournies.

Le but global de la Data Integrity est de s'assurer qu'une donnée est fiable et conservée. On doit être capable de faire confiance aux données fournies et pouvoir les consulter après leur archivage ainsi que de connaître le contexte d'obtention de celles-ci (Qui, Quand, Comment et Pourquoi le cas échéant).

Cette gestion complète des données doit permettre de retrouver la personne et la date à l'origine de l'émission d'une donnée. Cela a pour but de justifier de la « qualité » de celle-ci en permettant de prouver que la personne à l'origine de la donnée est formée et est autorisée à la créer : la personne qui a obtenu cette donnée est-elle apte à fournir ce type de donnée ? Est-elle formée à l'utilisation de l'équipement qui a fourni cette information ?

La date et la signature des documents sur des cahiers de laboratoire sont la garantie que les informations qui s'y trouvent ont été obtenues conformément aux BPF (ou autres textes détaillant des exigences réglementaires). Sur des systèmes informatiques, une gestion des accès aux systèmes doit être mise en place. Sur des systèmes simples, un logbook peut suffire à suivre

les utilisations d'un appareil, mais sur des systèmes plus complexes, la mise en place de comptes utilisateurs avec une restriction des droits doit être faite.

La gestion des archivages est également un point critique de la Data Integrity. Il doit être possible de conserver une donnée, sous un format papier ou numérique, ainsi que de s'assurer que cette donnée sera non falsifiable et consultable à n'importe quel moment. Il doit être possible de consulter une donnée obtenue sur un logiciel même des années plus tard. Par exemple : les données relatives aux médicaments dérivés du sang doivent être conservées pendant 40 ans [3].

3. Aspects réglementaires de la Data Integrity

3.1. La Data Integrity dans la réglementation

Les principes généraux de la Data Integrity sont régis par des textes réglementaires opposables et des normes émanant d'organismes privés qui permettent de justifier des bonnes pratiques en laboratoire.

La plupart des agences réglementaires des médicaments ont intégré des sections faisant référence à la gestion des systèmes informatisés et à la gestion de la Data Integrity. Elles incluent généralement dans leurs textes réglementaires des indications, des principes ou des obligations concernant les bonnes pratiques documentaires. Ces textes prennent en compte à la fois les données papiers et les données informatiques. Cependant, depuis quelques années, les autorités régulatrices tendent à fournir davantage d'indications concernant l'intégrité des données informatiques.

L'ANSM détaille ses exigences dans 2 parties :

• Le chapitre 4 (publié en 2011) [4] des BPF : « Documentation » traite de toutes les bonnes pratiques documentaires au sein d'une entreprise pharmaceutique. Les principes énoncés dans ce chapitre se retrouvent également dans les principes de l'ALCOA+. On y

retrouve les principes du bon remplissage des documents ainsi que les exigences en termes de conservation de ces données (Archivage). Les informations liées au remplissage et au suivi des dossiers de lot y sont clairement définies.

• L'annexe 11 des BPF (publiée en 2011) : systèmes informatisés. Cette annexe des BPF fait suite aux bonnes pratiques documentaires du chapitre 4. Elle décrit les principes de gestion et d'utilisation des systèmes informatisés au sein des entreprises pharmaceutiques. Des principes tels que la gestion des risques, la gestion des données, la validation ou la sécurité de ces systèmes y sont abordés.

La FDA décrit ses exigences en termes de Data Integrity dans le document « 21 CFR part 11: Electronic Records; Electronic Signatures » de la Food and Drug Administration (FDA) publié en 2003 [5]. La FDA est chargée de protéger la santé publique en garantissant l'innocuité, l'efficacité et la sécurité des médicaments à usage humain et vétérinaire aux États-Unis. Ce document fournit des bonnes pratiques aux industriels qui ont choisi de conserver et soumettre les enregistrements sous format électronique.

Des informations sur l'audit trail, sur la gestion des données et sur la gestion des accès y sont décrites. Des principes généraux du lexique y sont également détaillés (data, metadata, static data, dynamic data, …). Des informations sur les méthodes de revue des audits trail y sont décrites (Qui doit faire ces revues ? Quand doivent-elles être faites ? Comment doivent-elles être faites ? …). Le 21 CFR part 11 représente également une norme réglementaire exigée par de nombreuses entreprises (y compris celles qui ne sont pas agréées pour produire des médicaments pour les marchés américains). Il est nécessaire de se conformer à cette norme pour attester de la conformité des résultats et garantir la qualité des produits testés ou façonnés.

L'autorité régulatrice britannique des produits de santé, la MHRA, décrit des principes similaires dans le document de 2018 : "GxP" Data Integrity Guidance and Definitions [6]. D'autres commissions telles que la Commission nationale de la santé chinoise ont publié le « Drug Data Management Standard » et l'autorité australienne du médicament (TGA) avec le

DMDI (Data Management and Data Integrity) ont également décrit des principes et des exigences en lien avec les bonnes pratiques de gestion des données.

L'Organisation mondiale de la santé (OMS) a également décrit des principes et des exigences dans un document intitulé « Guidance on good data and record management practices » [7]. L'annexe 5 de ce document décrit des principes généraux de la Data Integrity (ALCOA, Audit trail, Backup, …) ainsi que des principes de procédures liées aux données et à leur protection (gestion des audits trail, gestion des accès, …).

Le PIC/s, une organisation composée de 54 autorités de santé, fournit des informations sur la gestion des données dans le but d'uniformiser les pratiques entre les différents pays (selon les mêmes principes moraux que les ICH). Ce document de 2021, le « Good Practices for Data Management and Integrity in regulated GMP/GDP environments » [8], reprend des principes généraux de la gestion des données mais donne également des indications sur le système de gestion des données papiers et des données numériques en interne et lors d'activités externalisées.

L'ISPE, un réseau de sociétés pharmaceutiques à but lucratif établissant des guides en lien avec la gestion des activités pharmaceutiques, a publié le GAMP 5 (dernière version en 2022) [9] : A Risk-Based Approach to Compliant GxP Computerized Systems. Il s'agit d'un guide donnant des indications sur la gestion des systèmes informatiques. Il contient des indications sur la validation de ces systèmes, la gestion des systèmes (au niveau de la gestion des accès, des sauvegardes et de l'archivage, de la sécurité, …) ainsi que des indications concernant la Qualité en général en lien avec les systèmes informatiques.

En dehors de ces obligations réglementaires qui peuvent s'apparenter à des contraintes, la mise en place des principes de Data Integrity présente des intérêts multiples.

4. But de la Data Integrity

4.1. Pour le patient

La Data Integrity n’est pas seulement présente pour s’assurer de la fiabilité et de la traçabilité des données. La finalité des protocoles et procédures liés à la Data Integrity est la sécurité du médicament pour le patient. Bien qu'un patient ne soit pas informé de la personne qui a effectué la maintenance de la ligne de conditionnement des médicaments qui lui sont prescrits, tous ces protocoles en place visent à établir sa confiance dans l'ensemble de la chaîne de production. Ces protocoles assurent la traçabilité des médicaments, depuis la fabrication des matières premières utilisées dans la production du produit fini jusqu’à la gestion de la conservation du produit fini dans la pharmacie de ville où ils seront délivrés au patient.

Tout cela vise à sécuriser le produit délivré aux patients en garantissant qu'il a été produit, testé, conservé, transporté, ... dans des conditions optimales, assurant ainsi la sécurité du produit pris par le patient.

4.2. Pour l’entreprise

Pour une entreprise, la mise en place de procédures et de protocoles liés à la Data Integrity représente une dépense importante en termes de ressources (temps et de personnel). La stricte application de ces mesures constitue une charge pour les entreprises, car elles nécessitent souvent des changements importants dans les méthodes de travail ainsi que des investissements financiers importants.

Néanmoins, il s'agit d'une valeur ajoutée essentielle pour les entreprises d'instaurer ces protocoles de gestion des données. Cela permet de sécuriser les processus de fabrication, d'améliorer la gestion des archives, de suivre la formation du personnel, d'uniformiser les pratiques documentaires et d'analyse, ainsi que d'améliorer la réactivité face aux demandes de renseignements spécifiques sur un écart ou un événement.

La mise en place de protocoles liés à la Data Integrity fait également partie intégrante du processus d'amélioration continue. L'analyse des systèmes permet d'identifier les points

sensibles à améliorer. Le suivi des améliorations peut être utilisé comme un indicateur de sécurité en matière de gestion des données.

Lors des inspections menées par les autorités régulatrices ou lors des audits des clients, une bonne gestion des données permet également de réduire le risque de rencontrer des écarts pouvant avoir des répercussions sur l'entreprise. L'image de l'entreprise sera améliorée si la gestion des accès, la traçabilité des résultats et le système d'archivage sont conformes aux exigences actuelles des autorités de santé.

4.3. Pour les autorités régulatrices

Les autorités de santé sont les garantes de la sécurité des médicaments sur les marchés. La mise en place, au sein des entreprises de production, de protocoles de gestion des données permet de sécuriser les médicaments présents sur le marché. La traçabilité des médicaments est un point crucial, et l'une des responsabilités des autorités de régulation des médicaments est le rappel des lots de produits de santé en cas de problèmes découverts après leur mise sur le marché. La mise en place de la traçabilité des données facilite le rappel des produits.

Après cette vision générale, nous allons voir dans le chapitre suivant l’application des principes de la Data Integrity au sein du Laboratoire de Contrôle Qualité.

Partie 2 : Data Integrity au Laboratoire de Contrôle Qualité

1. Introduction : La Data Integrity au sein d'un laboratoire de Contrôle Qualité

Au sein d'une industrie pharmaceutique, le laboratoire de Contrôle Qualité joue un rôle essentiel. Les analyses effectuées garantissent la qualité des Matières Premières (MP) entrant dans la composition des produits de santé ainsi que la conformité des Produits Finis (PF) aux spécifications définies par les Donneurs d'Ordres (entreprises clientes disposant d'une AMM) ou par les textes réglementaires (par exemple, la Pharmacopée Européenne, l'USP, les directives ICH, etc.). Les laboratoires de Contrôle Qualité sont en première ligne pour assurer la qualité et la sécurité des produits de santé. Les lacunes en termes d'intégrité des données peuvent être associées à de graves problèmes de santé publique (comme le scandale du laboratoire Able [2]). Les responsables des laboratoires de Contrôle Qualité jouent un rôle clé dans la mise sur le marché des produits de santé. Ils sont responsables de la qualité des analyses réalisées sur les matières premières et les produits finis, et peuvent être responsables de la libération "analytique" des produits de santé. Les pharmaciens responsables de la libération des lots ne possèdent pas forcement les compétences nécessaires à certifier la conformité des analyses Physico-chimiques et Microbiologiques aux spécifications. Ainsi, la Data Integrity joue un rôle primordial dans les laboratoires de Contrôle Qualité en termes de traçabilité des résultats et d'intégrité des analyses afin de définir les rôles et les responsabilités de chacun.

La Data Integrity représente donc un enjeu majeur de cette décennie au sein des industries pharmaceutiques, en particulier au sein des laboratoires de Contrôle Qualité.

Les auditeurs (lors d'audits internes, d'audits clients, ou d'inspections par les autorités de régulation des médicaments) portent généralement une attention particulière aux pratiques des laboratoires de Contrôle Qualité en matière d'intégrité des données. Des aspects tels que l'archivage des résultats, l'attribution des analyses et la supervision des résultats sont souvent examinés lors de ces audits et inspections.

La Data Integrity est omniprésente au sein d'un laboratoire de contrôle qualité. Les données fournies par ces laboratoires sont essentielles pour la libération des lots avant la commercialisation des médicaments. Il est donc crucial d'assurer la traçabilité des données ainsi que des méthodes utilisées pour les obtenir. La mise à niveau des processus et des équipements sous l'angle de l'intégrité des données constitue donc une préoccupation majeure des laboratoires pour se conformer aux réglementations et aux exigences des autorités sanitaires.

Une autre problématique de la Data Integrity dans les laboratoires de contrôle qualité concerne le contrôle documentaire, par exemple : les matières premières destinées à être utilisées dans les produits finis. Il incombe aux laboratoires de contrôler si les fabricants de MP fournissent des produits conformes aux spécifications établies. Les producteurs de matières premières ne sont pas toujours au fait des règlementations et des exigences spécifiques à l'industrie pharmaceutique. Certains de ces fournisseurs peuvent également servir d'autres industries telles que l'agroalimentaire, la chimie ou la cosmétique, qui ont des normes différentes en matière d'intégrité des données.

À titre d'exemple, un fournisseur a fourni à Delpharm Tours une matière première conforme à toutes les spécifications physico-chimiques requises, mais dont la provenance n'était pas clairement définie. Bien que tous les tests effectués sur cette matière première soient conformes, le lieu de production de cette MP ne correspondait pas à celui indiqué dans le dossier. Se pose alors la question de savoir si ce nouveau fabricant respecte toutes les réglementations associées à l'industrie pharmaceutique. La MP, bien que de bonne qualité physico-chimique, n'a pas pu être utilisée dans un produit fini en raison de son manque de traçabilité claire. La Data Integrity s'applique à tous les niveaux des contrôles réalisés dans les laboratoires de Contrôle Qualité.

2. Questions fréquentes en Audit

Pendant les audits d'un laboratoire de Contrôle Qualité, les questions et les points fréquemment abordés sont liés aux principes ALCOA. Les contraintes actuelles résultant de l'évolution réglementaire font que ces points sont de plus en plus notifiés par les clients et les autorités régulatrices. Les points les plus fréquemment abordés sont :

• Attribuable : Qui a réalisé les analyses ? Qui a revu les résultats ? Qui approuve les résultats ? Est-ce que ces différents acteurs sont formés et habilités à réaliser ces actions ?

• Lisible : Les données brutes et les résultats obtenus doivent être conservés de manière à pouvoir être réexaminés en cas de besoin (investigation en cas de litige, rappel de lot, etc.). Comment conserver de manière pérenne les données et pendant combien de temps ?

• Contemporaneous : Comment justifie-t-on qu'une analyse n'est pas antidatée ?

• Original : Comment justifie-t-on qu'une analyse n'est pas un retest ?

• Accurate : Comment justifier que les résultats obtenus sont fiables et non falsifiés ? Comment tracez-vous l'ensemble des déviations et des investigations ?

Depuis plusieurs années, les inspections des autorités régulatrices ou des clients sont axées sur ces différentes questions. Il incombe aux industries pharmaceutiques d'y répondre et de mettre en œuvre des actions correctives ou préventives permettant de fournir des informations claires sur ces sujets.

L'image d'une entreprise peut être impactée par des problèmes de Data Integrity. Si la traçabilité des données ne peut pas être démontrée, la confiance des autorités dans les processus de production peut être affectée.

3. Mise en Place d'une politque de Data Integrity

3.1. Etat des lieux,

La première étape de tout projet consiste à réaliser un état des lieux exhaustif, notamment en ce qui concerne le niveau de Data Integrity au sein du laboratoire. Pour évaluer les équipements informatiques d'un laboratoire, un outil sous la forme d'une cotation peut être utilisé pour définir les actions prioritaires à mettre en place. L'évaluation des systèmes informatisés repose sur plusieurs catégories :

• Procédures en place : Est-ce que le système documentaire décrit de manière claire et précise l'ensemble des processus d'utilisation de l'équipement (principes d'utilisation, modalités de gestion administrative, d'archivage et responsabilités) ?

• Gestion des accès : L'accès aux équipements est-il tracé et sécurisé ?

• Qualifications des appareils : Le suivi des qualifications des équipements est-il assuré pour garantir la fiabilité des résultats obtenus ?

• Protection des données : La suppression des données ne doit pas être possible sur les équipements informatiques. Il est nécessaire de mettre en place différents niveaux de sécurité afin de limiter l'accès à certaines fonctions uniquement à des administrateurs.

• Gestion des données : L'archivage et la conservation des données doivent être définis de manière à retrouver un résultat en cas d'investigation.

• Gestion des Audit Trails : L'enregistrement, la conservation et la relecture des trails d'audit doivent être décrits pour garantir la fiabilité des résultats obtenus.

Une évaluation globale, moins détaillée, peut également être construite en amont pour cibler les points critiques en fonction des critères ALCOA+ ainsi que des actions à mener à court terme afin de résoudre les problèmes de non-respect de ces critères. Le Tableau I : Analyse préliminaire de la Data Integrity sur les équipements d'un laboratoire, ci-dessous, permet de

synthétiser tous les points du système ALCOA+ sur les équipements. Il offre la possibilité de déterminer rapidement quels appareils ne sont pas conformes aux principes de la Data Integrity ALCOA+ et identifie rapidement les efforts à fournir.

Tableau I : Analyse préliminaire de la Data Integrity sur les équipements d'un laboratoire

ALCOA+	Attributable	Legible	Contemporaneous	Original	Accurate	Complete	Consistent	Enduring	Available
Potentiomètre 1	X	O	X	X	X	X	X	X	X
Potentiomètre 2	O	X	X	X	X	X	X	X	X
Osmomètre 1	X	O	X	X	X	X	X	X	X
Balance 5	X	X	X	X	X	X	X	X	X
Spectromètre IR1	O	X	X	X	X	X	X	X	X
Spectromètre UV 1	X	X	X	X	X	X	X	X	X
HPLC / UPLC	O	X	X	X	X	X	X	X	X
Viscosimètre 2	O	X	X	X	X	X	X	X	X
Lecture de boite de pétrie	X	X	X	X	X	X	X	X	X
Lecture du LAL en gel point final	O	X	X	X	X	X	X	X	X

O : ne respecte pas ce point X : point respecté

Ce tableau montre, par exemple, que les points à travailler pour ce laboratoire concernent l'attribution des analyses et la lisibilité des résultats. Le manque d'attribution peut être dû à l'impossibilité sur les équipements d'avoir une gestion des accès (par exemple, un logiciel trop ancien et non conçu pour cette fonction). Le manque de lisibilité peut résulter de l'absence d'imprimante de tickets de mesure ou d'une impression défectueuse des tickets de mesure.

Un autre outil permet de réaliser un état des lieux plus exhaustif du niveau de risque au laboratoire : le Gap Analysis. Il évalue le risque lié à un système informatisé vis-à-vis de la Data. Il s'agit d'une analyse détaillée des processus sur chaque équipement ou processus d'un laboratoire.

Tous les points sont étudiés afin de pouvoir établir un plan d'action ainsi qu'un niveau de risque :

- Aspect documentaire : La Data Integrity d'un système passe par la description des processus d'utilisation. Un système documentaire complet permet de décrire et standardiser l'utilisation des équipements et des processus, limitant ainsi le risque d'erreur humaine et facilitant la formation des nouveaux arrivants.
- Gestion des accès : Les textes réglementaires et les guidelines décrivent les rôles et responsabilités sur les systèmes informatisés. Il est crucial de sécuriser l'accès aux données pouvant potentiellement être utilisées pour falsifier des résultats.
- Qualification des équipements : Il est essentiel de s'assurer que l'équipement est qualifié lors de son installation et qu'il est toujours dans une période de qualification valide pour garantir des résultats conformes.
- Protection des données : Les données ne doivent pas être modifiables par les utilisateurs sur les systèmes informatisés. Elles doivent être protégées contre toute modification ou suppression pour garantir l'intégrité et l'authenticité des résultats.

- Audit Trail : L’audit trail enregistre toutes les actions réalisées sur un système informatique, permettant ainsi de tracer l’ensemble des interventions effectuées par les utilisateurs. Une revue de ces audits trails permet de garantir l’intégrité des données.

Chaque élément de cette analyse est associé à un score défini en fonction des priorités de chaque site selon les points de vigilance définis. Un score global est attribué à chaque système informatisé pour classer les systèmes en fonction d’un niveau de risque, permettant ainsi de mettre en place des actions à prioriser selon les besoins du laboratoire.

3.2. Cas concret

Dans le Tableau II ci-dessous, qui représente un exemple de Gap Analysis pouvant être réalisée dans un laboratoire de Contrôle Qualité, les systèmes sont évalués selon plusieurs aspects. Cette évaluation du risque repose sur une série de critères et de questions prenant en compte les capacités des appareils ainsi que leur configuration. Dans ce cas, on constate que le densimètre répond à un plus grand nombre d'exigences que le spectromètre IR. En effet, le densimètre dispose d'une gestion nominative des accès et d'une matrice des droits, ce qui n'est pas le cas pour le spectromètre IR. Sur ce dernier, les techniciens se connectent via un compte administrateur sans restriction des droits sur les paramètres.

Tableau II : Exemple de Gap Analysis

Nom du système	Procédures	Présence d' une procédure liée au système	Gestion des accès	Gestion des accès nominatifs	Le système se verrouille-t-il après une période d' inactivité ?	Disponibilité de la matrice des droits (Fonction/ profil)	La gestion des accès est-elle revue périodiquement ?	Qualifications	Qualification Equipement disponible	Protection des données	La date et l'heure du système ne sont pas modifiables par un utilisateur ?	Les données de base du système sont-elles verrouillées pour empêcher toute modification non autorisée ?	Les données sont-elles protégées pour empêcher toute suppression ?	Le format des données est-il modifiable ?	Les données brutes sont-elles horodatées ?	La saisie manuelle des données est-elle vérifiée par une 2eme personne ?
UPLC		OUI		NON	OUI	OUI	NON		OUI		OUI	OUI	OUI	NON	OUI	OUI
CPG		OUI		NON	OUI	NON	NON		OUI		OUI	NON	NON	NON	OUI	OUI
COMPTEUR DE PARTICULES		OUI		OUI	OUI	OUI	NON		OUI		OUI	OUI	OUI	NON	OUI	OUI
DENSIMETRE		OUI		OUI	OUI	OUI	NON		OUI		OUI	OUI	OUI	NON	OUI	OUI
SPECTROMETRE IR		OUI		NON	OUI	NON	NON		OUI		OUI	NON	NON	NON	OUI	NA
COT		OUI		NON	NON	NON	NON		OUI		NON	NON	NON	NON	OUI	OUI
POLARIMETRE		OUI		NON	NON	NON	NON		OUI		NON	OUI	NA	NON	OUI	OUI
OSMOMETRE		OUI		NON	NON	NON	NON		OUI		NON	NA	NA	NON	OUI	OUI
Karl Fischer		OUI		NON	NON	NON	NON		OUI		NON	OUI	NA	NON	OUI	OUI

Nom du système	Archivage	Les données sont-elles sauvegardées ?	Les données sont-elles archivées	La sauvegarde de ce système est-elle testée périodiquement ?	% occupation des disques	Système utilise / possède une fonction de signature ?	Audit trait	Le système dispose-t-il d'une piste d' audit ?	L'audit trail est-il activé et utilisée pour ce système ?	L'audit trail est-il revu périodiquement ?	**Niveau de risque Élevé = (<50%) Modéré = 50 % - 80 % Faible = (> 80 %)**
UPLC		OUI	NON	NON	70%	NON		OUI	OUI	OUI	**76%**
CPG		NON	NON	NON	80%	NON		NON	NON	NON	**37%**
COMPTEUR DE PARTICULES		OUI	OUI	NON	3%	NON		OUI	OUI	NON	**83%**
DENSIMETRE		OUI	OUI	NON	90%	OUI		OUI	OUI	NON	**80%**
SPECTROMETRE IR		NON	NON	NON	27%	NON		NA	NA	NA	**59%**
COT		NON	NON	NON	90%	NON		NA	NA	NA	**44%**
POLARIMETRE		NA	OUI	NA	NA	NA		NA	NA	NA	**72%**
OSMOMETRE		NA	OUI	NA	NA	NA		NA	NA	NA	**72%**
Karl Fischer		NA	OUI	NA	NA	NA		NA	NA	NA	**67%**

Il arrive que certains points ne soient pas applicables en raison des capacités des appareils. Par exemple, un équipement ancien, conçu avant que la Data Integrity ne devienne essentielle dans la gestion des données, n'est pas nécessairement capable d'être configuré pour réaliser une gestion des accès ou un enregistrement d'audit trail. Pour illustrer cela, prenons le cas du laboratoire CQ de Delpharm Tours : de nombreux équipements sont aujourd'hui capables de gérer informatiquement les accès. Cependant, certains appareils plus anciens mais en parfait état de fonctionnement ne permettent pas d'avoir des fonctionnalités avancées en termes de gestion des données. C'est le cas d'une des chaînes de chromatographie en phase gazeuse (CPG) actuellement en cours de mise à niveau. Cet équipement, datant d'une vingtaine d'années, est associé à un logiciel qui ne permet pas la réalisation d'actions liées à l'intégrité des données telles que l'audit trail ou la gestion des accès. La cotation de l'analyse des écarts a permis de mettre en évidence le risque élevé que représente cet équipement, et des actions devront être entreprises pour combler les lacunes de cet équipement dans la mise en place de la Data Integrity au sein du laboratoire.

Dans ces cas, des solutions peuvent être envisagées pour pallier le manque de capacités d'un système informatisé. Si aucune solution n'est viable, la possibilité de remplacer un équipement par un modèle de nouvelle génération doit être envisagée en fonction des besoins.

Dans le Tableau III ci-dessous, vous pouvez voir la cotation associée à chacune des réponses possibles pour chaque élément. Ensuite, une formule mathématique permet de synthétiser toutes ces cotations pour obtenir un résultat exprimant le niveau de risque de chaque appareil (par le total des points obtenus divisé par le nombre de points possibles).

Tableau III : Exemple de cotation de la Gap Analysis

Procédures	
Présence d'une procédure liée au système	Oui : 3 en cours : 2 Non : 1
Gestion des accès	
Gestion des accès nominatifs	Oui : 3 Partiel : 2 Non : 1
Le système se verrouille-t-il après une période d'inactivité ?	Oui : 3 Non : 1
Disponibilité de la matrice des droits (Fonction/ profil)	Oui : 3 Non : 1
La gestion des accès est-elle revue périodiquement ?	Oui : 3 Non : 1
Qualifications	
Qualification Equipement disponible	Oui : 3 Non : 1
Protection des données	
La date et l'heure du système ne sont pas modifiables par un utilisateur ?	Oui : 3 Non : 1
Les données de base du système sont-elles verrouillées pour empêcher toute modification non autorisée ?	Oui : 1 Non : 3
Les données sont-elles protégées pour empêcher toute suppression ?	Oui : 3 Non : 1
Le format des données est-il modifiable ?	Oui : 1 Non : 3
Les données brutes sont-elles horodatées ?	Oui : 3 Non : 1
La saisie manuelle des données est-elle vérifiée par une 2eme personne ?	Oui : 3 Non : 1
Archivage	
Les données sont-elles sauvegardées ?	Oui : 3 Non : 1
Les données sont-elles archivées	Oui : 3 Non : 1
La sauvegarde de ce système est-elle testée périodiquement (avec une fréquence définie) ?	Oui : 3 Non : 1
% occupation des disques	<20% : 3 <50 % : 2 >80% : 1
Système utilise / possède une fonction de signature électronique en place ?	Oui : 3 Non : 1
Audit trait	
Le système dispose-t-il d'une piste d'audit ?	Oui : 3 Non : 1
L'audit trail est-il activé et utilisée pour ce système ?	Oui : 3 Non : 1
L'audit trail est-il revu périodiquement ?	Oui : 3 Non : 1
Niveau de risque : > 80 % = Faible ; entre 50 % et 80% = Modéré ; < 50 % Elevé	

La finalité de cette Gap Analysis est de classer les différents équipements du laboratoire selon qu'ils soient jugés à risque élevé, modéré ou faible. Un équipement classé « Faible », c'est-à-dire avec un niveau « satisfaisant » sur les protocoles en lien avec la Data Integrity, demandera moins de travail et d'investissements afin qu'il satisfasse tous les critères souhaités pour être conforme aux exigences et aux réglementations par rapport à un équipement classé « élevé ».

Ce document permet également, lors de la revue des audits client ou des inspections par les autorités du médicament, de justifier de l'avancement de la mise à niveau des équipements du laboratoire ainsi que de l'avancement des projets.

Cette étude permet d'expliquer, lors d'audits ou lors d'inspections, que les faiblesses concernant la Data Integrity au laboratoire sont connues et que des travaux sont en cours afin de les combler et de les résoudre. Par exemple, il n'est pas possible de faire de la gestion des accès nominatifs sur la majorité des équipements électroniques du laboratoire. Ainsi, le suivi des utilisations par des logbooks papier est la solution permettant de pallier à ces défaillances sans nécessité d'investir dans un équipement plus récent ayant plus de fonctions de sécurité.

Une fois l'état des lieux effectué, il est nécessaire de lister les actions à réaliser afin d'améliorer la conformité du laboratoire en termes d'intégrité des données. L'état des lieux permet de cibler les actions à réaliser sur des critères logiques (système de cotation, capacité des équipements). La mise en place de ces actions est parfois ralentie par la complexité de celles-ci ou par les coûts que les modifications vont engendrer.

Il est nécessaire de rédiger un plan d'action prenant en compte ces critères afin de permettre à un laboratoire ou à une industrie d'anticiper les frais (financiers et humains) que les actions vont demander pour être mises en place.

4.1. Plan d’action

Le but du plan d’action est de lister et de prioriser les actions à mener, par équipement ou par processus, pour réduire le niveau de risque des équipements (traduit par une augmentation du score « niveau de risque » de la Gap Analysis).

Il permet également d’établir un calendrier opérationnel ainsi que les délais pour chaque action à mener, en fonction des ressources allouées pour leur mise en place.

Dans l'exemple du plan d’action (Tableau IV, plan d’action du densimètre), on remarque que l’avancement des actions est différencié et coté avec un système de pourcentage (0%, 25%, 50 %, 75 % et 100 %). Il est nécessaire de déterminer comment évaluer l’avancement des actions. Par exemple, concernant l’avancement de la mise à jour d’une procédure ou de la rédaction d’un protocole de validation des accès, j'utilise ces critères :

• 0 % : aucune avancée ;

• 25 % : mise à jour / projet débuté / procédure initiée / … ;

• 50 % : procédure / protocole rédigé(e) et en cours de relecture / projet au stade d’implémentation ;

• 75 % : procédure / protocole relu(e) et en cours de signature / Projet au stade de signature des rapports ;

• 100 % : procédure / protocole signé(e) / projets clôturés.

Tableau IV : Exemple de plan d'action : le Densimètre

SYSTÈME	THEME	ACTION	GAIN PROCESSUS	DIFICULTE MISE EN ŒUVRE	RESPONSABLE	DATE D'EMISSION	DATE CIBLE	AVANCEMENT ACTION	DATE DE CLOTURE	REMARQUE
DENSIMETRE	Gestion des accès	> Créer des comptes	Modéré	Faible	J. SIMON	01/09/2023	31/12/2023	100%	10/09/2023	NA
		> Définir les droits utilisateurs	Modéré	Faible	J. SIMON	01/09/2023		100%	10/09/2023	NA
		> Rédiger un protocole de validation des droits utilisateur	Modéré	Modéré	J. SIMON	01/09/2023		25%		
		> Tester les droits définis	Elevé	Modéré	J. SIMON	01/09/2023		0%		
	Paramétrage système	>Activer l'audit trail	Elevé	Faible	J. SIMON	01/09/2023		50%		
	Archivage	> Mettre à jour la procédure du système	Modéré	Modéré	J. SIMON	01/09/2023		100,00%	21/09/2023	Procédure à jour
	Connexion au réseau	> Relier le densimètre au réseau informatique	Elevé	Elevé	J. SIMON	01/09/2023		0%		

Ce plan d’action permet de prioriser les actions à réaliser en fonction d’une cotation tenant compte de la difficulté de mise en œuvre ainsi que du bénéfice que l'action apportera pour réduire le niveau de risque sur un équipement. La difficulté de mise en œuvre est évaluée selon le temps nécessaire à l'action ou la quantité de ressources exigées (financières ou humaines).

Les actions facilement réalisables et ayant un gain élevé seront prioritaires. Paramétrer de nouveaux comptes ou établir une matrice des droits est plus simple que mettre en place un système de sauvegarde automatique ou de revue des audits trails.

Ce plan d’action permet également d’anticiper les investissements futurs du laboratoire. Certains équipements ne disposent pas de logiciels permettant certains contrôles de sécurité, comme la gestion des accès ou de l'archivage informatique. Bien que la mise en place de documents tels que des logbooks ou la gestion d'un archivage papier soit conforme aux principes ALCOA+ et au 21 CFR part 11 [5], une gestion sécurisée informatiquement est préférable et fait partie de l'amélioration continue des pratiques. La sécurisation des données nécessite une gestion plus rigoureuse de ces éléments. Ainsi, la mise à niveau de ces équipements exige l'achat d'options sur les logiciels existants ou le remplacement complet du logiciel pour sécuriser toutes les étapes de la gestion des données. Évaluer la capacité des équipements à répondre ou non aux exigences liées aux principes ALCOA+ permet d'anticiper les demandes d'investissements du laboratoire sur plusieurs exercices. Par exemple, un équipement avec un logiciel trop ancien n'a pas permis la mise en place d'un protocole de contrôle d'accès avec une restriction des droits pour les techniciens ni l'enregistrement d'un audit trail. Pour réduire le niveau de risque de cet équipement, un investissement dans la mise à jour du logiciel sera nécessaire.

Ce plan d’action permet également de suivre l'avancement des actions menées et à mener. Ce suivi, conjointement avec la mise à jour régulière des informations contenues dans la Gap Analysis, témoigne de l'évolution du laboratoire vers une gestion plus sécurisée des données. En matière d'audits clients ou d'inspections, le plan d'action et la Gap Analysis

garantissent l'amélioration du laboratoire sur des domaines particulièrement surveillés aujourd'hui.

Le plan d'action met en évidence les capacités du laboratoire en fonction du rapport gains/investissements. Certaines actions sont simples à mettre en place et offrent des gains de processus importants, tandis que d'autres nécessiteront d'être traitées en mode "projet" (personnel dédié, demande d'investissement financier, relation interservices, groupe de travail, etc.).

Reprenons l'exemple de la chaîne chromatographique CPG : le plan d'action a permis d'identifier qu'une mise à jour du logiciel était nécessaire pour mettre en place des sécurités liées à l'intégrité des données. Aujourd'hui, une mise à jour a été effectuée permettant l'enregistrement d'un audit trail ainsi que la mise en place d'une gestion des accès.

Pour la mise en place de certaines des actions identifiées, des outils sont disponibles afin d'assurer une amélioration du niveau de risque dans la gestion des données.

5. Les outils de mise de niveau de la Data Integrity au sein d'un laboratoire de contrôle Qualité

5.1. La gestion des accès aux systèmes informatisés

L'un des points les plus simples à mettre en œuvre et très sécurisant en termes de gestion des données est la mise en place d'une politique de gestion des accès.

Conformément aux textes réglementaires et aux principes ALCOA+, un technicien ne doit pas avoir accès aux fonctions "sensibles" des appareils (paramètres, gestion des comptes, gestion des méthodes et des projets, etc.), mais doit pouvoir réaliser des analyses. Un administrateur ne doit pas avoir la possibilité de mener une analyse mais doit avoir les droits pour la gestion administrative du système. Il est possible que des comptes mixtes existent, permettant de gérer des fonctions sensibles de l'appareil, telles que les paramètres opérationnels

des méthodes d'analyses. De plus, chaque personne doit avoir un compte nominatif lié à un mot de passe personnel, permettant de tracer la personne ayant réalisé une modification ou une analyse lors de l'enregistrement de l'audit trail.

Pour répartir l'ensemble des intervenants sur un équipement, il est possible de se baser sur un système à différents niveaux de profils permettant différentes actions. Tous les équipements ne sont pas systématiquement concernés par tous les niveaux, néanmoins, les comptes "Administrateur" et "Opérateur" doivent être présents et avoir des fonctions distinctes. Voici quelques exemples de niveaux d'accès possibles :

Administrateur : Ce type de profil, contrairement aux recommandations, conserve tous les droits sur le logiciel. Pour pallier à cela, lors des revues des audits trails, une étude des actions de l'administrateur sera effectuée. Ce compte ne doit être dédié qu'à la gestion administrative des systèmes. Toutes les actions ne répondant pas à un besoin administratif devront être justifiées. Idéalement, les personnes nommées comme administrateur d'un système ne doivent pas avoir de lien direct avec ledit système. Au laboratoire de Contrôle Qualité, l'administrateur ne doit pas être une personne réalisant des analyses et, si possible, ne doit pas avoir d'intérêt pour les résultats. Par exemple, il est préférable que les administrateurs soient externes au service, des personnes des services informatiques plutôt que des responsables de laboratoire qui consultent et libèrent des résultats. Dans les faits, s'il est prouvé et démontrable, par le moyen de validation des droits d'accès aux équipements et par des revues d'audit trail, que les comptes Administrateurs n'ont pas intervenu (sauf de manière tracée) dans l'obtention des résultats, il est possible d'accorder des droits d'administration aux responsables du laboratoire.

Administrateur méthodes ou opérateur supérieur : Il s'agit d'un profil équivalent à des « Key-User » ou des Superviseurs. Les personnes bénéficiant de ce statut sont des techniciens formés sur la gestion des projets. Ils ont des droits similaires aux administrateurs sur la gestion opérationnelle mais ne sont pas habilités à réaliser des actions en lien avec la gestion administrative des appareils. Ces personnes sont généralement des techniciens de laboratoire

ayant reçu des formations supplémentaires sur les équipements. Ces profils sont uniquement présents pour de la gestion opérationnelle et il n'est pas faisable de lancer une analyse ou de retraiter des données. Ces profils sont également sollicités pour réaliser de la gestion des données telles que de l'archivage.

Opérateur : Il s'agit du profil destiné aux techniciens afin qu'ils puissent réaliser les analyses. Les droits utilisateurs sont restreints afin que les techniciens n'accèdent pas aux paramètres administratifs des appareils (la gestion des accès) et aux paramètres opérationnels (la gestion des projets et des méthodes). Les techniciens n'ont également pas accès à la gestion des données, ils doivent avoir des droits restreints sur l'archivage, ils peuvent réaliser des archives mais ne peuvent pas retirer des données des archives ni les supprimer (en théorie, personne ne doit être en capacité de supprimer définitivement une donnée). Une personne ayant un compte opérateur peut avoir un compte d'administrateur méthode mais les deux comptes doivent être distincts et utilisés de façon à ce que les actions faites avec chaque profil soient clairement définies.

Techniciens de maintenance : Lorsque les équipements le permettent, il est possible de définir des comptes spécifiques à la maintenance des appareils. Cela permet, si une personne externe au laboratoire vient pour réaliser des opérations de maintenance, de suivre les actions menées. Ces comptes ne doivent pas restreindre l'accès aux paramètres des équipements ni à la partie opérationnelle de ceux-ci, mais des restrictions peuvent être mises en place sur l'accès aux données des analyses. Une restriction sur l'enregistrement, l'archivage, la modification ou la suppression des données existantes peut être mise en place afin de s'assurer qu'aucune action ne pourra les altérer.

Personnel Informatique : Ce profil n'a aucun intérêt dans l'obtention des données et permet une gestion administrative des données. Il est intermédiaire au rôle d'administrateur, il a seulement accès à la sauvegarde des données en tant que garant de la sécurité informatique d'un site industriel.

5.2. Protocole de Validation de la matrice des droits

Tous les profils définis doivent être validés par le biais de protocoles de validation (sous la responsabilité du service propriétaire de l'équipement ou du service Qualification/Validation). L'avantage de ce service est qu'il n'a pas de lien avec l'équipement et offre donc un avis factuel sur les rôles et responsabilités de chacun. La rédaction des protocoles de validation des droits, permettant de justifier la restriction d'accès à certaines fonctions pour certains profils, suit dans le projet. Les protocoles sont nécessaires pour prouver que des mises à jour ont été effectuées et validées conformément aux exigences des principes de la Data Integrity. Ils peuvent donc être présentés lors d'audits ou d'inspections pour permettre de justifier une gestion des accès contrôlée.

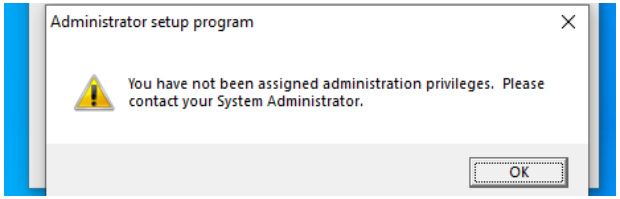
Le rôle de ces validations est de justifier l'incapacité pour certains profils de réaliser des tâches qui ne sont pas censées être effectuées. Le fait de prouver que les droits censés être bloqués sont inaccessibles pour la personne définie offre l'avantage de diminuer la charge de travail lors de la revue des audits trails.

Afin de rédiger le protocole, il est nécessaire de détailler le cheminement des actions à réaliser pour justifier de la non-disponibilité d'un droit. Il est admis qu'un droit est bloqué à partir du moment où la réalisation de la séquence d'action est stoppée par l'impossibilité de poursuivre à un moment donné de la série d'actions (par exemple : case à sélectionner inexistante ou non sélectionnable) ou si à la suite de la réalisation de la séquence complète aucune action n'est lancée. Le résultat attendu doit être de ne pas pouvoir accomplir une action bloquée par un droit non attribué.

Sur l'extrait d'un rapport de validation (Tableau V), les droits listés dans la première colonne ne doivent pas être disponibles pour l'utilisateur (ici, il s'agit des droits que le profil « opérateur » ne doit pas pouvoir avoir). En ce qui concerne la validation des droits des techniciens, il ne doit pas être permis d'accéder aux paramètres des méthodes d'analyse ni de les supprimer. Pour chaque droit non disponible, le chemin d'accès pour effectuer une action en lien avec ce droit est décrit par le protocole, ainsi que le résultat attendu si ce droit est

effectivement bloqué. Dans l'exemple ci-dessus, il est bien impossible pour le technicien de sauvegarder une méthode ou d'enregistrer des changements de paramètres. Les captures d'écran des fonctionnalités absentes ou bloquées sont insérées dans les rapports de validation comme preuve de la restriction des accès d'un profil à ces actions.

Tableau V : extrait d'un rapport de validation

Droit	Fonctions	Résultats attendus	Conforme	Preuve / capture d'écran	Notes / Observations
Enter the Reason for Change Reason	Application « Administration setup program » Set administration Set Reason text	Application non accessible aux techniciens	☒		NA
Open Method	Edit Method	Bouton grisé	☒		NA
Save Method	Edit Method	Bouton grisé	☒		Pas accès de base aux méthodes

Cette gestion informatique des accès permet également de suivre les connexions et les actions réalisées par les utilisateurs sur le logiciel via les audits trails. La gestion et la restriction des accès offrent un contrôle sur les individus autorisés à intervenir dans les analyses d'un produit. Un contrôle d'accès sur un équipement permet de tracer qui a effectué une opération et à quel moment, dans le but de garantir la validité d'une analyse (personne correctement formée, absence de possibilité de falsification des résultats, impossibilité d'antidater une analyse, etc.).

Comparé à un suivi des accès sur papier à l'aide de logbooks, la gestion informatique permet de limiter les fonctions accessibles à certaines personnes. L'analyse de l'audit trail permet de reconstituer la chronologie d'une analyse, de suivre la séquence des actions effectuées lors de cette analyse, afin d'identifier les causes d'un écart ou de prouver que tout a été réalisé conformément aux protocoles et aux méthodes validées.

5.3. Revue générale des accès

Pour être conforme aux exigences règlementaires relatives à la gestion des accès, une revue périodique des comptes et des droits qui leur sont associés doit être effectuée. Cette revue vise à suivre les mouvements de personnel au sein du laboratoire (changement de poste, départ de personnel, arrivée de nouveaux employés), ainsi que toute modification éventuelle des droits accordés aux différents profils.

La revue des accès se concentre sur la partie administrative des appareils, et chaque compte est analysé pour vérifier si l'utilisateur dispose des droits adéquats en fonction de ses missions. De plus, une vérification des matrices programmées est effectuée afin de garantir leur conformité avec les matrices validées dans les procédures en vigueur. Cette revue constitue également une occasion de s'assurer que tous les comptes disponibles sont attribués à des personnes travaillant effectivement sur l'équipement. Cela permet de désactiver (ou de supprimer, le cas échéant) les comptes qui ne sont plus utilisés. Toutes les modifications apportées aux matrices et aux listes des comptes doivent être consignées. Elles peuvent être documentées via des formulaires, justifiant ainsi la nécessité de modifier les droits d'accès pour un groupe de personnes.

Toute modification des accès doit être validée par le responsable de l'équipement. De plus, toutes les modifications apportées aux matrices et aux listes des comptes doivent être suivies d'une mise à jour de la documentation associée à l'appareil (par exemple : procédures, validation des nouveaux droits, ...).

5.4. Double réalisation d'une analyse

La gestion des accès est un moyen de sécuriser l'accès aux résultats obtenus via un logiciel informatique ou un système informatisé. De nombreuses analyses réalisées au sein des laboratoires de contrôle qualité physico-chimique et microbiologique sont obtenues via des contrôles "manuels". Les données qui en résultent sont des "*paper data*" et ne sont pas sécurisées. Par exemple, les résultats issus d'un comptage de colonies sur des géloses (pouvant garantir la stérilité d'une zone de production dans le cadre des contrôles de l'environnement de travail) ou les résultats obtenus via un titrage par colorimétrie effectué à l'aide d'une burette graduée.

Les outils utilisés pour obtenir ces résultats ne permettent pas de sécuriser les données. Comment s'assurer alors que le résultat n'a pas été falsifié ?

Une solution pour sécuriser les résultats et fournir des données fiables est la double réalisation des analyses.

Dans le cas ou des analyses ne peuvent pas être tracée informatiquement celles-ci peuvent être réalisées en double par deux personnes différentes à deux moments distincts. Cela permet de détecter les éventuelles erreurs commises par l'une des deux personnes. Dans le cas de résultats des 2 essais différents, une troisième personne effectue l'analyse pour déterminer le résultat conforme. Si le troisième résultat diffère significativement des deux autres, une enquête peut être initiée afin de déterminer la cause fondamentale de la mauvaise répétabilité de l'analyse.

Les doubles réalisations des analyses permettent également de prévenir la falsification des données. Les analyses étant réalisées de manière indépendante par deux personnes

différentes, cela élimine le risque de modification et de falsification des résultats, qu'ils soient intentionnels ou non.

Il est possible de déterminer si une analyse doit être réalisée en double en effectuant une analyse de risque répondant à plusieurs questions sur la façon dont les données brutes sont obtenues :

- Les données brutes sont-elles imprimées sur un ticket ? Si oui, le résultat est plus sécurisé que s'il est lu puis retranscrit dans un cahier de laboratoire.
- Les résultats peuvent-ils être interprétés différemment selon la personne les lisant ? La comparaison d'une solution colorée par rapport à une gamme de couleurs est très subjective. Par exemple, dans le cas d'un test LAL (détection d'endotoxines à l'aide d'une solution se gélifiant en présence d'un certain taux d'endotoxine), si un résultat est sujet à des interprétations différentes selon les personnes, il peut être nécessaire de mettre en place une double réalisation des analyses afin de limiter le risque d’obtenir une non-conformité à cause d’une erreur d’interprétation.

- Les données brutes sont-elles disponibles pour être vérifiées ? Par exemple, le comptage manuel du nombre de colonies sur une gélose peut être réalisé par deux personnes sur la même gélose. Il n'est pas nécessaire de réaliser l'analyse deux fois.

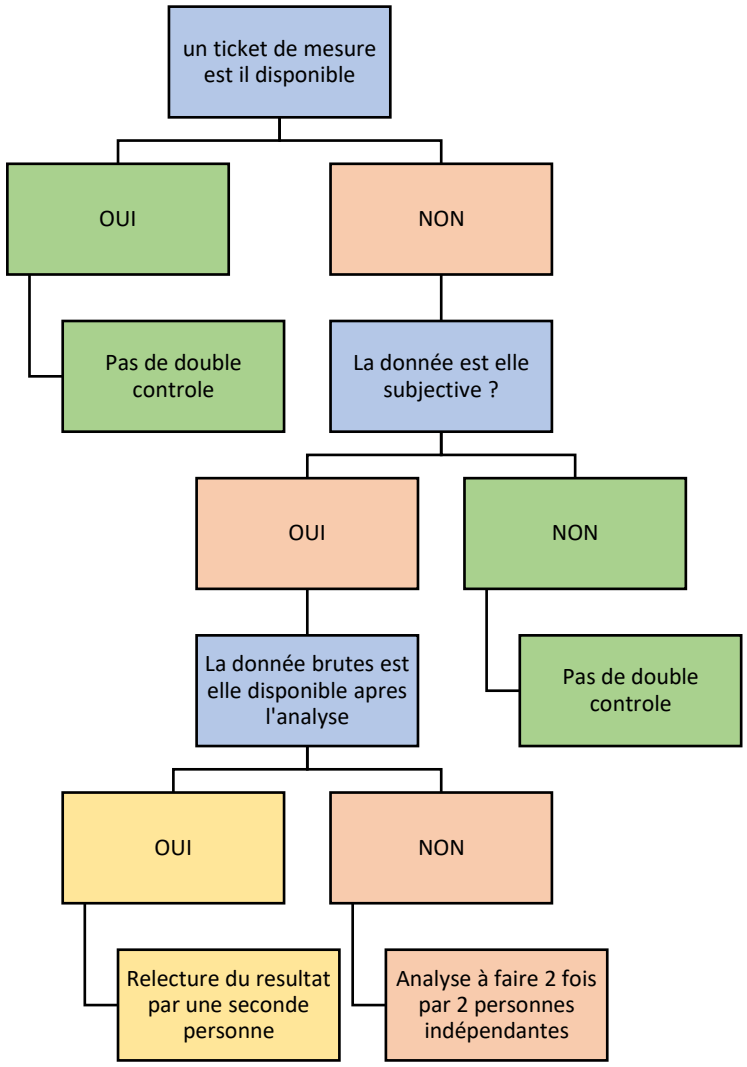


Figure 2 : Arbre décisionnel servant à déterminer la nécessité d'un double

À l'aide d'un arbre décisionnel (Figure 2), il est possible de déterminer si le double contrôle est nécessaire ou non.

Cet arbre décisionnel permet de classer les analyses manuelles en 3 catégories :

- Faiblement risqué : aucune double analyse nécessaire, le résultat est sûr et n'est ni interprétable ni falsifiable ;
- Moyennement risqué : Faire 2 analyses par 2 techniciens peut être nécessaire afin de vérifier qu'il n'y ait pas d'interprétations possibles du résultat ;
- Fortement risqué : L'analyse est interprétable et non vérifiable, il est donc nécessaire de la réaliser 2 fois afin de limiter le risque d'erreur et de falsification.

Une manière plus facile à mettre en œuvre dans le cadre d'analyses tracées à l'aide de ticket ou de données brutes est de double vérifier les résultats. La personne vérificatrice reprend les données brutes de l'analyse obtenue par le premier technicien (qui a déjà vérifié ses résultats) et vérifie l'ensemble des données. Cela passe par le contrôle des outils utilisés :

- Date de validité des instruments utilisés (par exemple : date de la dernière qualification)
- Date de péremption des réactifs et autres produits utilisés lors des manipulations ;
- Matériel adapté à la manipulation (géloses du bon type, balances adaptées aux pesées, type de colonne HPLC décrite dans la méthode analytique, …).

La double vérification des calculs permet également de réduire le risque d'erreur. L'ensemble des données doivent être datées et signées, soit par les 2 techniciens ayant réalisés les analyses de façon indépendante, soit par le technicien à l'origine des données brutes et des premiers résultats, ainsi que par le second technicien responsable de la vérification.

Cette double vérification, bien que moins sécurisée que le suivi des données par des audits trails, est un moyen efficace d'améliorer l'intégrité des données issues des "*Paper data*". Cela nécessite néanmoins un investissement plus important en termes de temps humain, car le temps d'analyse est doublé.

5.5. La supervision

La supervision est un principe décrit dans les BPF [4]. Il ne s'agit pas simplement d'une vérification des résultats comme mentionné dans le point précédent. La supervision des analyses englobe tous les aspects d'une analyse et représente la dernière étape avant la libération analytique d'un lot.

Pendant la supervision, en plus de la revue générale des données brutes telles que la vérification des calculs manuels, des méthodes et des réactifs utilisés il y a également la vérification de l'intégralité des données nécessaires à la libération d'un lot. L'aspect documentaire est vérifié durant cette étape. Toutes les données obtenues sont passées en revue : présence des tickets de mesure (le cas échéant), signatures complètes des techniciens, concordance des données avec celles saisies dans le dossier, présence des certificats matières si nécessaire (par exemple, les témoins utilisés doivent être accompagnés de certificats s'ils sont certifiés par la Pharmacopée Européenne).

Dans certains cas, c'est également lors de la supervision que la revue des audits trails peut être effectuée afin de vérifier l'absence de modification des paramètres d'une machine avant l'obtention d'une analyse.

En plus de la vérification opérationnelle des analyses, la supervision s'attarde également sur la conformité documentaire. Une fois tous les points conformes, tant au niveau analytique que documentaire, la personne responsable de la libération peut autoriser la validation de l'analyse. Cette série de vérifications vise à sécuriser l'obtention des données brutes avant la libération des analyses :

- Le technicien vérifie son analyse ;
- Le vérificateur contrôle les données brutes ;
- Le superviseur effectue les vérifications documentaires ;
- Le libérateur effectue une revue générale des résultats et des documents contenus dans le dossier analytique.

Comme évoqué, l'une des missions du superviseur est de vérifier les méthodes utilisées ainsi que le traitement des données. Comme mentionné en introduction, le scandale des laboratoires Able trouve son origine dans le manque de sérieux du laboratoire de Contrôle Qualité concernant la traçabilité des résultats. Tous les niveaux étaient impliqués dans les falsifications et les écarts ont pu être mis en évidence grâce à la revue des enregistrements électroniques.

5.6. Revu des audits trails

Un audit trail est un enregistrement électronique sécurisé, généré automatiquement et horodaté, permettant de reconstituer le déroulement des événements liés à la création, la modification ou la suppression d'un enregistrement. Ils peuvent se décomposer en un audit trail opérationnel enregistrant la création, la modification ou la suppression des données et en un audit trail administratif enregistrant les actions propres au système telles que les heures de connexion ou la modification des paramètres généraux, par exemple. L'audit trail est l'outil de référence pour répondre aux principes ALCOA (Attribuable, Contemporaneous, Original et Accurate).

L'objectif de réviser ces audits trails est de vérifier que chaque action est identifiée et tracée. Il doit être possible de retrouver qui est responsable de l'action et quand elle a été effectuée. Dans le meilleur des cas, il doit aussi être possible de retrouver pourquoi cette action a dû être réalisée (par le biais de commentaires devant être laissés par l'utilisateur en cas de modification de certains paramètres, mais seuls certains systèmes informatisés dotés de logiciels complexes permettent cette fonction).

Le processus de revue de l'audit trail opérationnel se base sur une analyse de risque. Il peut consister en l'analyse des modifications faites dans une méthode d'analyse ou en l'étude des résultats obtenus suite aux différents retraitements des données.

La revue de l'audit trail administratif consiste à vérifier la configuration du système : ajout d'utilisateur, modification des profils d'utilisateurs, droits des utilisateurs (consultation,

modification, administration), paramètres de configuration de l'application (system policies, etc.) et les opérations concernant des dossiers administratifs (gestion des accès).

Les appareils utilisés au laboratoire ayant la possibilité d'enregistrer un audit trail ne sont pas tous paramétrables de la même manière. Il n'est néanmoins pas toujours nécessaire de revoir ces audits trail systématiquement. En effet, ces revues sont souvent lourdes et demandent un investissement humain important. Il est donc nécessaire de justifier la nécessité de réaliser cette revue sur les systèmes informatiques par le biais d'une analyse de risque. La monographie USP <1058> [10] classe les équipements d'un laboratoire selon leur complexité, et cette monographie peut servir de base à la rédaction d'une analyse de risque adaptée aux besoins de chaque laboratoire.

La complexité des équipements peut être pondérée par plusieurs facteurs liés à l'activité propre du laboratoire :

- La fréquence d'utilisation de l'équipement : un équipement très peu utilisé représente un risque plus faible sur l'ensemble d'un laboratoire qu'un équipement servant quotidiennement. En cas de défaut sur l'équipement, si celui-ci est utilisé très fréquemment, le nombre d'analyses potentiellement impactées est plus élevé. On peut citer l'exemple d'une chaîne HPLC utilisée 5 fois par semaine, permettant de réaliser des dosages ainsi que le taux d'impureté de 10 produits pharmaceutiques par semaine. Si la méthode utilisée ou le logiciel administratif est corrompu, l'impact sur les investigations en cas de litige sera bien plus grand que sur un équipement servant à analyser 2 produits par an. L'importance de la fréquence d'utilisation dans cette analyse de risque permet de justifier une revue fréquente ou non des audits trails.
- La criticité des résultats : si on reprend l'exemple d'une chaîne HPLC, les résultats obtenus sont directement liés à la qualité et à la sécurité des produits de santé, ainsi qu'à la sécurité du patient.
- Le nombre d'interventions humaines lors de l'obtention des résultats : il est nécessaire de contrôler les données fournies par l'Homme. Toujours avec l'exemple de l'HPLC, il

est possible d'intégrer les chromatogrammes de manière automatique ou manuellement. Le risque d'erreur de l'intégration automatique est plus faible que lors de l'intégration manuelle, qui est plus subjective (il est de plus en plus fréquent que lors d'inspections, les autorités de santé demandent à limiter l'usage des intégrations manuelles des chromatogrammes et de devoir justifier son utilisation si cela est nécessaire). Selon l'usage, il ne sera pas défini la même fréquence de vérification des résultats.

- Le type d'analyse : ce critère reprend les caractéristiques des résultats. Si les instruments permettent de faire une mesure sans traitement de données, il est moins critique qu'un équipement donnant un résultat issu de calcul. On peut prendre l'exemple d'un spectromètre UV servant à mesurer l'absorbance d'un matériau sans calcul, contrairement à une SAA (Spectroscopie d'Absorption Atomique) prenant en compte plusieurs paramètres tels que la quantité de solution vaporisée ou la nature de la flamme. Par exemple, ce paramètre peut influencer la cotation d'équipement pourtant classer de la même manière dans la monographie de l'USP <1058> (Tableau VI). La SAA pourrait être "plus critique" qu'un simple spectromètre infrarouge, alors que ce sont des équipements fournissant des résultats basés sur le même principe théorique.

Tableau VI : Classification des équipements analytiques selon la monographie 1058 de l'USP

Category	Classification	Qualification Approach	Some Examples
A Low Risk	**Standard equipment,** no measurement capability or requirements for calibration	Conformance with requirements verified and documented by observation of operation.	▪ Magnetic stirrers ▪ Vortex mixers ▪ Sonic baths ▪ Shakers ▪ Class A Pipettes ▪ Nitrogen Evaporators
B Medium Risk	**Standard instruments** with measurement values or control physical parameters	User requirements typically within unit functions. Require calibration. Conformance to requirements via SOPs, Calibration Verification / Certificates, and IQ/OQ.	▪ Balances ▪ pH Meters ▪ Thermometers ▪ Timers ▪ Pumps ▪ Water baths ▪ Centrifuges ▪ Light Microscopes ▪ Variable Pipettes
C High Risk	**Complex instruments** and computerized systems	Full qualification process required. Specific function and performance tests	▪ HPLC, LCMS, GC, GCMS ▪ ICP-MS, AA, Analyzers ▪ Dissolution, UV/Vis ▪ Particle Analyzers, Densitom. ▪ Robotic Systems ▪ FTIR, DSC, TGA, SEM, TEM ▪ Autoclaves, Stability Chamb. ▪ Refrig, Freezers, Incubators

Une fois les critères définis, une grille de cotation permettra de définir les équipements critiques d'un laboratoire en fonction des analyses.

Dans le Tableau VII en exemple ci-dessous les critères choisis sont

- La criticité selon l'USP 1058 [10]
- La présence d'un audit trail sur l'équipement. Ce point est présent afin de mettre de cote les équipements n'ayant pas la possibilité de garder en mémoire des audits trails. Ces équipements pourront faire l'objet d'étude visant à définir si une mise à niveau de ceux-ci est nécessaire
- La fréquence d'utilisation
- Le type de données fournies

Tableau VII : Grille de cotation utilisé pour coter les équipements du laboratoire pour la revue des audits trails

		USP 1058 (C =10 ; B = 5 ; A = 1)	10		5		1	
		Type d'analyse (retraitement des données = 8 ; acquisition simple = 1)	8	1	8	1	8	1
Présence d'un AT (1 = oui ; 0 = non)	fréquence d'utilisation (1 fois / jour = 3 ; ≥1 fois / sem = 2 ; <1 fois / sem =1)		80	10	40	5	8	1
1	5	5	400	50	200	25	40	5
	3	3	240	30	120	15	24	3
	1	1	80	10	40	5	8	1
0	5	0	0	0	0	0	0	0
	3	0	0	0	0	0	0	0
	1	0	0	0	0	0	0	0

≥ 200 pts	Haute criticité
200 pts > X ≥ 50 pts	Criticité moyenne
< 50 pts	Peu critique
0 pt	Pas d'AT

Une fois la grille de cotation finalisée, il est nécessaire de déterminer la signification de chaque score :

Les appareils jugés critiques (score ≥ 200) verront leurs audits trails revus fréquemment selon les besoins. Il est possible de déterminer que ces audits trails doivent être revus avant la libération analytique des résultats fournis par l'équipement.

- Les appareils avec une criticité moyenne (score entre 50 et 200) verront leurs audits trails revus lors de la requalification périodique.
- Les audits trails des appareils jugés non critiques (score < 50) ne seront pas revus, mais ils seront enregistrés et archivés.
- Les appareils sans possibilité d'enregistrer un audit trail (score nul) seront, pour certains, mis à jour ou remplacés afin de permettre de répondre aux exigences de Data Integrity.

Tableau VIII : Cotation des équipements du laboratoire pour la revue des Audits trails

Appareil présent au laboratoire	Présence d'un AT	Complexité de l'appareil (USP 1058)	Fréquence d'utilisation	Sensibilité des données / type d'analyse	Score	Criticité
HPLC	1	10	5	8	**400**	**Haute**
CPG	0	10	3	8	0	**Pas d'AT**
COMPTEUR DE PARTICULES	1	10	5	1	**50**	**Moyenne**
DENSIMETRE	1	10	5	1	**50**	**Moyenne**
SPECTRO IR	1	5	5	1	0	**Basse**
SPECTRO UV	0	10	5	1	0	**Pas d'AT**
VISCOSIMETRE	1	5	3	1	15	**Basse**
COT	0	10	5	1	0	**Pas d'AT**
LECTEUR MICROPLAQUE	1	10	1	8	**80**	**Moyenne**
PTS	1	10	1	8	**80**	**Moyenne**
SAA	1	10	3	8	**240**	**Haute**
POTENTIOMETRES	0	5	5	1	0	**Pas d'AT**

Le tableau ci-dessus (Tableau VIII) présente la criticité des appareils en fonction des scores obtenus. Il met également en évidence certains investissements à prévoir pour certains appareils. On peut citer la CPG ou le Spectromètre UV, cotés pourtant B ou C selon la monographie de l'USP 1058 [10], mais qui ne fournissent pas la possibilité d'enregistrer un audit trail. Des investissements (mises à jour ou changements d'appareils) pourront donc être envisagés en fonction des besoins pour permettre d'avoir une traçabilité via un audit trail sur ces équipements. Ces dispositifs fournissent des données sensibles pouvant affecter la qualité et la sécurité d'un médicament en cas de falsification des résultats.

5.7. Comment revoir les audits trails ?

Sur les audits trails sont enregistrées toutes les opérations effectuées sur un appareil ou un logiciel. Toutes ces informations ne seront pas nécessairement revues. Seules les actions jugées critiques seront vérifiées lors de la revue des audits trails. Les actions jugées critiques enregistrées par les appareils sont décrites dans des protocoles associés à la revue des audits trails spécifiques sur un appareil.

Les appareils permettent de différencier différents types d'utilisateurs avec des droits différents (Administrateur ou Utilisateur). En règle générale, les comptes ayant des droits d'administrateur sont destinés à la gestion des systèmes. Ils ne doivent pas être utilisés pour réaliser des analyses ou retraiter des données. Dans le cas où les appareils permettent de définir une matrice des droits, lors de la revue des audits trails, toutes les actions réalisées par un compte administrateur seront contrôlées (absence de lancement d'une analyse, modification des paramètres du système, absence de suppression de données, création ou modification de méthodes, …). Sur ces appareils, les comptes utilisateurs ont des droits restreints sur la gestion des paramètres des systèmes ainsi que sur la gestion des projets.

Lors de la revue des audits trails, les actions relatives à la modification de méthodes (ou modification de projets), les actions relatives à la gestion des accès et des paramètres du système seront vérifiées. L'absence d'actions de suppression ou modification des données est contrôlée.

Revue des Audit trail sur les appareils de criticité Haute

D'après le tableau ci-dessus, les systèmes HPLC et la SAA sont classés comme fortement critiques. Ces appareils sont complexes dans leur utilisation et leur paramétrage. Les HPLC sont les systèmes les plus utilisés dans les laboratoires. Les logiciels permettant de piloter ces appareils sont également très paramétrables et donc plus sujets à l'erreur. Un contrôle plus régulier de l'audit trail de ces appareils est justifié. L'audit trail administratif doit donc être revu périodiquement. Lors de cette revue, les points critiques liés au management système sont vérifiés. Il est vérifié les points critiques liés management du système. Lors de cette vérification, on revoit les points liés à la gestion des accès (création/modification de compte/profil), la création ou la modification de projet et les modifications des paramètres de base du système. Les points revus sont justifiés par le fait qu'ils peuvent avoir un impact sur les données selon les Principes ALCOA.

Les audits trails opérationnels peuvent être revus avant chaque libération des résultats. Lors des opérations de supervision, l'audit trail opérationnel sera revu pour s'assurer que les informations relatives aux méthodes ou à l'analyse soient bien tracées et qu'aucune donnée n'a été effacée, permettant ainsi de répondre au principe ALCOA « Accurate ».

Revue des Audits trails sur les appareils de criticité Moyenne

D'après le tableau ci-dessus, le compteur de particules, le densimètre, le lecteur de microplaques et le lecteur cinétique (PTS) sont considérés comme moyennement critiques. Bien que certains appareils comme le densimètre soient utilisés quotidiennement, l'utilisation de cet appareil est simple. Si une restriction des accès a été validée sur ces appareils, les utilisateurs ont un accès très limité aux fonctions de l'appareil. Il n'est donc pas forcément nécessaire de contrôler systématiquement les audits trails comme pour les équipements critiques. Les autres appareils de cette catégorie, également simples dans leur conception et possédant une très forte restriction d'accès, sont utilisés moins fréquemment, et donc cela ne nécessite pas une revue systématique des audits trails.

Les audits trails sont enregistrés sur les appareils et sont revus de façon régulière, lors de la qualification périodique des appareils par exemple. Les points revus lors de cette vérification sont les mêmes que ceux des appareils critiques : la gestion des accès (création/ modification de compte/profil), la création ou la modification de projet et les modifications des paramètres de base du système.

Revue des Audits trails sur les appareils de criticité Faible

Les appareils jugés faiblement critiques ont leur audit trail enregistré mais ils ne sont pas revus. Ils sont archivés pour être revus si nécessaire. Il s'agit d'appareils de mesure de données physiques tels que des balances, potentiomètres, viscosimètres, … Les données de ces appareils sont archivées en version papier via des cahiers de laboratoire et l'accès aux appareils est tracé via des logbooks. Les audits trails ne nécessitent pas de relecture mais leur présence et leur enregistrement permettent de faire des recherches en cas de déviations liées à ces appareils.

Appareils ne possédant pas d'Audit Trail

Certains appareils du laboratoire ne possèdent pas de fonctions d'audit trail. Cela pour deux raisons possibles :

L'appareil est très simple et son utilisation ne nécessite pas un suivi informatique des utilisations (ex : pH-mètre, Karl Fisher, …). Le suivi de l'utilisation de ces appareils se fait via des logbooks datés et visés par les techniciens. En ce qui concerne les balances, seule la balance nommée « balance 52 » du laboratoire permet l'enregistrement d'un audit trail. Cette balance, se trouvant sous hotte, sert aux pesées de masses plus petites ou de produits potentiellement nocifs ou volatils. La nécessité d'investissements afin de changer toutes les balances pour qu'elles puissent toutes enregistrer un audit trail n'est pas justifiée pour le moment. Le suivi des utilisations via des logbooks et le suivi des pesées via les cahiers de laboratoire permet de répondre aux exigences en termes de Data Integrity.

L’appareil est trop ancien et le logiciel interne ne permet pas de réaliser des opérations liées à la Data Integrity selon les normes actuelles. C’est le cas des appareils de type spectromètres UV ou IR. Ces appareils utilisés de façon régulière ne possèdent pas des logiciels permettant de réaliser des actions en lien avec les règles d’intégrité des données comme le souhaitent les autorités aujourd’hui. Une mise à jour des logiciels ou un changement complet des appareils est prévu afin de se conformer aux exigences et permettre une gestion des accès, une sauvegarde des données informatiques et les enregistrements des audits trails. En attendant que les mises à jour soient disponibles et installées, certaines mesures ont été mises en place pour pallier à ces manques comme des logbooks pour suivre l’utilisation de ces appareils.

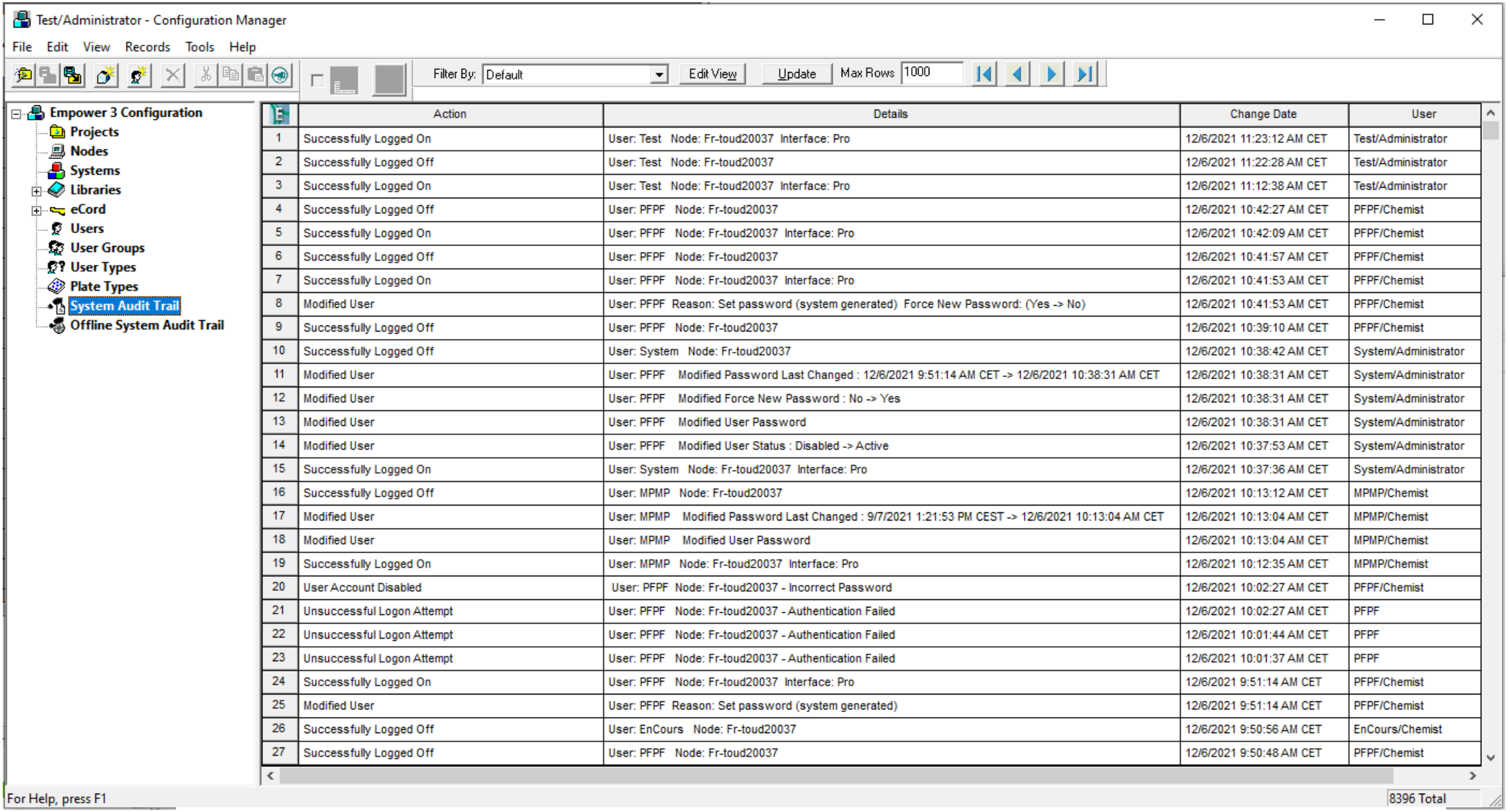
5.8. Méthodes de revue des audits trail

Qu'il s'agisse de l'audit trail administratif ou de l'audit trail opérationnel, toutes les revues doivent avoir fait l'objet d'une étude ou d'une analyse de risque. En effet, il n'est pas possible de vérifier 100 % des lignes de données enregistrées sur certains appareils (par exemple, pour une analyse, l'audit trail opérationnel sur une HPLC comporte plusieurs centaines de lignes). Toutes les opérations enregistrées ne sont pas critiques et ne nécessitent pas de faire l'objet d'analyses approfondies.

Il est possible de choisir selon deux axes d'études la manière de revoir les audits trails :

- Le premier consiste à déterminer les actions critiques (modification de méthodes, modification des paramètres, modification des comptes ou des projets, ...) et à effectuer une recherche sur la personne qui les a réalisées. Cela permet une revue plus exhaustive des audits trails et permet également de s'assurer que les droits utilisateurs sont bien paramétrés. Néanmoins, pour effectuer ce type d'analyse, il est nécessaire que la revue de l'audit trail soit assistée par un logiciel possédant un système de filtres. Sans ce système de filtration des données, ce type de revue est possible mais très chronophage.
- La seconde nécessite d'avoir une gestion des accès validée avec des droits restreints sur les paramètres et la modification de méthodes d'analyse. Si l'on considère qu'une personne ayant des accès de technicien ne peut pas avoir accès aux modifications de

données sensibles telles que la modification des méthodes d'analyses ou à la gestion des archivages, la recherche se porte sur les comptes ayant des accès plus larges. En effet, l'étude des actions faites par les comptes administrateur (n'ayant peu ou pas de restrictions) permet de prouver que celui-ci n'a été utilisé que pour des actions autorisées, tracées et justifiées. Cette solution a pour avantage de simplifier la revue des audits trails, les comptes administrateurs ne devant être utilisés que ponctuellement pour assurer la gestion administrative des systèmes. Le plus important en choisissant ce type de revue est de mettre en évidence le fait que les comptes administrateurs n'ont pas intervenu dans la génération des données, sauf de façon ponctuelle pour effectuer une maintenance.



	Action	Details	Change Date	User
1	Successfully Logged On	User: Test Node: Fr-toud20037 Interface: Pro	12/6/2021 11:23:12 AM CET	Test/Administrator
2	Successfully Logged Off	User: Test Node: Fr-toud20037	12/6/2021 11:22:28 AM CET	Test/Administrator
3	Successfully Logged On	User: Test Node: Fr-toud20037 Interface: Pro	12/6/2021 11:12:38 AM CET	Test/Administrator
4	Successfully Logged Off	User: PFPF Node: Fr-toud20037	12/6/2021 10:42:27 AM CET	PFPF/Chemist
5	Successfully Logged On	User: PFPF Node: Fr-toud20037 Interface: Pro	12/6/2021 10:42:09 AM CET	PFPF/Chemist
6	Successfully Logged Off	User: PFPF Node: Fr-toud20037	12/6/2021 10:41:57 AM CET	PFPF/Chemist
7	Successfully Logged On	User: PFPF Node: Fr-toud20037 Interface: Pro	12/6/2021 10:41:53 AM CET	PFPF/Chemist
8	Modified User	User: PFPF Reason: Set password (system generated) Force New Password: (Yes -> No)	12/6/2021 10:41:53 AM CET	PFPF/Chemist
9	Successfully Logged Off	User: PFPF Node: Fr-toud20037	12/6/2021 10:39:10 AM CET	PFPF/Chemist
10	Successfully Logged Off	User: System Node: Fr-toud20037	12/6/2021 10:38:42 AM CET	System/Administrator
11	Modified User	User: PFPF Modified Password Last Changed : 12/6/2021 9:51:14 AM CET -> 12/6/2021 10:38:31 AM CET	12/6/2021 10:38:31 AM CET	System/Administrator
12	Modified User	User: PFPF Modified Force New Password : No -> Yes	12/6/2021 10:38:31 AM CET	System/Administrator
13	Modified User	User: PFPF Modified User Password	12/6/2021 10:38:31 AM CET	System/Administrator
14	Modified User	User: PFPF Modified User Status : Disabled -> Active	12/6/2021 10:37:53 AM CET	System/Administrator
15	Successfully Logged On	User: System Node: Fr-toud20037 Interface: Pro	12/6/2021 10:37:36 AM CET	System/Administrator
16	Successfully Logged Off	User: MPMP Node: Fr-toud20037	12/6/2021 10:13:12 AM CET	MPMP/Chemist
17	Modified User	User: MPMP Modified Password Last Changed : 9/7/2021 1:21:53 PM CEST -> 12/6/2021 10:13:04 AM CET	12/6/2021 10:13:04 AM CET	MPMP/Chemist
18	Modified User	User: MPMP Modified User Password	12/6/2021 10:13:04 AM CET	MPMP/Chemist
19	Successfully Logged On	User: MPMP Node: Fr-toud20037 Interface: Pro	12/6/2021 10:12:35 AM CET	MPMP/Chemist
20	User Account Disabled	User: PFPF Node: Fr-toud20037 - Incorrect Password	12/6/2021 10:02:27 AM CET	PFPF/Chemist
21	Unsuccessful Logon Attempt	User: PFPF Node: Fr-toud20037 - Authentication Failed	12/6/2021 10:02:27 AM CET	PFPF
22	Unsuccessful Logon Attempt	User: PFPF Node: Fr-toud20037 - Authentication Failed	12/6/2021 10:01:44 AM CET	PFPF
23	Unsuccessful Logon Attempt	User: PFPF Node: Fr-toud20037 - Authentication Failed	12/6/2021 10:01:37 AM CET	PFPF
24	Successfully Logged On	User: PFPF Node: Fr-toud20037 Interface: Pro	12/6/2021 9:51:14 AM CET	PFPF/Chemist
25	Modified User	User: PFPF Reason: Set password (system generated)	12/6/2021 9:51:14 AM CET	PFPF/Chemist
26	Successfully Logged Off	User: EnCours Node: Fr-toud20037	12/6/2021 9:50:56 AM CET	EnCours/Chemist
27	Successfully Logged Off	User: PFPF Node: Fr-toud20037	12/6/2021 9:50:48 AM CET	PFPF/Chemist

Figure 3 : Exemple d'un audit trail sur une chaine CLHP

Par exemple, sur l'audit trail présenté dans la figure 3, la revue de celui-ci est simplifiée car sur cet appareil, les droits d'accès sont validés. En effet, les utilisateurs "user : MPMP, PFPF et EnCours" ont des accès restreints aux fonctions sensibles de l'équipement (modification des paramètres du logiciel, modification des utilisateurs, modification des méthodes, suppression des données, ...). Sur cet audit trail, il est possible de voir que le "user : System" (l'administrateur ayant des droits plus larges) a effectué des actions. Ce sont ces actions qui devront être justifiées afin de déterminer si elles sont critiques ou non et si elles ne compromettent pas l'intégrité des données fournies par l'équipement.

5.9. L'archivage

La conservation dans le temps des résultats est définie par les BPF [4] :

« Des exigences spécifiques s'appliquent aux dossiers de lots qui doivent être conservés au moins un an après la date de péremption du lot correspondant, ou au moins cinq ans après la certification du lot par la personne qualifiée, le délai le plus long s'appliquant. Dans le cas des médicaments expérimentaux, les dossiers de lot sont conservés au moins cinq ans après l'achèvement ou l'interruption formelle du dernier essai clinique au cours duquel le lot a été utilisé. D'autres exigences pour l'archivage des documents peuvent être décrites au sein des législations en ce qui concerne des types particuliers de médicament (par exemple, les médicaments de thérapie innovante (ATMP) et peuvent ainsi requérir des durées d'archivage plus longues pour certains documents. » (Chapitre 4.11 des BPF [4]). Les documents liés aux produits de santé doivent être conservés minimum 5 ans après l'approbation d'un lot (Art. R. 5124-58 CSP [11])

La conservation des documents liés à la production de produits classés I ou II sur la liste des stupéfiants est de 10 ans (Art. R.5132-10 CSP [12]). Dans le cadre d'activités liées à des médicaments dérivés du sang, les données doivent être conservées pendant une durée de 40 ans (Art. R.5121-195 CSP [13]). Il est donc nécessaire de stocker ces données de manière à pouvoir les consulter en cas de besoin. Ces besoins peuvent être liés à des investigations en cas de litiges lors de la production d'un lot mais aussi en cas de besoin de rappel de lot. Comment s'assure-

t-on que des données restent consultables pendant des décennies ? La solution la plus simple à mettre en place aujourd'hui est la conservation des données papier. Elle a été le moyen de conservation principale avant l'arrivée des outils numériques et reste aujourd'hui le moyen le plus simple de conserver une donnée dans le temps. Malgré cela, l'archivage papier entraîne un flux logistique important. Le papier occupe de l'espace de stockage qui pourrait être dédié à d'autres activités. Cet espace doit avoir des conditions de température et d'hygrométrie permettant de ne pas altérer les documents. Les documents archivés doivent être recensés afin de pouvoir être détruits lorsque leur durée de conservation est dépassée. Cela entraîne un travail continu de mise à jour d'une base de données permettant de retrouver facilement un document ou une donnée rapidement (pour la consultation ou la destruction). L'archivage papier permet néanmoins d'être certain de pouvoir avoir accès à une donnée sur du long terme. En effet, les mises à jour des logiciels informatiques peuvent entraîner l'incapacité à consulter un document des années après son obtention (cas des documents liés aux médicaments dérivés du sang qui doivent rester consultables 40 ans).

De plus en plus, l'archivage se fait numériquement. Les données sont sauvegardées sur des serveurs sécurisés afin d'être disponibles en cas de besoin. Cela apporte des avantages tels que la consultation des données peu importe l'endroit où l'on se situe. Il est également plus simple de partager une donnée ainsi que de limiter l'accès à une donnée aux personnes en ayant besoin. L'archivage numérique peut se faire de façon manuelle en stockant intentionnellement des informations ou il peut être effectué de manière automatique. Certains logiciels de systèmes informatisés proposent de faire des sauvegardes périodiques des données (ex : une sauvegarde programmée quotidiennement). Ce système permet de limiter les actions humaines et permet de rendre plus sécurisée la conservation des données.

Contrairement à l'archivage papier, l'archivage numérique limite le stockage physique des documents (gain de place) ainsi que la logistique associée. La base de données s'implémente automatiquement avec les nouvelles ressources disponibles et simplifie le tri de ces données. L'archivage numérique permet également de réaliser des copies des données archivées. Contrairement aux données papier qui sont sur un format « fragile » et non copiable,

les données stockées informatiquement sont disponibles en plusieurs copies gérées. Les données papiers sont sujettes à l'usure en cas d'incident. On peut citer comme exemple un incendie dans les locaux d'archivage ayant pour conséquence de détruire partiellement ou intégralement les données conservées. Les données numériques sont protégées et ne peuvent pas disparaître, des copies sont disponibles. En cas de crash informatique des serveurs de sauvegardes, celles-ci sont récupérables car disponibles sur plusieurs serveurs. Les données numériques doivent être protégées des piratages.

Un des enjeux de cette décennie est la protection des données. Il a été constaté des dizaines d'intrusions numériques dans les grandes instances ces dernières années. Il est possible de citer l'exemple d'hôpitaux ou d'administrations ayant été pris pour cible par des hackers menaçant de détruire ou de divulguer des données sensibles. L'industrie pharmaceutique est aussi la cible de ces attaques et de nombreux moyens sont mis en œuvre pour protéger les données de ces intrusions :

- Renforcement des sécurités lors des connexions ;
- Installation de logiciels de protection informatique (ex : antivirus) ;
- Mise en place de protocoles de sécurité en cas d'intrusion. Ces missions sont à la charge des services informatiques mais il est de la responsabilité de chacun de respecter les règles de protection des données afin de ne pas compromettre l'archivage des données.

6. Ces outils dans les principes ALCOA

Le but final de la mise en place de ces outils est de réduire le niveau de risque lié à l'intégrité des données. L'ensemble de ces actions vise à améliorer la traçabilité des médicaments, ce qui a un impact direct sur les principes garantis par les AMM (Autorisation de Mise sur le Marché) :

• Qualité : En établissant l'ensemble des actions menées pour la production d'un médicament, cela permet de limiter le risque d'erreur et de garantir la qualité du produit de santé.

• Sécurité : En traçant l'ensemble des actions de production et de contrôle d'un médicament et en s'assurant que ces tâches ont été réalisées par des personnes compétentes et habilitées, cela sécurise la production des produits de santé et donc la prise de ceux-ci par les patients.

• Efficacité : Les médicaments produits sont développés pour être les plus performants possibles pour les patients. Il est essentiel de se conformer aux règles établies afin de garantir aux patients que les produits fabriqués seront efficaces.

6.1. Attribuable

Il est important de garantir que les actions réalisées lors de la production ou du contrôle d'un médicament ont été effectuées par du personnel habilité et formé.

Dans le contexte d'un laboratoire de contrôle qualité, réduire le niveau de risque associé au principe de traçabilité (attribuable) peut passer par plusieurs actions :

- Mise en place de comptes personnels sur les équipements informatiques : Traquer les actions réalisées par les techniciens ou le personnel administratif permettra de suivre l'ensemble des analyses effectuées et de faciliter les investigations en cas de problème. L'établissement de comptes personnels pour le personnel technique ou administratif permet de définir les actions que chacun est autorisé à effectuer. Chaque technicien peut ne pas être formé pour toutes les analyses et parfois n'a pas l'autorisation d'effectuer certaines manipulations s'il n'est pas formé sur un équipement. Il est également crucial de définir qui est responsable du contrôle des analyses et de la libération finale d'un test analytique.
- Utilisation de logbooks : Pour les équipements informatiquement moins avancés, les logbooks jouent un rôle similaire aux comptes personnels, bien qu'ils ne sécurisent pas l'accès à une analyse. Les logbooks et le suivi de l'utilisation d'un équipement ou d'un processus permettent toutefois de faciliter les investigations en cas de problèmes, en permettant d'interroger les personnes ayant participé à l'obtention des données brutes.

- Respect des principes des BPF (Bonnes Pratiques de Fabrication) : Dater et identifier les tickets de pesée, les analyses, les protocoles et les rapports sont les premiers moyens d'attribuer une action à une personne sur les documents datés.

6.2. Legible

Les données doivent être lisibles et compréhensibles, un point également souligné dans les Bonnes Pratiques de Fabrication (BPF). Les notes manuscrites doivent être rédigées de manière à être lues sans interprétation, sur un support qui minimise les risques de perte (par exemple, éviter les post-it) et utilisant de l'encre indélébile. Idéalement, l'utilisation d'encre bleue est recommandée, non seulement pour sa lisibilité mais aussi pour la différencier aisément de l'encre noire des imprimantes (photocopies).

Concernant les tickets imprimés, il est crucial de vérifier leur durée de conservation en fonction du mode d'impression. En effet, les tickets thermiques ont tendance à s'estomper avec le temps. Est-il donc nécessaire de produire un duplicata de ces données pour assurer leur traçabilité ?

Pour les systèmes informatisés, cette problématique est davantage liée à l'obsolescence des logiciels. Les logiciels évoluent, les versions changent, mais il est toujours primordial de pouvoir consulter les données obtenues à partir d'anciens logiciels. Comment s'assurer donc de conserver un moyen de lire des données provenant d'un logiciel obsolète lors de son remplacement ?

La solution la plus simple consiste à conserver un moyen de lire ces données en conservant l'équipement qui a permis de les obtenir (anciens équipements ou PC équipés de la version obsolète du logiciel). Ces équipements "obsolètes" peuvent être isolés du réseau informatique principal afin de garantir leur fonctionnement sans risque d'altération par des mises à jour ou des interférences extérieures.

6.3. Contemporaneous

Il est essentiel que les individus ou les systèmes enregistrent des données chaque fois qu'une activité ou une action a lieu dans le but de garantir son intégrité. Ce principe s'applique à tous les types de données, mais il est particulièrement important pour les données papier ou obtenues manuellement afin d'éviter toute perte d'information.

- Respecter les principes des BPF [4] : Dater et identifier les tickets de pesée, les analyses, les protocoles et les rapports constituent le premier moyen d'attribuer une action à quelqu'un concernant les « *Paper data* ».
- Les données informatiques doivent être datées. En complément de la restriction des accès, les personnes ayant accès à l'instrument de mesure ne doivent pas pouvoir modifier la date et l'heure sur l'équipement.
- La réalisation d'un horodatage automatique des rapports obtenus via un système automatisé permet de dater une analyse. Cela permet également de reconstituer une chronologie en cas d'investigation sur un problème analytique.

6.4. Original

Pour assurer la fiabilité d'une donnée, il est essentiel de conserver les documents originaux plutôt que des copies ou des transcriptions, qu'ils soient sur papier ou sur un système informatisé. De plus, pour les données papier, il est préférable de les enregistrer sur leur support destiné. Il est donc recommandé d'écrire directement la donnée sur une feuille de travail plutôt que de la noter sur une feuille volante pour ensuite la retranscrire. La création de copies certifiées constitue également un moyen fiable d'assurer la conservation de l'enregistrement original.

- Concernant les données numériques, il est impératif de mettre en place des protocoles afin de prévenir toute modification des données originales :

- L'implémentation d'audit trails et leur revue permet de vérifier que les données n'ont pas été altérées après leur acquisition.
- La gestion des accès, en restreignant les droits de modification des données pour les utilisateurs, est également un moyen employé pour garantir l'intégrité de la donnée originale.

6.5. Accurate

L'exactitude des données se réfère à des enregistrements fiables et sans erreurs, pouvant être utilisés comme une source d'information. Il est crucial de ne pas altérer les informations originales, et si une modification s'avère nécessaire, celle-ci doit être tracée et justifiée.

Dans le contexte des rendus de résultats dans un laboratoire de contrôle, le double contrôle des analyses et la supervision sont des moyens pour garantir l'exactitude des données. Ces outils permettent de vérifier la conformité des données produites.

La mise en place de qualifications périodiques des équipements est également essentielle. Cette pratique consiste à contrôler régulièrement que les équipements fournissent des résultats non altérés, évitant tout dysfonctionnement susceptible de compromettre la précision des résultats.

Ce point est souvent négligé lors des audits. Les laboratoires de contrôle qualité ont toujours dû être rigoureux en matière de précision et d'exactitude des résultats, car les analyses qui y sont effectuées garantissent la qualité et la sécurité des produits de santé.

7. Critiques et perceptions

La mise en place de nouveaux protocoles liés à la Data Integrity doit être accompagnée d’explications visant à donner du sens à toutes ces procédures.

En effet, la conformité à la Data Integrity implique de nouvelles règles pouvant être perçues comme entravant le travail habituel.

La mise en place d'une gestion des accès avec des droits stricts, limitant l'accès à certaines fonctions d'un logiciel, engendre une nouvelle manière hiérarchisée de travailler. Si ces procédures visent à limiter les erreurs commises par le personnel lors des analyses, elles rendent cependant le personnel dépendant de la hiérarchie pour toute modification justifiée. Bien que ces protocoles aient pour objectif de fluidifier et de sécuriser les processus, leur mise en œuvre peut entraîner un ralentissement des activités en cas d'indisponibilité des décideurs (administrateurs, service informatique, service maintenance, etc.).

De plus, l'implémentation d'une gestion des accès implique la création de mots de passe individuels, généralement avec des règles de complexité. La gestion de plusieurs mots de passe sur différents équipements de laboratoire peut ralentir les activités et entraîner des erreurs ou des blocages de compte, compromettant ainsi la réalisation des analyses.

La mise en place de ces protocoles et procédures constitue également un processus long. Les changements de processus ne sont pas toujours facilités par les équipements eux-mêmes. Certains équipements anciens ne sont pas conçus pour intégrer toutes ces sécurités, rendant leur mise en place fastidieuse. Par exemple, l'enregistrement des audits trails peut nécessiter beaucoup d'espace de stockage dans les mémoires d'équipement, exigeant un archivage fréquent.

Certaines activités liées à la Data Integrity sont également très chronophages. La revue des audits trails, bien que sécurisant les données obtenues, est très longue et nécessite un investissement important en temps humain. Par exemple, la revue des audits trails opérationnels d'une HPLC doit être réalisée lors de la vérification des résultats et constitue un prérequis avant la libération. Ainsi, le temps de supervision est impacté par la mise en place d'une revue complète des audits trails.

Globalement, l'instauration d'une gouvernance Data Integrity dans un laboratoire génère une charge de travail supplémentaire. Cette charge peut se présenter de deux manières :

• Temporaire : une augmentation de l'activité peut survenir pendant la mise en place du projet. Par exemple, l'implémentation d'une gestion des accès peut nécessiter une reconfiguration des paramètres sur un équipement ainsi que la validation des accès. Une fois le projet terminé, le temps d'analyse des techniciens retrouve son niveau d'avant la mise en place de la gestion des accès.

• Permanente : la revue des audits trails, la vérification des accès, les revalidations périodiques des équipements, la mise en place de doubles contrôles, etc., doivent être intégrées à la routine des analyses. Il est crucial d'estimer les ressources nécessaires pour que cette charge supplémentaire ne perturbe pas la routine établie.

Dans le domaine pharmaceutique, l'introduction d'une gouvernance Data Integrity est bien accueillie par les équipes opérationnelles. Bien que certains protocoles prennent du temps pour être intégrés dans les routines, le sens réel attribué à ce surplus d'activités favorise l'adhésion des équipes. La finalité de ces protocoles étant la santé du patient, il est légitime de vouloir fournir les produits de santé les plus sûrs possible.

Cependant, il est essentiel de veiller à éviter un excès de qualité qui pourrait entraîner une perte de temps sans gains significatifs en termes de qualité des résultats d'analyses. Il n'est pas toujours nécessaire de doubler les analyses ou de mettre en place des protocoles de sécurité coûteux en temps. Il est primordial d'adapter le niveau de Data Integrity au risque inhérent à chaque analyse.

Conclusion Générale

Pour conclure, la Data Integrity est aujourd'hui primordiale dans l'industrie pharmaceutique et constitue l'un des enjeux majeurs de cette décennie. Les autorités de santé sont de plus en plus exigeantes sur la qualité des médicaments et des produits de santé qui seront délivrés et administrés aux patients. Les laboratoires de Contrôle Qualité, au même titre que l'ensemble des secteurs industriels, vont devoir s'adapter à ces contraintes afin de garantir un niveau de traçabilité optimal, permettant ainsi d'assurer la sécurité, la qualité et l'efficacité des médicaments. La mise en place des outils détaillés dans cette thèse permet de réduire les risques associés à la production des médicaments.

La Data Integrity n'est pas réservée au seul domaine de l'industrie ; l'ensemble des secteurs de la santé est désormais concerné par ces mesures. Le secteur de la recherche doit également mettre en place ces pratiques, au même titre que les industries. Afin d'obtenir des financements, les organismes financeurs privés ou publics sont de plus en plus exigeants sur ce sujet. Au même titre que les autorités de santé, ces organismes demandent de mettre en place des actions visant à documenter les recherches ainsi qu'à sécuriser les résultats fournis. Les normes et les recommandations détaillées dans cette thèse (21 CFR part 11, GAMP 5, …) sont aujourd'hui applicables aux secteurs de la Recherche Privée ou Publique (Laboratoires de Recherches universitaires).

La Data Integrity dans le domaine de la recherche universitaire revêt une importance capitale pour garantir la fiabilité, la transparence et la validité des données scientifiques produites. Ses exigences impliquent une gestion rigoureuse des données, incluant leur collecte, leur stockage, leur traitement et leur partage. En assurant l'intégrité des données, les chercheurs contribuent à renforcer la crédibilité des résultats, à promouvoir la confiance dans la recherche scientifique et à soutenir l'avancée des connaissances dans leurs domaines respectifs. Cette rigueur accrue favorise également la reproduction des études et la vérification des conclusions, renforçant ainsi la qualité et l'impact de la recherche universitaire.

Bien que la Data Integrity soit vitale dans les deux contextes, les différences majeures résident dans les objectifs, les priorités et les contraintes spécifiques à chaque domaine. Cependant, la rigueur et la transparence dans la gestion des données restent des éléments fondamentaux pour garantir la fiabilité et la validité des résultats, qu'ils soient destinés à la recherche académique ou à l'industrie.

Bibliographies

[1]. Rattan AK. Data Integrity: History, Issues, and Remediation of Issues. PDA J Pharm Sci Technol. 2018 Mar-Apr;72(2):105-116. doi: 10.5731/pdajpst.2017.007765. Epub 2017 Nov 20. PMID: 29158286.

[2]. Graham O'Keefe 2005 Able Laboratories Scandal accessible sur le lien https://learngxp.com/good-manufacturing-practices-cgmp/2005-able-laboratories-scandal/, [consulté le 07/12/23]

[3]. Articles R.5121-195 du Code de la santé publique [en ligne]. Disponible sur : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006914965 [consulté le 07/12/23]

[4]. Bonne pratique de fabrication de médicaments à usage humain. Disponible sur : https://ansm.sante.fr/documents/reference/bonnes-pratiques-de-fabrication-de-medicaments-a-usage-humain [consulté le 07/12/23]

[5]. Guidance for Industry Part 11, Electronic Records; Electronic Signatures — Scope and Application. Disponible sur : https://www.fda.gov/regulatory-information/search-fda-guidance-documents/part-11-electronic-records-electronic-signatures-scope-and-application [consulté le 07/12/23]

[6]. MHRA GxP Data Integrity Definitions and Guidance for Industry. Disponible sur : https://www.gov.uk/government/news/mhra-gxp-data-integrity-definitions-and-guidance-for-industry [consulté le 07/12/23]

[7]. Guidance on good data and record management practices. Disponible sur : https://www.gmp-compliance.org/gmp-news/final-who-guidance-document-on-good-data-and-record-management-practices [consulté le 07/12/23]

[8]. Pharmaceutical Inspection Convention and Pharmaceutical Inspection Co-operation Scheme, « Good practices for data management and integrity in regulated gmp/gdp environments ». [En ligne]. Disponible sur : https://picscheme.org/docview/4234 [consulté le 07/12/23]

[9]. ISPE GAMP® 5: A Risk-Based Approach to Compliant GxP Computerized Systems (Second Edition). Non disponible en ligne

[10]. ⟨1058⟩ Analytical Instrument Qualification. Non disponible en ligne

[11]. Article R. 5124-58 du Code de la santé publique [en ligne]. Disponible sur : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000026903086 [consulté le 07/12/23]

[12]. Article R.5132-10 du Code de la santé publique [en ligne]. Disponible sur : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000018042965 [consulté le 07/12/23]

[13]. Article R. 5121-195 du Code de la santé publique [en ligne]. Disponible sur : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006914965 [consulté le 07/12/23]

université de TOURS | Faculté de pharmacie Philippe-Maupas

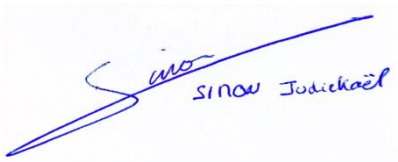
ENGAGEMENT DE NON PLAGIAT

Je, soussigné (e) M. SIMON Judickaël

Déclare être pleinement conscient(e) que le plagiat de documents ou d'une partie d'un document publiés constitue une violation des droits d'auteur ainsi qu'une fraude caractérisée. *(Décret n°92-657 du 13 juillet 1992)*

En conséquence, je m'engage à citer toutes les sources que j'ai utilisées pour écrire ce mémoire.

Signature :



université de TOURS | Faculté de pharmacie Philippe-Maupas

SIGNATURES DU DIRECTEUR DE THESE ET DU DOYEN

N° Étudiant : 21300931 N° Thèse : 119

Nom et Prénom : SINON Jedickael

Sujet : La Data Integrity au sein de l'industrie Pharmaceutique Enjeux et mise en application au sein du Laboratoire de Contrôle Qualité de Delphinum Tours

Tours, le : .....

Le(s) Directeur(s) de Thèse :
Nom(s) et signature(s)

FRANTZ SAINTEN
le 05/01/24

Vu et Transmis :
Le Doyen

Le directeur de la Faculté
des Sciences Pharmaceutiques

Pr Denys BRAND

SIMON Judickaël thèse n° 119

Titre de la thèse

La Data Integrity au sein de l'industrie Pharmaceutique : enjeux et mise en application au sein du laboratoire de Contrôle Qualité de Delpharm Tours

Résumé de la thèse

Aujourd'hui, les réglementations liées à la production des produits de santé se durcissent dans un seul but avec un seul objectif : la sécurité du patient. La traçabilité des données liées aux médicaments est donc un enjeu majeur de la santé publique mondiale.

La mise en place d'une traçabilité globale est résumée sous le terme « Data Integrity ». La mise en place de protocoles et d'actions en lien avec l'intégrité des données doit se faire dans tous les domaines de l'industrie pharmaceutique.

Le but de cette thèse est d'établir un résumé condensé des actions et des outils pouvant être mis en œuvre dans le but d'accroître la sécurisation des données fournies par les laboratoires pharmaceutiques (avec comme exemple le cas des laboratoires de Contrôle Qualité). Les outils et principes généraux qui y sont décrits sont des prérequis essentiels à la mise en place de protocoles d'intégrité des données au sein des laboratoires pharmaceutiques.

Mots clés significatifs de son contenu, attribués par le candidat en liaison avec la bibliothèque universitaire et les membres du jury

Data Integrity / Industrie Pharmaceutique / Contrôle Qualité

Jury

Présidente : Mme Leslie BOUDESOCQUE, Pharmacien, Professeur, Faculté de Pharmacie de Tours

Membres :

M. Fabien FRANTZ, Responsable Contrôle Qualité, Delpharm Tours

Mme Jackie VERGOTE, Pharmacien, Maitre de Conférence, Faculté de Pharmacie de Tours

Mme Christine MORER, Pharmacien, Responsable Assurance Qualité, Delpharm Tours

Mme Perrine MANDREUX, Pharmacien, Responsable Assurance Qualité produit , Sanofi Tours

Date et lieu de soutenance : Université de Tours, UFR de Pharmacie le 22/12/2023