Université de Lille Faculté de Pharmacie de Lille

Année Universitaire 2018/2019

THESE

POUR LE DIPLOME D'ETAT

DE DOCTEUR EN PHARMACIE

Soutenue publiquement le 23 octobre 2019

Par M. DELPLANQUE THIBAUT

Développement d'une politique d'intégrité des données sur un site de production pharmaceutique

---

Membres du jury :

Président :

Pr. Anne Gayot : Professeur à la Faculté de Pharmacie de Lille

Membre(s) extérieur(s) :

Mme. Hélène Zentar: Manager Affaires Réglementaires GSK SAE

M. Yannic Lepage : Manager AQ et AR Minakem Mont-Saint-Guibert

Faculté de Pharmacie

de Lille

3, rue du Professeur Laguesse - B.P. 83 - 59006 LILLE CEDEX

☎ 03.20.96.40.40 - 🖷 : 03.20.96.43.64

http://pharmacie.univ-lille2.fr

Université de Lille

Président :	Jean-Christophe CAMART
Premier Vice-président :	Damien CUNY
Vice-présidente Formation :	Lynne FRANJIÉ
Vice-président Recherche :	Lionel MONTAGNE
Vice-président Relations Internationales :	François-Olivier SEYS
Directeur Général des Services :	Pierre-Marie ROBERT
Directrice Générale des Services Adjointe :	Marie-Dominique SAVINA

Faculté de Pharmacie

Doyen :	Bertrand DÉCAUDIN
Vice-Doyen et Assesseur à la Recherche :	Patricia MELNYK
Assesseur aux Relations Internationales :	Philippe CHAVATTE
Assesseur à la Vie de la Faculté et aux Relations avec le Monde Professionnel :	Thomas MORGENROTH
Assesseur à la Pédagogie :	Benjamin BERTIN
Assesseur à la Scolarité :	Christophe BOCHU
Responsable des Services :	Cyrille PORTA

Liste des Professeurs des Universités - Praticiens Hospitaliers

Civ.	NOM	Prénom	Laboratoire
Mme	ALLORGE	Delphine	Toxicologie
M.	BROUSSEAU	Thierry	Biochimie
M.	DÉCAUDIN	Bertrand	Pharmacie Galénique
M.	DEPREUX	Patrick	ICPAL
M.	DINE	Thierry	Pharmacie clinique
Mme	DUPONT-PRADO	Annabelle	Hématologie
M.	GRESSIER	Bernard	Pharmacologie
M.	LUYCKX	Michel	Pharmacie clinique
M.	ODOU	Pascal	Pharmacie Galénique
M.	STAELS	Bart	Biologie Cellulaire

Liste des Professeurs des Universités

Civ.	NOM	Prénom	Laboratoire
M.	ALIOUAT	El Moukhtar	Parasitologie
Mme	AZAROUAL	Nathalie	Physique
M.	BERTHELOT	Pascal	Onco et Neurochimie
M.	CAZIN	Jean-Louis	Pharmacologie – Pharmacie clinique
M.	CHAVATTE	Philippe	ICPAL
M.	COURTECUISSE	Régis	Sciences végétales et fongiques
M.	CUNY	Damien	Sciences végétales et fongiques
Mme	DELBAERE	Stéphanie	Physique
M.	DEPREZ	Benoît	Lab. de Médicaments et Molécules
Mme	DEPREZ	Rebecca	Lab. de Médicaments et Molécules
M.	DUPONT	Frédéric	Sciences végétales et fongiques
M.	DURIEZ	Patrick	Physiologie
M.	FOLIGNE	Benoît	Bactériologie
M.	GARÇON	Guillaume	Toxicologie
Mme	GAYOT	Anne	Pharmacotechnie Industrielle
M.	GOOSSENS	Jean François	Chimie Analytique
M.	HENNEBELLE	Thierry	Pharmacognosie
M.	LEMDANI	Mohamed	Biomathématiques
Mme	LESTAVEL	Sophie	Biologie Cellulaire
M.	LUC	Gerald	Physiologie

Mme	MELNYK	Patricia	Onco et Neurochimie
M.	MILLET	Régis	ICPAL
Mme	MUHR – TAILLEUX	Anne	Biochimie
Mme	PAUMELLE-LESTRELIN	Réjane	Biologie Cellulaire
Mme	PERROY	Anne Catherine	Législation
Mme	ROMOND	Marie Bénédicte	Bactériologie
Mme	SAHPAZ	Sevser	Pharmacognosie
M.	SERGHERAERT	Eric	Législation
Mme	SIEPMANN	Florence	Pharmacotechnie Industrielle
M.	SIEPMANN	Juergen	Pharmacotechnie Industrielle
M.	WILLAND	Nicolas	Lab. de Médicaments et Molécules

Liste des Maîtres de Conférences - Praticiens Hospitaliers

Civ.	NOM	Prénom	Laboratoire
Mme	BALDUYCK	Malika	Biochimie
Mme	GARAT	Anne	Toxicologie
Mme	GOFFARD	Anne	Bactériologie
M.	LANNOY	Damien	Pharmacie Galénique
Mme	ODOU	Marie Françoise	Bactériologie
M.	SIMON	Nicolas	Pharmacie Galénique

Liste des Maîtres de Conférences

Civ.	NOM	Prénom	Laboratoire
Mme	ALIOUAT	Cécile Marie	Parasitologie
M.	ANTHERIEU	Sébastien	Toxicologie
Mme	AUMERCIER	Pierrette	Biochimie
Mme	BANTUBUNGI	Kadiombo	Biologie cellulaire
Mme	BARTHELEMY	Christine	Pharmacie Galénique
Mme	BEHRA	Josette	Bactériologie
M	BELARBI	Karim	Pharmacologie
M.	BERTHET	Jérôme	Physique
M.	BERTIN	Benjamin	Immunologie
M.	BLANCHEMAIN	Nicolas	Pharmacotechnie industrielle
M.	BOCHU	Christophe	Physique
M.	BORDAGE	Simon	Pharmacognosie
M.	BOSC	Damien	Lab. de Médicaments et Molécules
M.	BRIAND	Olivier	Biochimie
M.	CARNOY	Christophe	Immunologie
Mme	CARON	Sandrine	Biologie cellulaire
Mme	CHABÉ	Magali	Parasitologie
Mme	CHARTON	Julie	Lab. de Médicaments et Molécules
M	CHEVALIER	Dany	Toxicologie
M.	COCHELARD	Dominique	Biomathématiques
Mme	DANEL	Cécile	Chimie Analytique
Mme	DEMANCHE	Christine	Parasitologie
Mme	DEMARQUILLY	Catherine	Biomathématiques
M.	DHIFLI	Wajdi	Biomathématiques
Mme	DUMONT	Julie	Biologie cellulaire
Mme	DUTOUT-AGOURIDAS	Laurence	Onco et Neurochimie
M.	EL BAKALI	Jamal	Onco et Neurochimie
M.	FARCE	Amaury	ICPAL
Mme	FLIPO	Marion	Lab. de Médicaments et Molécules
Mme	FOULON	Catherine	Chimie Analytique
M.	FURMAN	Christophe	ICPAL
Mme	GENAY	Stéphanie	Pharmacie Galénique
M.	GERVOIS	Philippe	Biochimie
Mme	GOOSSENS	Laurence	ICPAL
Mme	GRAVE	Béatrice	Toxicologie
Mme	GROSS	Barbara	Biochimie
M.	HAMONIER	Julien	Biomathématiques

Mme	HAMOUDI	Chérifa Mounira	Pharmacotechnie industrielle
Mme	HANNOTHIAUX	Marie-Hélène	Toxicologie
Mme	HELLEBOID	Audrey	Physiologie
M.	HERMANN	Emmanuel	Immunologie
M.	KAMBIA	Kpakpaga Nicolas	Pharmacologie
M.	KARROUT	Youness	Pharmacotechnie Industrielle
Mme	LALLOYER	Fanny	Biochimie
M.	LEBEGUE	Nicolas	Onco et Neurochimie
Mme	LECOEUR	Marie	Chimie Analytique
Mme	LEHMANN	Hélène	Législation
Mme	LELEU-CHAVAIN	Natascha	ICPAL
Mme	LIPKA	Emmanuelle	Chimie Analytique
Mme	MARTIN	Françoise	Physiologie
M.	MOREAU	Pierre Arthur	Sciences végétales et fongiques
M.	MORGENROTH	Thomas	Législation
Mme	MUSCHERT	Susanne	Pharmacotechnie industrielle
Mme	NIKASINOVIC	Lydia	Toxicologie
Mme	PINÇON	Claire	Biomathématiques
M.	PIVA	Frank	Biochimie
Mme	PLATEL	Anne	Toxicologie
M.	POURCET	Benoît	Biochimie
M.	RAVAUX	Pierre	Biomathématiques
Mme	RAVEZ	Séverine	Onco et Neurochimie
Mme	RIVIERE	Céline	Pharmacognosie
Mme	ROGER	Nadine	Immunologie
M.	ROUMY	Vincent	Pharmacognosie
Mme	SEBTI	Yasmine	Biochimie
Mme	SINGER	Elisabeth	Bactériologie
Mme	STANDAERT	Annie	Parasitologie
M.	TAGZIRT	Madjid	Hématologie
M.	VILLEMAGNE	Baptiste	Lab. de Médicaments et Molécules
M.	WELTI	Stéphane	Sciences végétales et fongiques
M.	YOUS	Saïd	Onco et Neurochimie
M.	ZITOUNI	Djamel	Biomathématiques

Professeurs Certifiés

Civ.	NOM	Prénom	Laboratoire
M.	HUGES	Dominique	Anglais
Mlle	FAUQUANT	Soline	Anglais
M.	OSTYN	Gaël	Anglais

Professeur Associé - mi-temps

Civ.	NOM	Prénom	Laboratoire
M.	DAO PHAN	Hai Pascal	Lab. Médicaments et Molécules
M.	DHANANI	Alban	Droit et Economie Pharmaceutique

Maîtres de Conférences ASSOCIES - mi-temps

Civ.	NOM	Prénom	Laboratoire
M.	BRICOTEAU	Didier	Biomathématiques
Mme	CUCCHI	Malgorzata	Biomathématiques
M.	FRIMAT	Bruno	Pharmacie Clinique
M.	GILLOT	François	Droit et Economie pharmaceutique
M.	MASCAUT	Daniel	Pharmacie Clinique
M.	ZANETTI	Sébastien	Biomathématiques
M.	BRICOTEAU	Didier	Biomathématiques

AHU

Civ.	NOM	Prénom	Laboratoire
Mme	DEMARET	Julie	Immunologie
Mme	HENRY	Héloïse	Biopharmacie
Mme	MASSE	Morgane	Biopharmacie

Université de Lille

Faculté de Pharmacie de Lille

Faculté de Pharmacie de Lille

3, rue du Professeur Laguesse - B.P. 83 - 59006 LILLE CEDEX
Tel. : 03.20.96.40.40 - Télécopie : 03.20.96.43.64
http://pharmacie.univ-lille2.fr

L'Université n'entend donner aucune approbation aux opinions émises dans les thèses ; celles-ci sont propres à leurs auteurs.

Remerciements :

Au professeur Anne Gayot,
Merci de m'avoir guidé au sein de cet exercice et d'avoir eu suffisamment de patience pour traiter avec ma procrastination chronique.

A Hélène Zentar,
Merci d'avoir été présente dans les bons comme les mauvais moments. Une oreille attentive et un bon coup de pied aux fesses quand il le fallait : être un bon chef c'est surement bien, être une bonne personne c'est forcément mieux.
Surement l'une des personnes avec qui j'aurai aimé avoir des conversations, sacrée culture : chapeau !

A Yannic Lepage,
Une personne capable de vous parler de musique/sport/jeux comme un expert tout en enchainant sur la nouvelle mise à jour de texte réglementaire. Capable de comprendre le problème le plus tordu en un coup d'œil et de prendre son bâton de pèlerin pour le résoudre. Professionnellement stupéfiant et personnellement très sympa !

A Carine Foulon,
Un grand merci d'avoir répondu présente au dernier moment et d'avoir rapidement réglé une situation complexe. Sans toi je ne serai peut-être pas docteur !

A ma mère,
A toi la place de choix. Merci d'avoir eu le courage de me supporter pendant tout ce temps, je pense que je n'ai pas été l'enfant le plus facile à élever. Merci pour tous ces sacrifices sans jamais dire un seul mot.

Table des matières :

Développement d'une politique d'intégrité des données sur un site de production pharmaceutique

INTRODUCTION :

Les données enregistrées sont un élément majeur dans la prise de décision. Qu'il s'agisse de libérer un lot ou de présenter un rapport aux autorités, les données sont ainsi essentielles à la compréhension des activités réalisées sur un site pharmaceutique. Il apparait ainsi nécessaire de garantir que ces informations sont fiables et correspondent à la réalité du produit afin d'assurer la prise de décisions qualité. Sans donnée fiable, il est impossible de prendre les bonnes décisions pour le patient.

Suite à la troisième révolution industrielle et à l'émergence de l'informatique, les données électroniques se sont ajoutées aux données manuscrites. Le volume de données générées dans le monde connait alors une croissance exponentielle, passant de 0,130 zetaoctets (10^{21} octets) par an en 2005 à une prévision de 160 zetaoctets en 2025, soit une augmentation d'un facteur 1200 en 20 ans(1).

Les diverses autorités ont pris en considération cette augmentation du nombre et de la diversité de données générées, en publiant des textes relatifs aux données, notamment :

- La **World Health Organization (WHO):** Guidance on good Data and Record Management Practices *2015*(2)
- La **Food and Drug Administration (FDA)**: Data Integrity and Compliance with cGMP *2016*(3)
- L'**European Medicines Agency (EMA)**: Good Manufacturing Practice guidance to ensure the Integrity of Data *2016*(4)

- Le **Pharmaceutical Inspection Co-operation Scheme (PIC/S)**: Good Practices for Data Management and Integrity in regulated GMP/GDP environments *2016*(5)
- La **Medicines and Healthcare products Regulatory Agency (MHRA)**: Data Integrity Definitions and Guidance for Industry *2018*(6)

Présente dès le premier chapitre des BPF, l'intégrité des données est devenue l'un des sujets de préoccupations du monde pharmaceutique et de l'inspection réglementaire. C'est dans ce contexte que de nombreux sites pharmaceutiques mettent aujourd'hui en place des plans de développement de leur politique d'intégrité des données.

PREMIERE PARTIE:
Veille réglementaire

A. Des textes réglementaires historiques

1. EMA

L'intégrité des données a toujours existé sans être au cœur des préoccupations. En effet, dès 1991 la commission européenne décrit dans la directive 91/356 article 9 (7), directive établissant les principes et lignes directrices de bonnes pratiques de fabrication pour les médicaments à usage humain, que :

- Tout fabricant doit disposer d'un système de documentation.
- Les documents doivent être clairs, exempts d'erreurs et tenus à jour.
- Cet ensemble de documents doit permettre de retracer l'historique de chaque lot fabriqué.
- Les documents relatifs à un lot doivent être conservés au moins un an après la date de péremption du lot concerné.
- Lorsque l'usage de documents écrits est remplacé par des systèmes de traitement électronique […], le fabricant doit avoir validé le système adopté.
- Les données conservées doivent pouvoir être facilement restituées de façon lisible.
- Les données conservées par des systèmes informatiques doivent être protégées contre toute perte ou altération de données.

Cette directive établit les principaux requis concernant la **documentation papier** et aborde la **validation des systèmes informatisés**. Mise à jour en 2003 (directive 2003/94 (8)) elle apporte un complément d'information :

- Le fabricant dispose de procédures […] et de documents particuliers à la fabrication de chaque lot.

- Dans le cas d'un médicament expérimental, les documents relatifs à un lot sont conservés au moins cinq ans après l'achèvement ou l'interruption formelle du dernier essai clinique durant lequel le lot a été utilisé.

- Les données mémorisées sur support électronique sont protégées par des méthodes telles que la réalisation de copies de secours et le transfert sur un autre système de mémorisation de façon à ce qu'elles ne risquent pas d'être perdues ou endommagées.

En parallèle, la création en 1992 de l'**annexe 11 de l'Eudralex** s'intéresse d'avantage aux données électroniques et a pour but d'assurer le même niveau d'exigences à ces données qu'aux données papier. Suite au développement de l'utilisation des systèmes informatisés, cette annexe a été mise à jour en juin 2011 et développe notamment :

- Le système de management du risque : l'utilisation des systèmes informatisés doit être intégrée au système de gestion du risque du site tout au long de leur cycle de vie.

- Le personnel : les activités doivent être ségréguées pour éviter tout conflit d'intérêt.

- La validation : les systèmes informatisés doivent être validés et tout changement doit être effectué selon le processus de gestion des changements.

2. FDA

La directive européenne 91/356 a été accompagnée outre-Atlantique dès 1997 par la réglementation 21 CFR partie 11 (9) qui se focalise sur **l'enregistrement électronique des données** et sur l'**utilisation de la signature électronique**. Aujourd'hui encore, ce document est celui de référence concernant l'intégrité des données et il évoque notamment :

- L'utilisation de documents avec signature électronique à la place d'un système papier est possible.

- La création, modification, conservation et transmission de données électroniques doit être procédurée.

- Des contrôles doivent être en place afin d'assurer l'authenticité, l'intégrité et la confidentialité de ces données.

- Les systèmes informatisés doivent être validés afin d'assurer l'exactitude, la fiabilité et la cohérence des données générées. Il doit être possible de discerner une donnée invalide ou altérée.

- Les données électroniques doivent être protégées durant l'entièreté de leur période de rétention afin de conserver leur exactitude et leur récupération rapide.

- L'accès aux systèmes informatisés générant des données doit être limité aux personnes autorisées.

- Toute personne impliquée dans le cycle de vie d'une donnée doit avoir les formations ainsi que l'expérience requises afin d'assurer l'exactitude de ces données.

- Chaque signature électronique doit être spécifique à un individu et ne doit pas être utilisée par une autre personne.

- Chacun est responsable des activités réalisées grâce à sa signature électronique.

- Tout enregistrement électronique doit posséder :

    - Le nom de la personne ayant signée l'enregistrement
    - La date et l'heure de cette signature
    - Le contexte de cette signature (par exemple : revue, approbation, auteur…)

- Les signatures électroniques basées sur une identification biométrique doivent choisir des caractéristiques biologiques ne permettant une utilisation que par leur réel propriétaire.

- Les signatures électroniques qui ne sont pas basées sur une identification biométrique doivent :
    - Nécessiter au moins deux moyens d'identification distincts (identifiant et mot de passe)
    - N'être utilisées que par leur propriétaire
- L'utilisation de signatures électroniques basées sur un couple « identifiant/mot de passe » doit être contrôlée afin d'assurer leur bon fonctionnement :
    - Chaque couple « identifiant/mot de passe » doit être unique afin que deux individus ne puissent avoir la même signature
    - L'attribution des identifiants doit être revue périodiquement (par exemple : afin de s'assurer que chaque individu ait une signature et qu'une personne ayant quittée la société ne puisse plus signer de document)
    - Des mesures de protection doivent être mises en place afin de détecter et empêcher une utilisation non autorisée de la signature électronique
    - Les systèmes générant ou utilisant des signatures électroniques doivent être revus périodiquement afin de s'assurer qu'ils fonctionnent correctement et n'ont pas été modifié de manière non autorisée
- Chaque système informatisé doit posséder un audit trail afin d'enregistrer chaque action réalisée sur ce système.
- Les modifications apportées à un système informatisé doivent faire l'objet d'un processus procéduré de gestion des changements.

Les deux documents publiés par l'EMA et la FDA établissent les fondations de l'intégrité des données, qu'elles soient papier ou électroniques, mais ne définissent encore aucun critère permettant d'identifier une donnée intègre.

B. Le renforcement de l'intégrité des données de 2015

1. WHO

Suite à une concertation du WHO en avril 2014 ayant pour thème le management du risque, un projet de nouvelle note explicative sur « la bonne gestion des données » a été soumis. Au vu du nombre croissant d'observations publiées sur ce sujet lors d'inspections réglementaires, le projet d'établir cette note explicative a été validé en octobre 2014. En septembre 2015 une première ébauche a été soumise au WHO et qui constitue toujours un document de travail, n'ayant pas encore été officialisée (2).

Le WHO souligne le besoin pour l'industrie pharmaceutique de moderniser ses stratégies de contrôle des données et d'appliquer son processus de gestion des risques aux nouvelles technologies (par exemple : utilisation de systèmes informatisés). Ce programme de suivi des données doit inclure une politique et des procédures organisant les différents éléments clés cités ci-dessous :

- **Données papier et électroniques** : Les requis concernant l'intégrité des données sont les mêmes, qu'elles soient sous format papier ou électronique.

- **Sous-traitant** : Le laboratoire pharmaceutique est responsable de l'intégrité des données générées par ses sous-traitants et des décisions prises sur la base de ces données. Cette responsabilité nécessite de garantir l'assurance que les sous-traitants possèdent un programme permettant de supporter l'intégrité et la fiabilité de leurs données.

- **Bonnes pratiques documentaires** : Les bonnes pratiques documentaires doivent être respectées afin d'assurer que tous les enregistrements, qu'ils soient papier ou électroniques, permettent de reconstituer avec précision l'ensemble des activités réalisées.

- **Gestion des données** : Afin d'établir un programme robuste et durable de gestion des données il est important que les plus hauts niveaux hiérarchiques assurent qu'une gouvernance des données soit en place. Cette note explicative inclut :

- L’application de la gestion des risques au système déjà en place afin de s’assurer que les données actuelles sont fiables.
- Les responsables d’unités doivent s’assurer que le personnel n’est pas soumis à des pressions commerciales, politiques et financières pouvant impacter la qualité et l’intégrité de leur travail.
- Toute personne menée à diriger une équipe doit s’assurer que ses collaborateurs comprennent l’importance de l’intégrité des données et de son impact sur la qualité du produit et la sécurité du patient.

- **Culture de la qualité** : la direction doit établir et maintenir un environnement de travail propice à la qualité afin de minimiser le risque d’enregistrement non conforme. Les deux éléments essentiels sont la culture de la transparence et la libre remontée des déviations, erreurs, omissions et résultats atypiques. Cette responsabilité de la direction est dans la lignée de l’ICH Q10 (système qualité pharmaceutique) datant de 2008.
- **Conception des documents d’enregistrement** : les documents d’enregistrement doivent être conçus de manière à favoriser le respect des principes de l’intégrité des données.

Toute entreprise réalisant des activités GxP doit posséder un système de gestion de la qualité et cette activité est à documenter dans le manuel qualité de l’entreprise. Ce système a pour but de :

- Permettre à l’entreprise de développer ses procédures, processus et systèmes pouvant impacter l’intégrité des données,
- D’allouer les ressources humaines et matérielles de manière proportionnée à l’impact de ces données sur la qualité du produit et la sécurité du patient,
- D’évaluer chaque système d’enregistrement afin de corriger les éventuelles non conformités,

- D’informer la direction des éventuelles opportunités d’amélioration des processus et systèmes grâce aux outils d’audits qualité, auto-inspections et revue des risques.

Le personnel doit être formé aux principes de l’intégrité des données et la direction doit s’assurer que chaque personne présente sur le site travaille en adéquation avec les bonnes pratiques. De plus, le personnel clé (équipe qualité, responsables et managers) doit être formé à la détection et la prévention des risques au sein de son unité.

Afin d’assurer l’intégrité des données générées pas un système informatisé, l’ensemble de ces systèmes doivent être validés. Cette validation doit identifier les contrôles nécessaires permettant d’assurer que les données répondent aux critères ALCOE.

2. EMA

En Aout 2016, suite aux nombreuses interrogations des entreprises pharmaceutiques, l’agence européenne du médicament publie un document sous la forme d’une série de questions/réponses. Reprenant une majeure partie des requis présents dans la note explicative du WHO, celle-ci ajoute, entre autres, des réponses à ces questions :

Comment le risque associé à une donnée peut-il être évalué ?

L’évaluation du risque doit prendre en compte la vulnérabilité d’une donnée face aux modifications volontaires ou involontaires. Des mesures de contrôle permettant d’éviter ces modifications ou de faciliter leur détection peuvent être des actions de réduction du risque.

Cette évaluation doit porter sur l’ensemble des services de l’entreprise et non pas uniquement sur les ressources informatiques. Les facteurs à prendre en compte sont les suivants :

- La complexité du processus

- Le degré d'automatisation
- La subjectivité du résultat obtenu

Les interfaces entre l'homme et le système informatisé sont ainsi prises en compte dans l'évaluation du risque. En effet, un système informatisé validé peut toujours présenter un risque critique si l'utilisateur est en capacité d'influencer sur le résultat.

Comment la criticité d'une donnée peut-elle être évaluée ?

Les décisions prises sur la base de données n'ont pas toutes le même degré d'importance : l'impact de ces décisions varie lui aussi. Les aspects à prendre en compte lors de l'évaluation de la criticité d'une donnée sont les suivants **:**

- Quelle décision est prise sur la base de cette donnée ?
  Par exemple : Lors de la libération de lot, les données liées aux attributs qualités critiques sont plus sensibles que les rapports de nettoyage du magasin.
- Quel est l'impact de cette donnée sur la qualité du produit et la sécurité du patient ?
  Par exemple : Pour un comprimé, l'analyse du principe actif est plus critique que les dimensions de ce comprimé.

Comment une entreprise doit-elle créer et contrôler son système de documentation papier afin d'éviter les modifications non autorisées de données ?

Les formulaires vierges utilisés pour l'enregistrement de données peuvent être créés par un système électronique (par exemple : Word, Excel). Le document maitre correspondant doit être approuvé et sa gestion contrôlée.

Les formulaires vierges doivent répondre aux requis suivants :

- Avoir un numéro de référence unique le liant à une procédure
- Avoir un numéro de version unique

- Leur gestion doit être appropriée de manière à ce que seule la dernière version puisse être imprimée
- Leur distribution doit être traçable en utilisant un registre ou tout autre système approprié. La date de distribution, le nombre de copie ainsi que le service concerné doivent être connus.
- Les copies distribuées doivent être protégées contre la photocopie en utilisant un marquage sécurisé ou en utilisant un papier de couleur uniquement disponible au sein du département chargé de l'impression.

3. FDA

En avril 2016 la FDA publie un projet de document sur l'intégrité des données. Ce document est, comme celui de l'EMA, rédigé sous la forme de questions/réponses permettant d'éclaircir de nouveaux points.

Quand est-il permis d'exclure les données d'une prise de décision ?

Toutes les données enregistrées doivent être évaluées par le service qualité. Afin d'exclure des données de la prise de décision, la justification doit être basée sur une analyse scientifique et documentée.

Comment doit-on restreindre l'accès aux systèmes informatisés ?

Des contrôles doivent être en place afin de s'assurer que seules les personnes autorisées puissent agir sur les enregistrements. La FDA recommande de restreindre les accès aux paramètres par des moyens techniques (par exemple : en limitant les droits d'accès informatiques). La gestion des accès à un équipement doit ainsi être supervisé par un administrateur et ce rôle doit être assigné à une personne indépendante du service utilisant le système afin d'éviter tout conflit d'intérêt. Afin de faciliter la gestion des accès informatiques, la FDA recommande de maintenir à jour, par système, une liste des personnes ayant des accès informatiques ainsi que leur niveau d'accès.

Dans de petites entreprises, s'il n'est pas possible d'avoir un administrateur indépendant du service, la FDA suggère que chaque action effectuée par l'administrateur soit contrôlée par une seconde personne pour éviter tout conflit d'intérêt.

Comment contrôler l'impression des formulaires ?

La FDA recommande que l'impression des formulaires soit contrôlée par le service d'assurance qualité. L'une des pistes envisagées est que chaque impression ait un numéro unique et qu'après utilisation, l'ensemble des formulaires fasse l'objet d'une réconciliation afin de déterminer si des formulaires sont manquants ou ont été réimprimés.

Faut-il revoir les audit trails ?

Les audit trails comportant une modification d'une donnée critique doivent être revus à chaque enregistrement et avant approbation final de cet enregistrement

Les audit trails qui concernent les modifications apportées aux appareils du laboratoire de contrôle qualité et à la production doivent être revu de façon régulière. La FDA recommande cependant d'établir cette revue des audit trails comme étant une opération de routine.

Qui doit revoir les audit trails ?

Les audit trails sont considérés comme partie intégrante de la donnée. Le personnel responsable de la revue de ces données est aussi responsable de la revue des audit trails.

Peut-on réaliser une copie numérique d'un document papier ?

La numérisation d'un document est possible tant que la copie conserve le contenu et le sens du document original.

4. PICS/S

La convention internationale des inspecteurs pharmaceutiques a rédigé en Aout 2016 la première ébauche de sa note explicative sur l'intégrité des données. Ce document reprend les grands concepts du WHO et de la FDA en développant quelques spécificités sur la gestion de la culture qualité et sur les critères d'une donnée intègre.

Culture qualité :

C'est l'ensemble des valeurs, croyances, opinions et comportements portées par la direction, les responsables et le personnel en charge de la qualité qui contribuent à créer un environnement favorable à l'amélioration quotidienne des pratiques.

Cette culture qualité est essentielle à la gouvernance des données notamment en introduisant la notion de transparence : chacun doit être libre de pouvoir identifier et remonter tout problème au département d'assurance qualité sans être pénalisé dans son travail. Dans les entreprises ayant un manque de transparence, il est nécessaire d'insister sur la surveillance et la revue afin de parvenir à un niveau de contrôle équivalent. Un processus de remontée anonyme de problèmes doit être une solution envisageable dans de telles circonstances.

La direction se doit de promouvoir la culture de la qualité en :

- Suivant un code d'éthique et un code de bonne conduite
- Montrant l'exemple
- Acceptant la responsabilité des actions et décisions prises
- Etant proactif
- Ayant des attentes mesurées et réalistes en ses équipes afin de ne pas appliquer de pression inutile
- Fournissant les ressources humaines et matérielle nécessaires

Un code d'éthique doit être mis en place afin d'être le reflet des attentes de la direction en matière de qualité. Ce code doit insister sur la culture de la qualité et développer un environnement de confiance dans lequel chaque individu est responsable d'assurer la qualité du produit et la sécurité du patient.

Chaque membre du personnel doit prendre connaissance de ce code et l'appliquer au quotidien.

Les comportements non désirés doivent être pris en charge au plus vite par des mesures disciplinaires.

Nouveaux critères d'une donnée intègre :

Ce document est le premier à introduire de nouveaux critères afin de renforcer l'intégrité des données, passant ainsi de ALCOE à ALCOE+. Une donnée doit maintenant satisfaire aux nouveaux requis suivants :

- Cohérente
- Complète
- Disponible
- Durable

Ces principes seront détaillés dans la deuxième partie de cette thèse.

5. MHRA

Le MHRA a publié en Juillet 2016(10) une note explicative modifiée en Mars 2018 (6). Ce texte définit un troisième type de systèmes, outre les systèmes papier et électroniques, le système hybride. Celui-ci est une combinaison des deux précédents et doit obéir aux requis de chacun d'entre eux.

DEUXIEME PARTIE:
Des données intègres

A. Cycle de vie des données

La société internationale d'ingénierie pharmaceutique (ISPE) définit le cycle de vie d'une donnée, qu'elle soit sous format papier ou électronique, comme étant la succession de 5 grandes étapes(11). Ce cycle retrace la vie d'une donnée : depuis sa création jusqu'à la destruction, des années plus tard. Chaque étape de ce cycle peut avoir un impact sur l'intégrité des données.

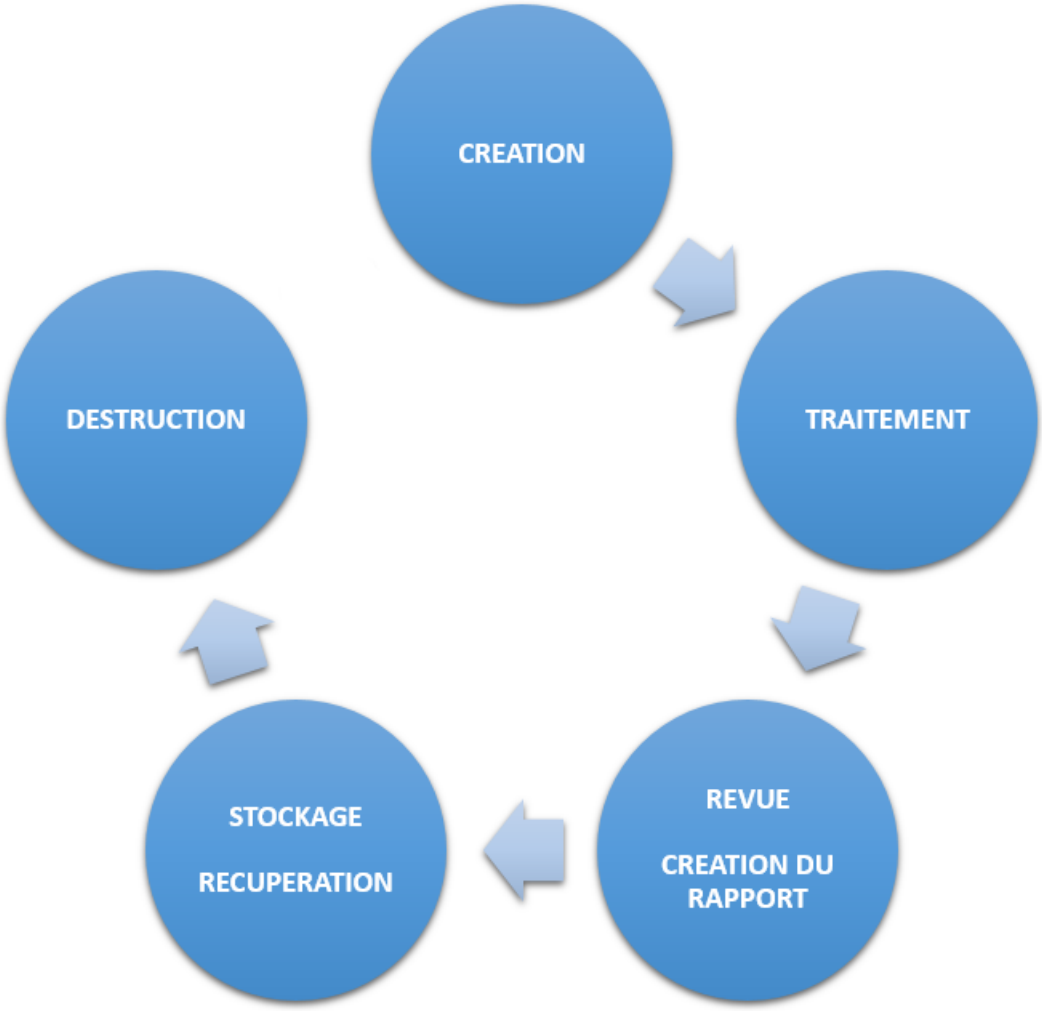


Figure 1 : Cycle de vie d'une donnée selon le guide GAMP 2017 de l'ISPE

Dans ce chapitre seront détaillées les différentes étapes de ce cycle de vie.

1. Création

La création d'une donnée est le point clé de son cycle de vie. Si celle-ci n'est pas réalisée de manière précise, alors tout le cycle de vie est compromis. Cette création peut être réalisée de différentes façons :

- Capture d'une donnée par un équipement (par exemple : appareil de mesure)
- Retranscription manuelle d'un affichage
- Encodage dans un système informatique (par exemple : retranscription dans un ERP)

Lorsque la donnée fait intervenir un système informatisé, ce dernier doit être entretenu et subir une vérification métrologique afin de garantir sa conformité. Pour tout appareil de mesure, il convient de s'assurer que ses paramètres de résolution, gamme, linéarité et sensibilité permettent de réaliser une mesure précise.

Si le système qui génère la donnée possède un faible niveau de sécurité (par exemple aucune protection des modifications de paramètres critiques), alors un processus de « vérification 4 yeux » (aussi appelé "4 eyes principle") effectué par une seconde personne sera réalisé en temps réel si la criticité de la donnée le justifie. Cette vérification doit pouvoir répondre à la notion de « témoignage » : une personne réalise l'action, une seconde observe et valide l'intégralité de l'action : de l'utilisation des bons paramètres à la validité du résultat. Il est alors important que chacune des deux personnes soit formée à cette activité afin de témoigner du bon déroulement de celle-ci. Il ne s'agit pas de valider uniquement le résultat obtenu mais d'assurer le bon déroulement de l'ensemble du processus.

Dans tout processus faisant intervenir plusieurs étapes générant chacune une donnée, la création ainsi que l'enregistrement de la première donnée doivent être réalisés avant de passer à l'étape suivante, ceci afin d'éviter une éventuelle perte de donnée. On obtient ainsi notre "original record" aussi appelé "donnée brute".

2. Traitement

La seconde étape du cycle de vie d'une donnée est son traitement : la donnée brute est modifiée (par exemple : traduction de langage informatique, calcul, génération de graphique…) afin d'obtenir un résultat interprétable.

Dans le cas de l'utilisation d'un système informatisé, le langage propre au système est le binaire. La donnée brute est donc une succession de "0" et de "1" qui est alors illisible par un être humain. Le traitement de la donnée permet de passer d'un langage informatique à un langage couramment utilisé par l'être humain (alphabet et nombres).

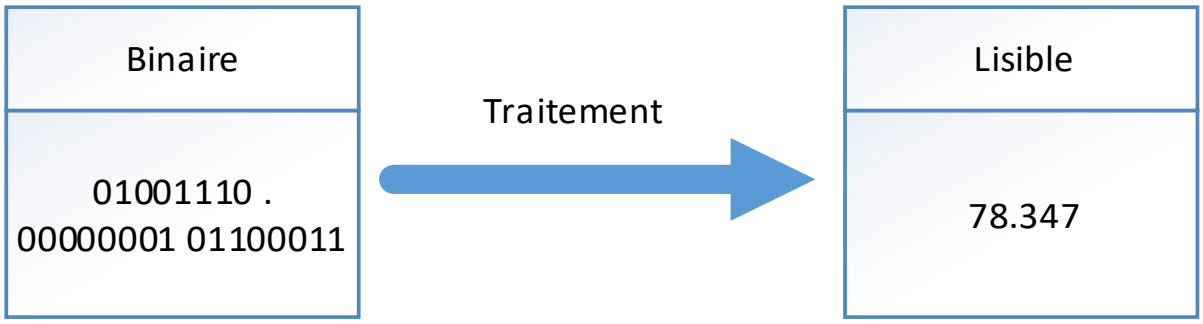


Figure 2 : Exemple de traitement de donnée informatique

Le résultat est lisible par tous mais seule, cette donnée n'a aucun sens : il n'y a aucun contexte pour comprendre ce qu'elle représente. Le traitement de cette donnée va donc faire intervenir les métadonnées. Celles-ci permettent de contextualiser l'information afin que le tout soit lisible et compréhensible. Il peut donc s'agir d'un numéro de salle, d'une date, des unités, de la sonde ayant créé la donnée, etc... Faisant partie de l'ensemble des données générées, elles sont soumises aux mêmes règles concernant leur intégrité.

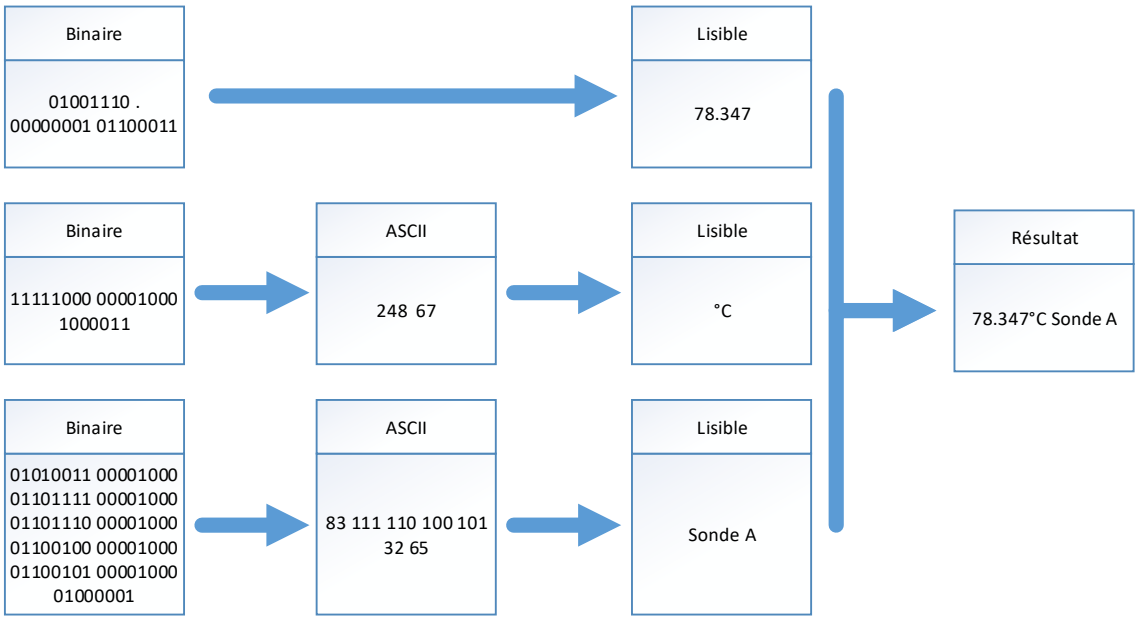


Figure 3 : Exemple de combinaison de données afin d'obtenir un résultat cohérent

Regroupant données et métadonnées, l'information est maintenant compréhensible et possède un contexte : chacun est capable de comprendre de quoi il s'agit. Cependant, certaines données, utilisées seules, ne permettent pas de prendre une décision (par exemple : suivi de température), il est parfois nécessaire de compiler cette information avec d'autres de même nature afin de pouvoir suivre une évolution des celles-ci dans le temps.

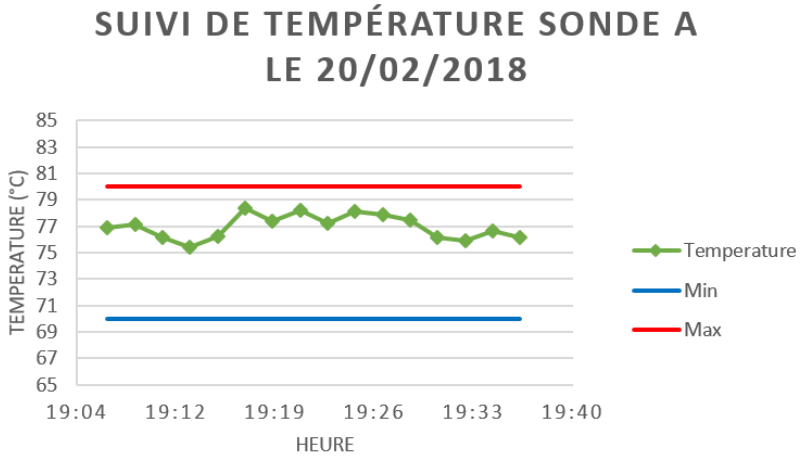


Figure 4 : Compilation des données

On obtient ainsi une donnée traitée nécessaire à la création d'un rapport d'activité.

3. Revue des données et création du rapport

a) Revue des données :

Une fois l'ensemble des données disponibles, celles-ci doivent être revues par une seconde personne (par exemple par le service d'Assurance Qualité) qui déterminera si les paramètres d'acceptation ont été atteints. Ce processus de revue documentaire doit être décrit dans une procédure et doit être basé sur une compréhension du procédé et de l'éventuel équipement utilisé afin de déterminer l'impact de la donnée sur la qualité du produit.

Il est important de distinguer cette revue du processus de la vérification 4 yeux évoquée plus haut. En effet, la vérification 4 yeux s'applique en temps réel lors de la génération de la donnée et porte sur l'action génératrice de la donnée. Elle est généralement effectuée par une personne du même service que la personne à l'origine de l'action. La revue, quant à elle, est faite à postériori et consiste à prendre acte du résultat, qu'il soit conforme ou non conforme, et à définir les actions dépendantes de ce résultat.

La revue des données s'accompagne dans certains cas de la revue de l'audit-trail du système ayant généré les données. Cet audit trail est une fonction d'enregistrement de chaque action réalisée sur le système répondant aux points suivants :

- Quelle action est réalisée ?
- Qui fait l'action ?
- Quand l'action est réalisée ?
- Les justifications appropriées en cas de modification ou d'interruption d'action
- Quelle était la précédente valeur en cas de modification ?

Afin de faciliter la lecture de l'audit trail il est nécessaire d'effectuer au préalable un travail de configuration de ce dernier(10). En effet, un audit trail non configuré peut, dans certains cas, générer plusieurs centaines de pages par lot et dans d'autres cas, ne générer aucune information.

Cette revue de l'audit-trail permet de s'assurer que les conditions opératoires ont été respectées et qu'aucune modification inappropriée des paramètres n'a permis de générer un résultat conforme alors que ce dernier aurait pu être non conforme si la procédure avait été respectée.

Date	Heure	Action	Login	Justification
28/08/2017	09:32	Connexion	TD862365	N/A
28/08/2017	09:34	Ouverture du menu "Paramètres" Sélection Recette N°1 Ouverture du menu "Analyse" Lancement de l'analyse	TD862365	Vérification des paramètres et lancement de l'analyse
28/08/2017	09:57	Fin de l'analyse	TD862365	N/A
28/08/2017	10:00	Ouverture du menu "Rapports" **Suppression du rapport "Analyse n°11"**	TD862365	N/A
28/08/2017	10:05	Ouverture du menu "Paramètres" Sélection Recette N°1 Modification de la durée d'analyse de "20min" à "15min"	TD862365	N/A
28/08/2017	10:08	Ouverture du menu "Analyse" Lancement de l'analyse	TD862365	N/A
28/08/2017	10:23	Fin de l'analyse	TD862365	N/A
28/08/2017	10:25	Ouverture du menu "Rapports" Impression du rapport "Analyse n°11"	TD862365	Impression du rapport final

Figure 5 : Exemple d'un audit trail d'un équipement analytique

Dans l'exemple ci-dessus, l'audit-trail permet de déterminer qu'une première analyse a été réalisée sans impression de rapport. Une seconde analyse a été réalisée en ayant modifié le temps d'analyse mais sans justifier ce changement de paramètre. On peut alors se demander si la suppression de ce premier rapport d'analyse ne cache pas des résultats qui auraient dû être revus. Il est à noter que sans cette revue d'audit-trail, il n'y a aucun élément permettant de déceler qu'un premier test a bien eu lieu mais n'a pas été imprimé avant d'être supprimé. Un audit trail n'est en aucun cas un logiciel d'espionnage afin d'imposer des cadences : celui-ci est uniquement conçu pour fiabiliser au mieux les données et faciliter les investigations en cas de déviation.

b) Création du rapport :

La création d'un rapport contenant l'ensemble des informations nécessaires doit permettre de prendre une décision. Ce rapport doit faire l'objet d'une procédure dont les principaux requis sont de :

- Définir le modèle du document
- Définir quelle donnée doit être inclue dans le rapport
- Décrire les décisions pouvant être prises sur base de ce rapport
- Définir les niveaux d'approbations nécessaires de ce rapport
- S'assurer que l'ensembles des données sont inclues, y compris les résultats non espérés
- Prendre en compte chaque annotation manuscrite sur le rapport
- Permettre l'investigation des résultats atypiques
- Décrire les actions correctives et préventives établies suites à des tests invalidés, erreurs ou répétition de tests

Ce rapport est ensuite approuvé (par le service d'assurance qualité) et sera nécessaire à la libération du lot s'il contient des données critiques pour la qualité du produit mis sur le marché.

4. Stockage et récupération

Une fois ce rapport émis et utilisé, il convient de le conserver en lieu sûr afin de pouvoir le récupérer en cas de demande d'un client ou d'une autorité de santé.

De même, les données brutes doivent être conservées. N'ayant subies aucune transformation, elles possèdent un risque d'erreur faible. En effet, chaque étape de traitement de donnée est susceptible d'induire des erreurs ou de diminuer la précision (par exemple : arrondi sur un résultat). En conservant les données brutes, l'entreprise pharmaceutique garde la source de son rapport. Ces données brutes sont de plus en plus souvent demandées en inspection réglementaire. Il n'est plus rare qu'un inspecteur fasse d'avantage confiance en celles-ci qu'au rapport.

La période de rétention légale des données pouvant être de plusieurs dizaines d'années, il convient de choisir des conditions et un support adapté afin de garantir la lisibilité de la donnée sur toute cette période. Ainsi, l'accès aux données et enregistrements doit être limité aux seules personnes autorisées. Des mesures adéquates de protection contre les dommages (par exemple : lutte contre l'humidité, le feu, les rongeurs) doivent être envisagées.

En cas de données électroniques, des procédures doivent être mises en place afin de garantir :

- La réalisation de sauvegarde en double afin de lutter contre tout désastre
- Le choix du support en fonction de la durée de stockage
- L'encryptage des données sensibles

Lorsque l'archivage des données est confié à un tiers, l'entreprise conserve la responsabilité de l'intégrité de ses données : elle doit ainsi régulièrement auditer les pratiques de son fournisseur de services. Un cahier des charges strict doit être rédigé afin d'établir les rôles et responsabilités de chacun. Celui-ci doit à minima contenir :

- Les procédures à suivre et la localisation des données
- La gestion des incidents
- Une stratégie de sauvegarde et de destruction des données

5. Destruction

Le processus de destruction d'une donnée doit permettre de s'assurer que cette dernière ne puisse être rendue disponible passée sa période de rétention. Cette période de rétention est définie dans la réglementation applicable (par exemple : Eudralex Volume 4), ou à défaut en fonction du type de données et de leur criticité.

Ce processus doit notamment être décrit dans une procédure qui détaille :

- La documentation nécessaire pour déterminer la période de rétention de chaque donnée
- Le personnel autorisé à réaliser la destruction de la donnée
- Les méthodes appropriées à la destruction des différentes données (électroniques versus papier)
- La revue du système générant la donnée pour s'assurer qu'elle ne soit plus disponible sur ce système

Cette destruction est néanmoins facultative : pour des raisons pratiques, une entreprise peut décider de conserver l'ensemble de ses données électroniques, auquel cas les requis sur l'archivage des données devront s'appliquer.

B. Les critères ALCOE+

Pour être considérée comme fiable, une donnée doit pouvoir répondre à un ensemble de critères regroupés sous l'acronyme ALCOE+ (ALCOA+ en anglais). Cet acronyme n'apparait pas en tant que tel au sein des GMP mais derrière chaque critère qui le compose se trouve de nombreux requis présents dans les GMP :

- Attribuable
- Lisible
- Concomitante
- Originale
- Exacte

ALCOE

WHO Guidance on good Data and Record Management Practices *2015*

- Cohérente
- Complète
- Disponible
- Durable

+

PIC/S Good Practices for Data Management and Integrity in regulated GMP/GDP environments *2016*

Au sein de ce chapitre, chacun de ces différents critères sera développé.

1. Attribuable

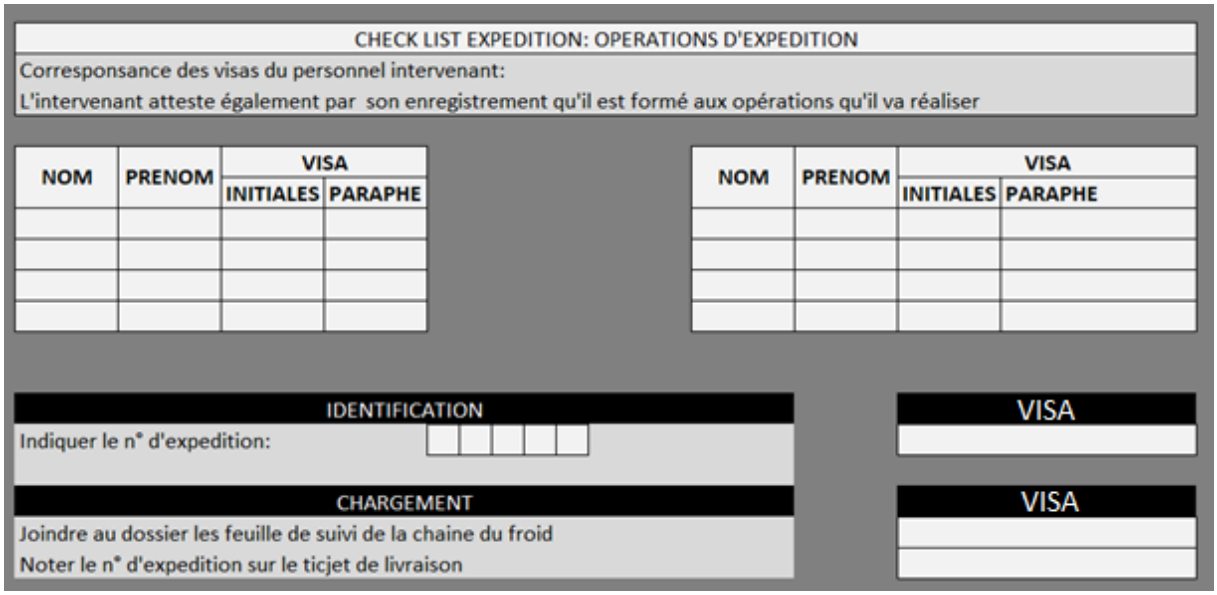
Une donnée doit être attribuable : cela signifie que pour chaque information obtenue il est nécessaire de pouvoir répondre à ces questions :

- Qui a réalisé l'action ?
- Qui a modifié la donnée ?
- Pourquoi cette donnée a-t-elle été modifiée ?
- Quand cette donnée a-t-elle été créée/modifiée ?

Système papier :

Dans le cas d'un système papier, l'opérateur doit s'identifier par la combinaison de ses initiales et de son paraphe pour chaque activité effectuée, ainsi que noter la date (et aussi l'heure si le document le demande) de réalisation de cette activité. Chaque modification doit être justifiée, signée et datée.

Ainsi, les documents papier doivent être conçus afin que chaque action soit clairement identifiable, par le biais d'une signature directement face à l'action ou, pour le cas où une page est complétée par une unique personne, grâce à une signature en bas de la page. Il doit, à tout moment, être aisé d'identifier les personnes sans ambiguïté, en attribuant des initiales uniques à chacun ou en jouant sur l'unicité de la combinaison initiales + paraphe. Ces informations seront présentes au niveau des ressources humaines pour qu'il soit possible de faire la correspondance avec ce qui est inscrit dans le document qualité. Une solution envisageable est d'ajouter sur la première page du dossier de lot, la liste des personnes ayant participées à la complétion de ce document et leur signature/paraphe afin de pouvoir relier la signature/paraphe au nom de cette personne.



CHECK LIST EXPEDITION: OPERATIONS D'EXPEDITION

Corresponsance des visas du personnel intervenant:
L'intervenant atteste également par son enregistrement qu'il est formé aux opérations qu'il va réaliser

NOM	PRENOM	VISA	
		INITIALES	PARAPHE

NOM	PRENOM	VISA	
		INITIALES	PARAPHE

IDENTIFICATION

Indiquer le n° d'expedition:

VISA

CHARGEMENT

Joindre au dossier les feuille de suivi de la chaine du froid
Noter le n° d'expedition sur le ticjet de livraison

VISA

Figure 6 : Exemple de document correctement conçu

Système électronique :

Pour un système électronique, celui-ci doit prévoir une identification de l'opérateur grâce à un identifiant et un mot de passe et enregistrer l'heure du système. Ce critère est à relier directement au 21 CFR part 11 de la FDA concernant la signature électronique de documents.

S'il existe actuellement sur le marché des appareils permettant de créer un compte unique pour chaque personne travaillant sur cet équipement, les systèmes les plus anciens ne permettent pas de créer autant de compte qu'il y a d'utilisateurs. Il existe alors des comptes dits « partagés » entre plusieurs utilisateurs ce qui n'est plus toléré suite à l'évolution des requis.

UNIT = 209891
USER = ADMIN
PROGRAM = PROG f t3 D
ID = 00-078 05/04/17
SAMPLE VOL = 1.0 CF SAMPLE = 1 COUNTS/CM

TIME	>0.5	>5.0	FLOW
10:49:19	0	0	1.00

Figure 7 : Exemple de donnée non attribuable

Dans l'exemple ci-dessus, l'appareil n'a pas été correctement paramétré puisqu'il existe un unique compte partagé (c'est-à-dire un compte utilisé par plusieurs personnes). Outre le fait que cet unique compte soit le mode administrateur et puisse donc changer tous les paramètres de marche, il est impossible de faire le lien entre le rapport et la personne réalisant l'action. De ce fait, chaque système informatisé doit être paramétré de sorte que chaque personne ait son propre compte avec les droits d'accès nécessaires à son activité.

L'utilisation de comptes partagés (par exemple : opérateur, technicien, superviseur) n'est tolérée que pour les systèmes dit « simples » pour les appareils de paillasse (par exemple : pH-mètre, thermomètre). En de telles circonstances, une contre-signature manuelle sur le rapport sera nécessaire. Attention cependant, le niveau d'accès « administrateur » ne peut en aucun cas être partagé.

Le partage de compte (suite à un oubli de mot de passe ou en attente de création de compte) peut être assimilé à une fraude. Il est ainsi nécessaire de remonter à son administrateur tout oubli de mot de passe et de faire le nécessaire pour qu'une personne ait accès à ses identifiants le jour de son arrivée sur le site.

L'utilisation d'un scribe (utilisation d'une seconde personne enregistrant l'action pendant que la première la réalise) est formellement interdite sauf lorsque le fait d'enregistrer l'activité entraine un risque pour le produit ou la sécurité du personnel. Typiquement, certaines activités réalisées en zone aseptique peuvent être enregistrées par un scribe afin de limiter le risque de contaminer le produit. L'utilisation d'un scribe peut également être justifiée en cas de manipulation de produits dangereux pour le personnel. Lorsque l'activité est terminée, scribe et personne ayant réalisé l'activité devront tous deux signer le document. Toute activité nécessitant l'utilisation d'un scribe doit être indiquée dans la procédure concernée.

En cas de donnée non attribuable, il est impossible de faire le lien entre l'action et la formation du personnel à l'origine de la donnée. Si la personne n'est pas formée, peut-on se fier à cette donnée ?

2. Lisible

Une donnée doit être lisible : durant tout son cycle de vie, la donnée doit pouvoir être extraite puis lue et comprise par une personne même étrangère à l'activité.

Système papier :

Pour les données papier, une procédure décrivant les bonnes pratiques documentaires permettent d'assurer cette propriété. Cette procédure doit s'assurer que :

- Les informations sont retranscrites de façon lisible et concise.
- Les documents sont remplis à l'encre indélébile (de préférence bleue).
- Le blanc couvrant n'est pas utilisé.
- Il n'y ait pas de surcharge (par exemple : rature illisible, écrire par-dessus une précédente valeur).
- Les ratures permettent la lecture de la précédente valeur.
- La nouvelle valeur est signée, datée et la raison du changement de valeur est expliquée en commentaire.
- Aucune abréviation non répertoriée dans la procédure n'est utilisée.
- Les formats de dates utilisés sont compréhensibles par tous (non correspondance entre une date au format français et au format anglais) et procédurés.
- Les documents sont paginés de façon à ce qu'une page manquante soit détectée.

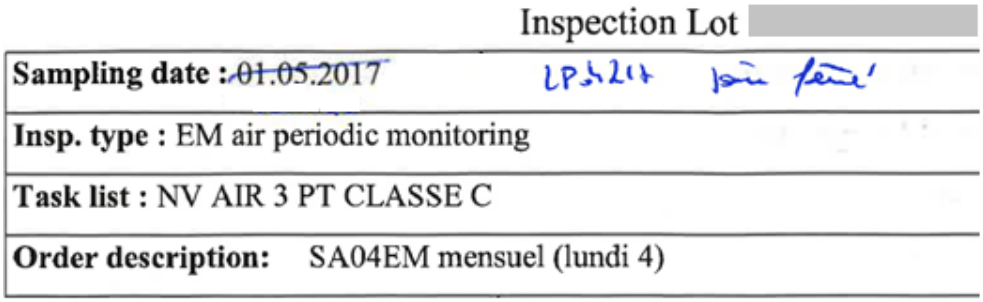


Figure 8 : Exemple de donnée papier non lisible

Dans l'exemple ci-dessus la nouvelle date n'est pas lisible : on lit "LP04217" au lieu de "28.04.2017". Cette mauvaise lisibilité peut entrainer des confusions et une incohérence dans le dossier de lot. De plus, la nouvelle date n'est pas signée, ce qui entraine un problème d'attribution de la donnée.

Systèmes électroniques :

Pour les données électroniques, il faut s'assurer de toujours disposer du logiciel permettant d'ouvrir les fichiers enregistrés. En effet, les données brutes ne sont pas souvent enregistrées dans des documents figés (exemple : fichiers PDF), mais dans des bases de données, et un changement de version du programme ou un déclassement de l'équipement peut entrainer la perte de lisibilité d'une donnée.

De plus, il faut toujours vérifier que les sauvegardes n'écrasent pas un précédent fichier afin de ne pas perdre d'information. Il convient ainsi de s'assurer que la mémoire de l'équipement permette de sauvegarder suffisamment de données et que ces données soient régulièrement transférées vers un espace de stockage de telle manière que des informations ne soient pas perdues faute de mémoire.

Une donnée illisible peut aboutir à une confusion et une prise de décision sur la base de valeurs erronées.

3. Concomitante

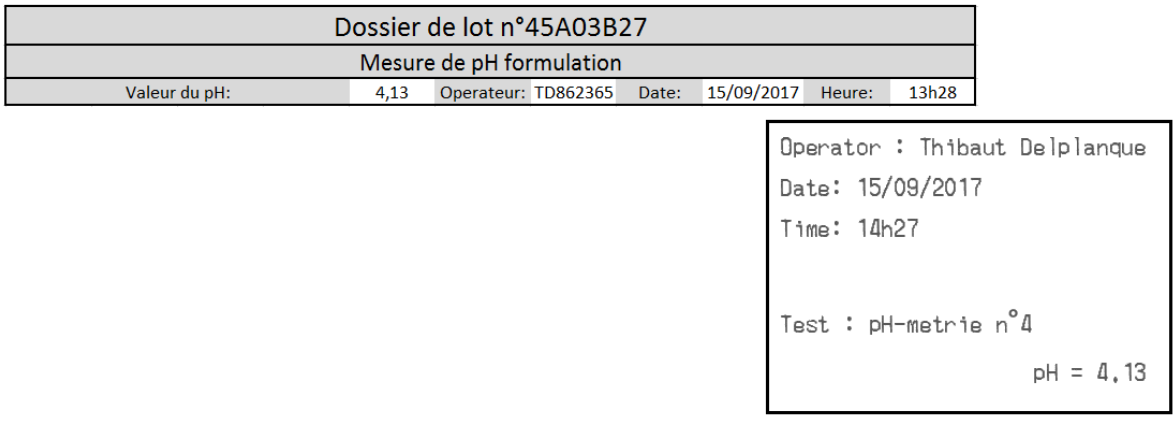
Une donnée doit être concomitante : pour chaque activité, la donnée doit être enregistrée en temps réel (au plus proche de l'activité d'un point de vue temporel).

Système papier :

Il convient ainsi de s'assurer que lors de toute activité nécessitant une inscription manuelle de l'heure, une horloge synchronisée à l'heure du site et validée soit visible par l'opérateur. L'utilisation de montre ou horloge du téléphone portable est proscrite car l'utilisation de ces systèmes n'est pas validée et que chacun est libre de modifier l'heure de ces équipements.

Systèmes électroniques :

Dans le cas des systèmes électroniques, ceux-ci doivent être validés afin d'enregistrer une heure qui ne puisse être modifiée par la personne réalisant l'activité. De plus, il est essentiel de réaliser un suivi périodique des équipements dont l'horloge n'est pas synchronisée avec une horloge de référence. Dans le cas contraire, une procédure doit régir la vérification périodique de l'heure sur chaque système, opération réalisable uniquement avec le statut d'administrateur (par exemple après les changements heure d'été/hiver).



Dossier de lot n°45A03B27							
Mesure de pH formulation							
Valeur du pH:	4,13	Operateur:	TD862365	Date:	15/09/2017	Heure:	13h28

Operator : Thibaut Delplanque
Date: 15/09/2017
Time: 14h27

Test : pH-metrie n°4
pH = 4,13

Figure 9 : Exemple de donnée non concomitante

L’exemple ci-dessus montre un pH-mètre dont la mise à l’heure n’a pas été effectuée. Dans ces conditions le ticket laisse penser que la mesure a été réalisée après avoir rempli le dossier de lot. Un auditeur pourrait suspecter que le dossier de lot est prérempli et que les mesures sont ensuite réalisées jusqu’à obtenir un résultat valide. Attention, une suspicion d’anticipation d’un résultat pourrait être perçue comme une fraude !

Une activité qui n’est pas enregistrée en temps réel peut engendrer des incohérences entre deux documents et remettre en cause toute une production liée à cette activité.

4. Originale

Une donnée doit être originale : il faut toujours conserver ses données brutes. En effet, chaque retranscription ou traitement de donnée risque d'engendrer des erreurs et il est donc vital de conserver la source d'information la plus précise.

Systèmes papier :

Afin de conserver ce caractère d'originalité de la donnée, l'usage de brouillon est proscrit : tous les résultats doivent directement être encodés sur le document officiel (par exemple : dossier de lot). En cas d'annotation sur un brouillon ou post-it, ceux-ci doivent être traités comme toute donnée : suivre le cycle de vie d'une donnée et être archivés pendant des années.

De plus, si le document utilisé est altéré (par exemple : projection d'acide, d'alcool, humidité, etc…) il est interdit de retranscrire les données sur un document « propre » puis de jeter l'ancien document. Il convient de photocopier/numériser la donnée brute, s'identifier sur la copie et conserver le document altéré en annexe.

L'utilisation de copie certifiée est acceptable mais doit être procédurée. La création d'une copie certifiée se réalise en plusieurs étapes :

- Une copie est réalisée par une première personne
- Une seconde personne compare l'original et la copie afin de déterminer si la copie préserve le contenu et le sens du document original
- Si la copie est identique à l'original, la personne ayant vérifié cette copie indique sur la copie qu'il certifie qu'elle est identique à l'original

L'aspect Original de la donnée s'exprime aussi à travers la validation du document utilisé. En effet, il est nécessaire de s'assurer que la version du document utilisé est bien la version effective. Dans le cas contraire, les informations présentes sur le document périmé utilisé pourraient être différentes de celles demandées par la version effective. Si le document est une procédure de travail, le déroulé des opérations pourrait avoir changé.

LSOP Local SOP	Approval Date:	31 MAY 2014
9000012345 version 08	Effective Date:	30 JUN 2014
Info Category: Proprietary	Next review Date:	30 JUN 2017

PROCEDURE DE GESTION DES DOCUMENTS GMP

Figure 10 : Exemple d'utilisation d'un document périmé

L'impression de certains documents clés (par exemple : dossier de lot) doit être procédurée et sécurisée de telle manière qu'il ne puisse y avoir une réimpression qui ne serait ni détectée ni autorisée. Une identification du document avec numéro unique sur chaque copie ou une impression uniquement accessible un service indépendant de la production sont deux solutions envisageables.

Systèmes électroniques :

Les systèmes informatisés doivent permettre la sauvegarde des données brutes de façon indépendante des rapports électroniques. En effet, un rapport est souvent enregistré dans un format statique (par exemple : format PDF). Ce format est peu adapté au retraitement de la donnée qui doit garder son caractère dynamique afin de pouvoir être réutilisée. Le cas le plus évident concerne l'intégration des pics lors de l'utilisation d'une HPLC (High Performance Liquid Chromatography) car cette étape d'intégration est fortement personne dépendante. De plus, une réintégration des pics ne sera pas toujours détectable sur le chromatogramme (rapport d'HPLC) quand celui-ci est imprimé.

Les documents électroniques utilisés doivent être mis à disposition sur un système sécurisé pour s'assurer que la version utilisée est la version effective. Il ne faut en aucun cas créer une copie de travail sur votre espace personnel car en cas de modification du document source, le document obtenu via le raccourci ne sera pas modifié. Dans le meilleur des cas le raccourci sera obsolète et ne pourra pas être utilisé mais dans certains cas il pourrait continuer d'ouvrir une version périmée du document.

La copie de données électroniques doit être limitée aux administrateurs du système et doit être procédurée.

5. Exacte

Une donnée doit être exacte : cela signifie qu'elle doit avoir la précision nécessaire à la prise de décision.

Comme vu lors du cycle de vie des données, la présence des métadonnées est nécessaire à la compression de l'information. Ainsi, pour garantir le caractère d'exactitude d'une information, il est nécessaire de toujours avoir à disposition l'intégralité des métadonnées.

Systèmes papier :

Les documents doivent permettre à l'opérateur de noter l'intégralité de l'information et être conçus de telle manière qu'il ne puisse y avoir de doute sur la manière d'inscrire la donnée sur un document. Ainsi, l'utilisation de « cases » permet de guider l'utilisateur.

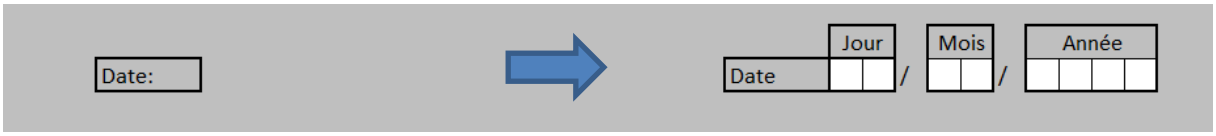


Figure 11 : Optimisation des champs d'un document

De plus, l'utilisation des règles d'arrondis et l'utilisation adéquate des chiffres significatifs doit être procédurée. Les personnes amenées à compléter un document doivent suivre une formation comportant plusieurs exemples sur les règles de calculs et d'arrondis.

Les documents ne doivent pas contenir de cases non renseignées. Si une opération ne doit pas être effectuée, l'utilisation du « N/A » (Non applicable) doit être procédurée.

Checklist des activités			
Liste des activités	Paraphe	Date	Heure
Activité 1	[illegible]	17/03/16	11H43
Activité 2			
Activité 3	[illegible]	17/03/16	14H27

Figure 12 : Exemple de donnée non exacte

Dans l'exemple ci-dessus, deux personnes ont réalisé des activités : l'une postée le matin a réalisé l'activité n°1, l'autre, posté d'après-midi a réalisé l'activité n°3.

Concernant l'activité n°2 il n'y a ni visa ni indication temporelle :

- Est-ce la personne postée du matin qui a oublié de renseigner son activité ?
- Est-ce la personne postée d'après-midi qui a oublié de renseigner son activité ?
- L'activité a-t-elle été réalisée ?

Systèmes électroniques :

L'ensembles des systèmes informatisés utilisés doivent être validés avant leur utilisation afin de s'assurer de l'exactitude des résultats générés et de leur reproductibilité.

Les niveaux d'accès doivent être correctement paramétrés et les champs non nécessaires à l'activité doivent être bloqués. Il convient ainsi de toujours travailler avec le niveau d'accès le plus bas possible, ceci afin d'éviter d'avoir accès à des options de configuration pouvant modifier le résultat d'une opération.

La génération de rapport doit elle aussi être validée afin de garantir que les données présentes sur le rapport sont bien celles enregistrées par l'appareil.

Une donnée présente mais non compréhensible se révèlera être plus difficile à défendre qu'une donnée non présente : l'opération a été réalisée mais le manque d'information soulève de nombreuses questions face à un inspecteur.

6. Cohérente

Une donnée doit être cohérente : cela signifie qu'une même information présente à deux endroits doit être différentes (hors arrondis). De plus, deux informations ne doivent pas être contradictoires.

Cette cohérence est directement impactée lors de l'encodage ou la retranscription d'une donnée, une erreur d'inattention pouvant entrainer la modification d'une donnée lors de son passage dans un système informatisé. L'ERP étant à la base de la prise de décision dans une majorité d'entreprise, la donnée erronée sera ensuite celle utilisée.

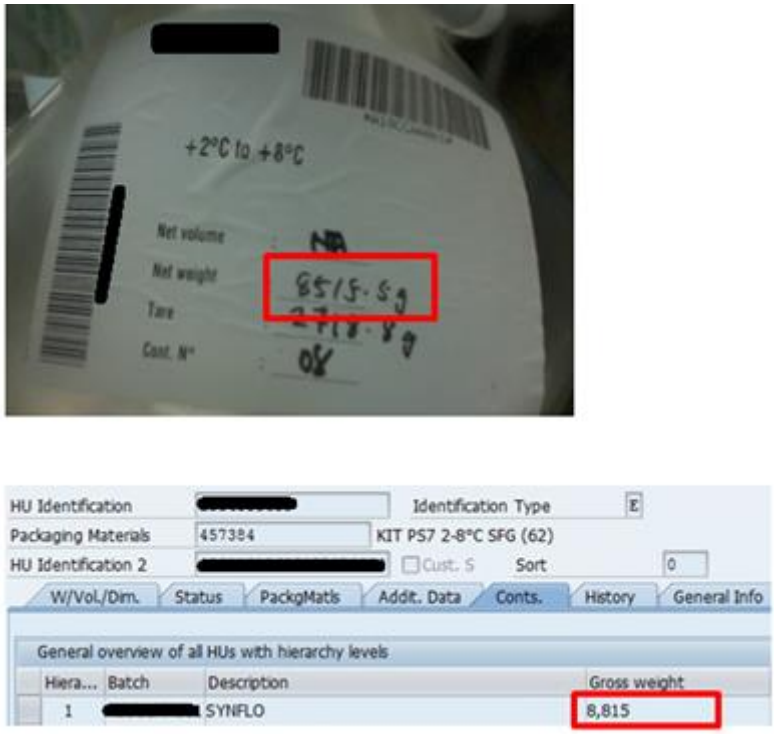


Figure 13 : Exemple de donnée non cohérente entre la base donnée informatisée et la retranscription papier

Afin de garantir la cohérence des actions de production, celles-ci doivent être réalisées dans un ordre logique et l'agencement des documents doit permettre de suivre cet ordre logique. Afin d'atteindre ce but, une connaissance du terrain ainsi qu'un travail en collaboration avec les utilisateurs du document final doit être mis en œuvre.

7. Complète

Une donnée doit être complète : l'ensemble des informations disponibles doit être présent pour pouvoir comprendre la donnée.

Toutes les pages d'un document GxP doivent être présentes et, dans le cas de rapports de tests, chaque résultat doit être disponible : qu'il soit valide, invalide ou annulé.

Test d'intégrité des filtres							
Status:	PASS	Operateur:	TD862365	Date:	12/05/2017	Heure:	21h37

Test d'integrite de filtre PALLTRONIC

Operateur : TD862365

Date : 12/05/2017 Heure:21h37

Test n°4

Status : PASS

Figure 14 : Exemple de donnée non complète

Dans l'exemple ci-dessus, un seul ticket est disponible sur le test d'intégrité de filtre. Ce ticket valide le test mais présente le numéro « 4 ». Or, il n'y a aucune trace des tests précédents. Un inspecteur se demandera si le test ne s'est pas avéré être « Fail » lors des trois premiers tests et qu'un quatrième test a été réalisé afin d'avoir un statut conforme.

Ne pas retracer les résultats invalides entraine un manque de transparence et engendrera une suspicion de fraude de la part des inspecteurs.

Afin qu'une donnée soit considérée comme complète, l'audit-trail du système informatisé doit être adjoint. Cet audit trail doit être clair, concis et compréhensible. Celui-ci doit être revu par la personne responsable de la revue documentaire afin de valider ou invalider un résultat. Un échantillon des audit trails générés par chaque système doit être revu par le service d'assurance qualité lors du processus d'audit interne.

8. Disponible

Une donnée doit être disponible : cela signifie que l'information doit être rapidement récupérable à toute étape de son cycle de vie, notamment lors de son archivage.

Les données doivent être stockées de manière organisée afin de pouvoir être consultées à tout moment : lors d'une inspection ou d'une investigation. En cas d'archivage des données hors du site, le cahier des charges contracté avec le fournisseur de services doit prévoir cette mise à disposition rapide des données.

Afin d'assurer que l'ensemble des rapports informatisés soit à disposition, la sauvegarde des opérations effectuées sur un système doit être automatique. A chaque intervention il est nécessaire que le système s'affranchisse des actions de l'opérateur pour sauvegarder ses résultats et que ceux-ci ne puissent être supprimés.

9. Durable

Une donnée doit être durable : cela signifie que l'archivage de la documentation doit être efficace. Ce critère est à mettre en corrélation directe avec la partie « stockage » du cycle de vie des données.

Cela implique que son support doit être durable dans le temps : il est par exemple impossible de stocker sur CD ou papier thermique des données devant être conservées 20 ans.

C. *Reconnaitre les écarts Data Integrity*

Il existe deux grands types d'écarts à l'intégrité des données(12) :

- Les erreurs : elles sont involontaires et nécessitent des actions correctives et/ou préventives afin de limiter leur probabilité d'apparition et leur impact.
- Les fraudes : elles sont volontaires et nécessitent des mesures disciplinaires

1. Risque d'erreurs

Le risque d'erreur peut être représenté, sous la forme d'un triangle ayant pour facteurs :

- Les requis : « Les procédures sont-elles claires et applicables ? »
- La justesse : « Les enregistrements reflètent-ils la réalité ? »
- La vérification : « Suis-je le seul à suivre l'action ? »

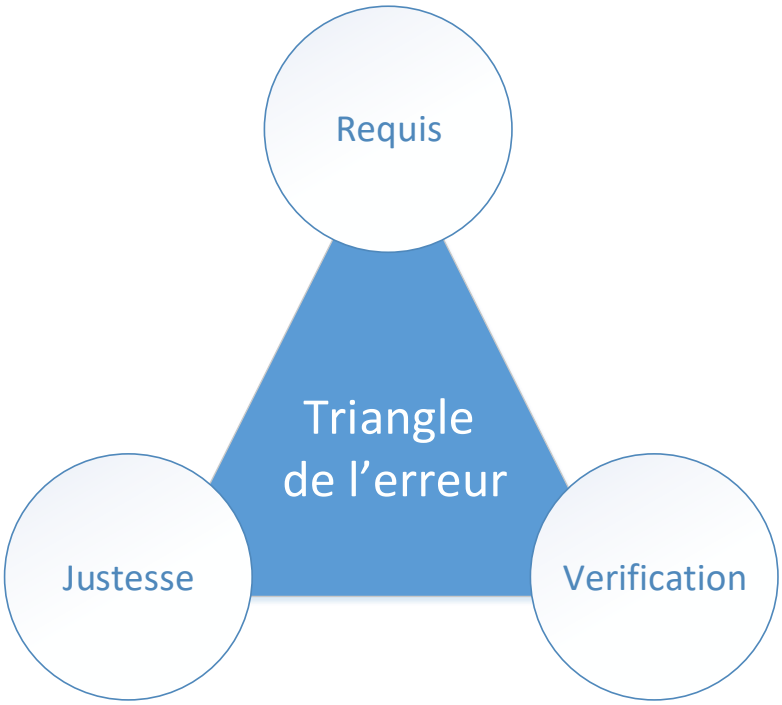


Figure 15 : Triangle de l'erreur

Les **requis** représentent l'ensemble des documents mis à disposition d'une personne pour lui détailler ce qu'elle doit réaliser et la manière de le réaliser, il s'agit le plus souvent de procédures. Ces documents se doivent d'être clairs et complets afin de ne pas laisser de place à l'interprétation : une personne tirant ses propres conclusions risque d'agir de façon différente par rapport à ce qui était attendu, ce qui peut engendrer des erreurs sans que cette personne ne s'en rende compte.

La j**ustesse** des enregistrements nécessite que ces derniers retranscrivent le plus précisément possible ce qui s'est réellement passé. Ce facteur est critique notamment dans les opérations manuelles où l'activité est dépendante de la personne : il est alors possible de réaliser des erreurs d'inattention ou de prendre une décision sans avoir toutes les informations à disposition.

Agir sur ces deux facteurs permet de diminuer la probabilité d'erreur.

La **vérification** des actions, données et enregistrements par une seconde personne permet d'augmenter la détectabilité d'une erreur et de diminuer son impact en permettant d'investiguer et de corriger l'erreur juste après son apparition.

L'un des messages clés de l'intégrité des données est qu'il nous arrive à tous de faire des erreurs mais qu'il est important de communiquer cette erreur. Chaque erreur est la source d'actions correctives et préventives nous permettant d'éviter, à nous même ainsi qu'aux autres, de reproduire cette erreur. Il est d'ailleurs de la responsabilité de la direction de l'entreprise de créer une Culture Qualité et une organisation qui favorisent la remontée des erreurs.

2. Risque de fraudes

Le risque de fraudes peut être représenté, comme le risque d'erreurs, sous la forme d'un triangle ayant pour facteurs :

- La pression : « Ai-je un intérêt à frauder ? »
- La justification : « Cela me dérange-t-il de frauder ? »
- L'opportunité : « Ai-je la possibilité de frauder ? »

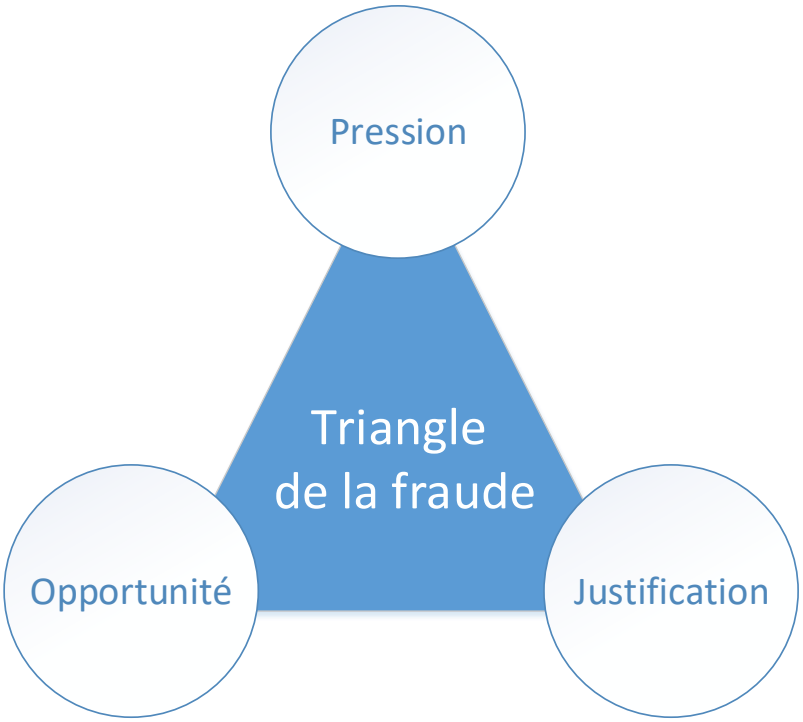


Figure 16 : Triangle de la fraude

La motivation d'une personne à frauder est en lien direct avec la **pression** qu'elle subit. Celle-ci peut provenir de la peur d'éventuelles sanctions dans un milieu où chaque action est tracée et évaluer sous la forme d'indicateurs de performance. Elle peut aussi provenir du management hiérarchique qu'elle soit réelle ou perçue (par exemple : date limite irréaliste, limitation de budget, charge de travail excessive).

La **justification ou rationalisation** est le résultat de l'attitude et de l'éthique/honnêteté d'une personne. De plus, nos activités sont parfois éloignées du patient et nous pensons donc, à tort, que celles-ci sont sans impact sur sa santé. Face à un problème nous réagissons tous de la même manière en nous comparant à

ce qui a déjà été vécu par d'autres et en cherchant une justification pour atténuer le problème et le rendre acceptable. Nous sommes tous tentés de nous dire « Si je remonte un problème, mon curseur passera dans le rouge, je ferai mieux de me taire. » ou « Pourquoi serai-je puni si mon collègue ne l'a pas été dans les mêmes circonstances ? ».

S'il peut être envisageable d'agir sur ces deux premiers facteurs (notamment en introduisant une culture qualité dans l'esprit de chacun) afin de briser ce triangle, il est nettement plus facile d'agir sur l'opportunité de fraude.

Cette **opportunité** se développe lorsque :

- Il n'y a pas ou peu moyen de contrôle sur les actions effectuées et que les conséquences d'une modification volontaire ne sont pas sévères pour la personne à l'origine de cette fraude. Il est ainsi aisé de limiter cette opportunité en introduisant des vérifications supplémentaires (notamment le vérification 4 yeux et la revue documentaire) mais aussi grâce aux enregistrements informatisés. Qu'il s'agisse d'un numéro d'incrémentation non modifiable ou d'une sauvegarde automatisée sans possibilité de suppression, ces moyens permettent de limiter le champ des possibilités de la personne réalisant l'action.

- L'accès aux données n'est pas suffisamment sécurisé : dans le cas des données électroniques, l'utilisateur de l'équipement possède niveau d'accès trop élevé qui lui permet de désactiver l'audit trail, modifier des paramètres, etc. Pour les données manuscrites, un système d'impression des documents de travail non sécurisé laisse l'opportunité de manipuler des données enregistrées au format papier.

Il est ainsi beaucoup plus simple d'apporter des solutions matérielles pour briser le triangle de la fraude que de parvenir à modifier le comportement de chacun. Si agir sur l'opportunité est nécessaire, elle n'est cependant pas suffisante car il est toujours possible de contourner les sécurités. Il est ainsi essentiel de faire évoluer les mentalités en développant dans l'esprit de chacun une culture Data Integrity. Si cette culture doit être partagée par tous, il est de la responsabilité du management de créer une culture d'entreprise et de la promouvoir quotidiennement.

TROISIEME PARTIE:
Développement d'une culture Data Integrity

Dans cette partie sera détaillée la mise en place d'un programme Data Integrity au sein d'un site de production pharmaceutique.

A. Gouvernance

1. Création de l'équipe projet et réseau d'experts

Le développement d'une culture qualité au sein d'un site impacte chacun des différents services qui le compose. Ce programme étant de grande envergure, il apparait nécessaire de constituer une équipe pouvant gérer cette tache sous la forme de gestion de projet.

Ainsi, l'équipe projet devra à minima réunir :

- Une personne ayant l'expérience du site : alliant connaissance de la partie production et de la partie qualité, cette personne est garante de la coordination des actions à mettre en place.
- Un expert de l'intégrité des données : responsable de la veille règlementaire et ayant une profonde connaissance des requis, cette personne est garante du respect des textes règlementaires.

A cette équipe projet il est nécessaire, selon l'envergure du site, d'y associer plusieurs experts capables de prendre en charge de grandes thématiques, notamment :

- Expert des documents : cette personne sera garante du déploiement des actions relatives à tous les enregistrements papier
- Expert des équipements : cette personne sera garante du déploiement des actions relatives à la fiabilisation des équipements générant des données électroniques.
- Expert IT : cette personne sera garante du déploiement des actions à mettre en place pour fiabiliser le logiciel de gestion du site.

- Expert Formation : cette personne sera garante du déploiement des formations nécessaires pour changer l'état d'esprit des personnes présentes sur le site

Le chef du projet « Data Integrity » sera la personne référente au sein du comité de direction du site pharmaceutique. En effet, la mise en place d'un tel projet impactant chaque personne présente sur le site, il est nécessaire que la direction soit au fait de l'état d'avancé des actions.

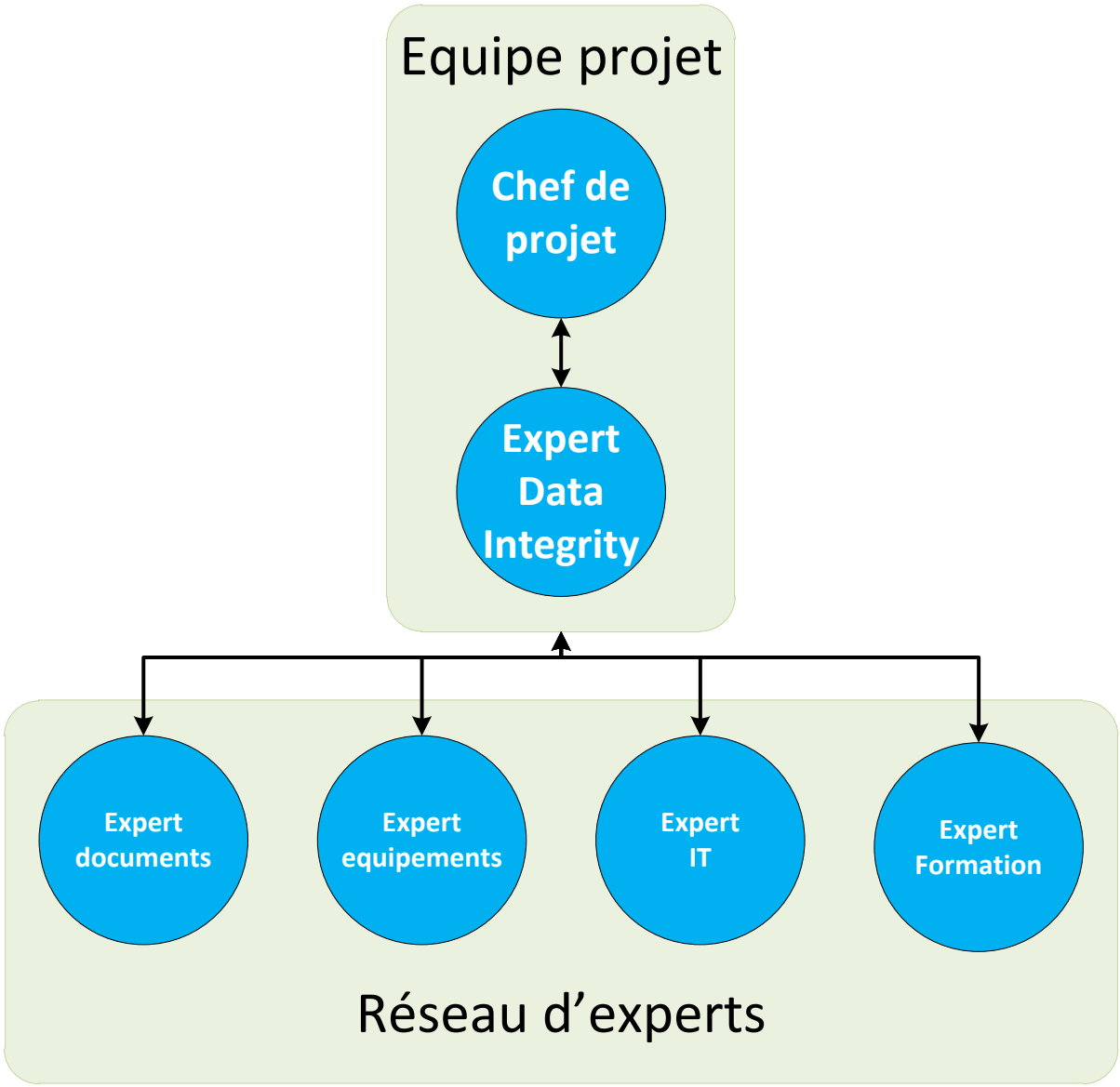


Figure 17 : Composition de l'Equipe Data Integrity

Ensemble, l'équipe et leurs experts auront la responsabilité de déployer les actions nécessaires et suffisantes pour assurer l'intégrité des données au niveau du site pharmaceutique.

2. Création d'une communauté

Selon l'envergure du site, il peut être intéressant de développer une communauté composée de relais présents dans chacun des services. Ces personnes auront un rôle décisif dans le développement du projet, notamment en :

- Remontant les spécificités de leur service à l'équipe projet : en travaillant quotidiennement au sein de leur service, ces relais maitrisent l'ensemble des documents et systèmes utilisés. En outre, ils connaissent mieux que quiconque les éventuels écarts présents sur le terrain.

- Déclinant les informations de l'équipe projet à leur service : les messages sont souvent bien mieux acceptés lorsqu'ils viennent d'une personne du même service.

- Aidant quotidiennement leur service : formés à Data Integrity mais aussi à leurs activités quotidiennes, ces relais seront les plus à même de répondre aux questions de leurs collègues.

- Mettant en place les actions correctives et préventives proposées suite à l'évaluation des systèmes papier et informatisés.

Apportant ainsi une vision sur l'ensemble des services du site, ces relais doivent faire partie intégrante du projet et seront régulièrement consultés par l'équipe projet. Une réunion rassemblant l'ensembles des relais permet à chacun de partager les difficultés de son service. Ainsi, l'ensemble de la communauté Data Integrity peut réfléchir aux actions à mettre en place afin de résoudre ces difficultés, harmoniser les pratiques entre les différents services et partager les bonnes pratiques.

La majorité du travail reposant sur les épaules de ces personnes, il apparait ainsi essentiel de fédérer cette communauté afin que l'ensemble de ses membres se sente impliqué dans le développement d'une nouvelle culture qualité.

3. Evaluation de l’état d’esprit du site et plan d’actions

Selon l’échelle du site, un tel projet pouvant durer des mois voire des années, il convient de réaliser un état des lieux de l’état d’esprit du site en matière d’intégrité des données, en début de projet. Cet état des lieux permettra de déceler les lacunes du site et de prioriser les actions à implémenter.

Le GAMP5 (11) définit un modèle d’évaluation de la maturité de l’intégrité des données sur une échelle à 5 niveaux :

- Niveau 1 : Aucun programme d’intégrité des données
- Niveau 2 : L’intégrité des données est en partie définie mais il n’existe aucun contrôle et les actions sont personne dépendantes
- Niveau 3 : Le programme est défini mais son application n’est pas systématique
- Niveau 4 : Le programme est défini et suivi par l’ensemble du personnel
- Niveau 5 : Il existe un programme d’amélioration continue de l’intégrité des données et la société est force de proposition pour le secteur pharmaceutique

Ce modèle s’accompagne d’un questionnaire où chaque point est évalué selon les 5 niveaux de criticité, les thèmes suivants sont examinés :

- Culture
- Gouvernance
- Programme Data Integrity
- Affaires Réglementaires
- Cycle de vie des données

Sujet concerné	Facteur de maturité	Caractérisation du niveau de maturité				
		Niveau 1	Niveau 2	Niveau 3	Niveau 4	Niveau 5
Culture						
Connaissance et compréhension de l'intégrité des données	Connaissance de l'importance de l'intégrité des données et compréhension des principes	La connaissance du sujet est limité à l'équipe projet.	Connaissance générale du sujet mais qui ne se reflete pas dans les pratiques.	Les principes sont connus mais ne sont pas systématiquement appliqués.	Les principes sont pleinement appliqués .	Programme de maitrise de la connaissance en place. L'entreprise est au courant du développement du sujet au sein de l'industrie pharmaceutique.
Culture de la société et cadre de travail	Une culture de la libre remontée des erreurs, omissions et résultats atypiques. Une envie de participer aux objectifs Data Integrity.	Réticence à remonter tout résultat suspect.	Les problèmes peuvent être remontés mais aucune action de mitigation n'est mise en place.	La politique et les procédures encouragent à remonter les résultats suspects mais leur suivi est service dépendant.	La direction montre l'exemple et les actions de mitigation sont systématiquement déployées.	L'entreprise anticipe de potentielles faiblesses et applique des controles appropriés.
Culture Qualité	Un envrionnement dans lequel les employés ont l'habitude de suivre des règle de qualité et où chaque actions est pensée en terme de qualité.	Peut de connaissance de la culture qualité. N'est remonté que ce que la direction souhaite entendre.	L'usage des bonnes pratiques est personne dépendant.	Les bonnes pratiques sont suivies par tous mais pas de manière constante.	Les bonnes pratiques sont constamment suivies.	Il existe un programme de développement de la culture qualité au sein de l'entreprise.

Figure 18 : Exemple d'évaluation du niveau de maturité du site selon le GAMP 5

Suite à cette première évaluation, un plan global d'actions doit être détaillé afin que la direction soit au fait des différentes actions à mener et du temps nécessaire à la réalisation de ces actions. L'ensemble de ces actions doit s'accompagner d'un chiffrement en ressources humaines et matérielles.

Une des stratégies possibles est de suivre le plan de cette partie et de décliner le projet en trois piliers :

- Gouvernance : préparation et suivi du projet
- Education et Formation : ensemble des actions permettant à l'état d'esprit du site d'évoluer
- Process et systèmes : ensemble des actions nécessitant de travailler sur la documentation, les processus et les systèmes informatisés

4. Communication

Développer une nouvelle culture et imposer de nouvelles exigences réglementaires n'est pas aisé, il faut lutter contre la résistance au changement. Il est ainsi fondamental que chaque personne présente sur le site comprenne pourquoi il est nécessaire de changer les mentalités car il ne s'agit pas uniquement de réduire les risques actuels mais de prévenir les éventuelles futures erreurs.

Ainsi le lancement du projet devra s'accompagner d'une communication permettant d'expliquer l'intégrité des données, la nécessité de travailler sur ce sujet, les personnes faisant partie du projet ainsi que les résultats espérés. Tout moyen de communication possible est à envisager, qu'il s'agisse de réunions, du journal de la société, de communication numérique (par exemple : mails et intranet de la société) de message sur les écrans et de distribution de prospectus.

Suite au lancement du projet, l'effort de communication doit persister afin que l'engouement suscité par le lancement d'un tel projet perdure. En effet, un tel projet s'échelonne sur plusieurs mois/années et nécessite de nombreuses ressources sans autre récompense que le fait de ne pas avoir de problème. Face à de fortes exigences sans retour immédiat sur investissement, nombreux sont ceux qui peuvent baisser les bras et le fait de communiquer sur les réussites du projet permet de rassurer ceux-ci.

Enfin, comme nous avons tous le droit à l'erreur mais qu'il est essentiel qu'une même erreur ne se reproduise pas, la communication périodique d'une mauvaise pratique retrouvée sur le site peut être une solution envisageable. Cette dernière n'a pas pour but de fustiger la personne à l'origine de la mauvaise pratique mais doit permettre d'exposer la problématique, d'expliquer pourquoi celle-ci est un écart d'intégrité des données, de détailler les éventuelles conséquences en matière d'impact qualité et patient et enfin de définir la marche à suivre ou ce qu'il aurait fallu faire. Cette communication est créée par l'équipe projet en concertation avec sa communauté puis partagée directement entre les différentes équipes grâce aux membres de la communauté.

B. Education et formations

Si la mise à niveau des systèmes est importante pour garantir l'intégrité des données, l'éducation du personnel est essentielle. A ce titre, chaque personne présente sur le site doit être formée à la culture qualité ainsi qu'à l'intégrité des données.

1. Développement de la culture de la transparence

Cœur de l'intégrité des données et pilier essentiel de la culture qualité, la culture de la transparence doit être promue quotidiennement afin que celle-ci soit adoptée par chacun. Il est normal que des erreurs ou des résultats non espérés surviennent et ceux-ci doivent être remontés afin de pouvoir investiguer leur cause et évaluer leur impact sur la qualité du produit.

Ainsi, chaque employé devra suivre annuellement un code de bonne conduite reprenant les principes éthiques auxquels l'entreprise adhère. En suivant cette formation, le personnel s'engage à respecter les différents principes de savoir vivre en communauté, respects des données confidentielles, respect du patient et principes de la transparence. Afin de faciliter la remontée des évènements indésirables, la hiérarchie doit elle-même comprendre que les erreurs techniques et humaines sont possibles et qu'il est préférable de les solutionner plutôt que de les taire.

Outre une formation ponctuelle, il est conseillé d'encourager le maintien de cette culture de la transparence autour de différentes communications (notamment de la direction vers les équipes) mais aussi en encourageant la remontée de ces erreurs plutôt qu'en blâmant les services susceptibles de générer le plus de déviations. S'il est parfois difficile de résoudre une problématique seule, en se concertant avec d'autres services il est probable de trouver une solution ensembles.

Enfin, comme suggéré par le PIC/S, un processus de remontée anonyme des problèmes peut être envisagé afin de palier à un défaut d'encadrement. Les problèmes remontés par ce processus doivent être étudiés par une équipe libre de tout conflit d'intérêt et exposés à la direction du site.

2. Formation du personnel

Chaque personne présente sur le site doit se voir attribuer un parcours de formations adapté à ses besoins. Ainsi, plusieurs formations concernant l'intégrité des données seront dispensées par la communauté mais aussi par l'assurance qualité.

- Formation Bon Remplissage des Documents : cette formation destinée à toute personne sur le site pouvant remplir des document GMP permet d'aborder l'intégrité des données au niveau pratique. Cette formation permet à tout le personnel du site de connaitre les bases de l'intégrité des données, de l'ALCOE+ et offre des exemples pratiques de comment bien remplir ses documents au quotidien.

- Data Integrity Learning Map : cette formation destinée au personnel encadrant permettra de définir l'intégrité des données au sein du processus de gestion des équipes. Le message essentiel est que chaque encadrant doit s'investir auprès de ses équipes afin de permettre à tous de diminuer les écarts relatifs à l'intégrité des données. Comme vu précédemment, la pression exercée sur chacun est en lien direct avec le risque de fraude. Il ne faut pas penser que productivité mais laisser à ses équipes le temps de bien travailler et remplir correctement les documents. Il est conseillé de ne pas envisager cette formation comme une transmission verticale de connaissance mais de profiter de cette occasion pour développer un espace de partage où chacun puisse faire profiter les autres de ses propres expériences.

- Formation Auto-inspection : afin de pouvoir fiabiliser les processus générant des données, il est essentiel que chacun puisse remonter les écarts et les risques possibles au sein de son secteur. Ainsi, chaque personne participant à des auto-inspection au sein de son service sera formé aux principes ALCOE+ et à la remontée de ces écarts.

En outre, chaque membre du personnel doit suivre, annuellement, une formation aux bonnes pratiques de fabrications. Cette formation devra contenir un chapitre sur les

bonnes pratiques de l'intégrité des données et notamment insister sur la culture de la transparence.

3. Création et mise à jour des procédures

a) Procédure Data Integrity :

Afin d'intégrer l'ensemble des requis Data Integrity au sein du système qualité de l'entreprise, il est essentiel de rédiger une procédure définissant l'architecture du programme sur le site. Cette procédure peut être scindée en deux grandes parties :

- Gouvernance : cette première partie détaille l'ensemble des objectifs, des responsabilités de chacun et des moyens mis en œuvre sur le site pour obtenir des données intègres.

- Cycles de vies des données : pour plus de lisibilité, les données papier et électroniques peuvent être fractionnées en deux sous parties. Dans cette partie, il est conseillé de reprendre le cycle de vie d'une donnée et pour chaque étape, d'y joindre l'ensemble des requis et des procédures présentes sur le site et permettant d'y répondre. Cette partie permet d'avoir une cartographie complète des différentes procédures permettant l'intégrité des données papier ou électroniques sur le site.

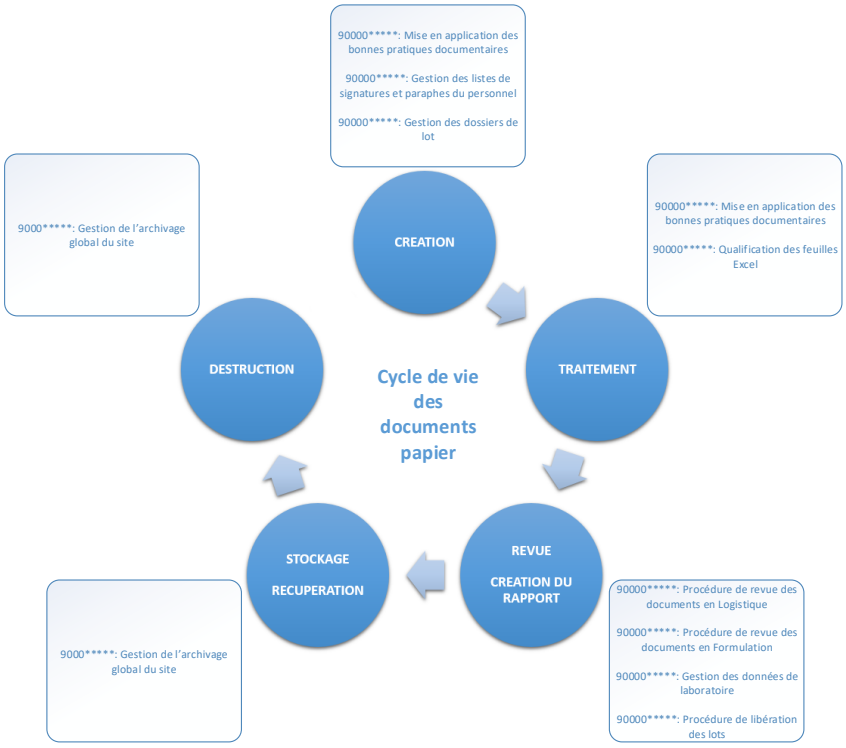


Figure 19 : Exemple du cycle de vie appliqué à un site pharmaceutique

b) Procédure des systèmes papier :

La procédure des bonnes pratiques documentaires est l'un des documents clé du système qualité. Présente dans le profil de formation de chaque employé, cette procédure décrit les règles à respecter pour s'assurer que les documents GMP sont utilisés et complétés de façon à garantir leur fiabilité. L'ensemble des principes Data Integrity propres à la documentation papier sont retrouvés dans cette procédure :

- Pagination
- Encre indélébile
- Information claire et lisible
- Règles pour éventuelles modifications
- Date et signature

Il est conseillé d'apporter une liste d'exemple pratiques au sein de cette procédure afin de guider les employés au quotidien :

- Que faire en cas de document perdu.
- Que faire en cas de document détérioré.

- Quelles sont les règles d'arrondis et d'utilisation des chiffres significatifs.
- Quels sont les formats de dates et heures applicables au sein de la société.
- Comment réaliser une copie certifiée conforme à l'original.

c) Procédures des systèmes électroniques :

Afin de garantir le caractère attribuable des données il est essentiel que chaque système possède une liste de comptes permettant à chacun de travailler avec ses propres identifiants. Une procédure devra définir et décrire les mesures à mettre en place pour gérer la création des accès pour chacun.

Il est à noter que la liste actuelle et historique des utilisateurs de chaque équipement peut être demandée ce qui nécessite d'avoir une complète traçabilité. Certains systèmes ne permettant pas de conserver la liste des comptes inactivés, il peut être judicieux de garder cette traçabilité sous format papier en utilisant un formulaire papier pour chaque demande de création/inactivation d'accès.

Une procédure de gestion des alarmes doit être en place sur le site pour définir et décrire la stratégie du site concernant chaque type d'alarme, qu'elle soit relative à la sécurité du personnel, à la qualité du produit ou simplement du maintien en bon état de l'équipement. Ainsi, chaque problème doit faire l'objet d'une évaluation par une équipe pluridisciplinaire afin de catégoriser ce problème et de définir quel type d'alarme doit être instaurée face à ce problème.

Une procédure de gestion des audit trails doit être en place sur le site pour définir et décrire la stratégie du site concernant chaque type d'audit-trails mis en place sur les équipements générant des données. L'une des stratégies possibles est de définir deux types d'audit trail par équipement :

- Audit trail complet : remontant l'ensemble des informations, cet audit trail est peu pratique pour être revu au quotidien mais sera fort utile en cas d'investigation.
- Audit trail GxP : cet audit trail ne remonte que les données critiques, permettant une revue rapide par les équipes opérationnelles.

Enfin, selon la criticité des informations remontées, la revue procédurée de ces audit trails peut être :

- Systématique après chaque production
- Périodique de façon mensuelle ou trimestrielle
- Uniquement pour investigation

C. *Process et systèmes*

1. Evaluation des systèmes papier

Lors d'une inspection réglementaire, les systèmes papier sont le plus souvent au cœur des préoccupations et il appartient à chaque laboratoire de s'assurer que ses documents répondent aux requis de l'intégrité des données.

L'analyse de chaque document étant un travail laborieux, il est conseillé de mettre le focus sur les processus ayant le risque connu/perçu le plus élevé et générant des données critiques (dossiers de lots, analyses du laboratoire de contrôle qualité) : ce risque peut être remonté à travers des observations d'audits ou de tout autre mécanisme. Chaque secteur doit donc identifier les documents GxP vitaux qui seront analysés.
Cette analyse doit porter sur le format du document, les procédures associées ainsi que sur l'analyse des pratiques quotidiennes. Il est donc recommandé d'utiliser un dossier de lot rempli afin de pouvoir analyser si les pratiques correspondent aux procédures.

L'équipe chargée de l'évaluation doit être constituée de personnes ayant l'expérience, les compétences, la connaissance et le comportement adapté afin d'être capable de travailler collectivement et de comprendre la perspective de chacun. Il faut à minima réunir :

- Un responsable du service documentation : propriétaire du système, celui-ci est responsable du suivi du planning, de l'organisation des séances de travail et de la mise à jour de la documentation.

- Un expert Data Integrity : son rôle sera celui de facilitateur. Ayant la connaissance des requis il sera à même d'identifier les risques, donner des conseils et proposer des solutions.

- Un membre de la production : cette personne à une profonde connaissance du processus et complète la documentation chaque jour. Son expertise permet d'évaluer si les pratiques quotidiennes son en adéquation avec les requis procédurés.

- Un membre de la qualité opérationnelle : allant de pair avec la personne de production, cette personne pourra challenger les différents intervenants et évaluer si les solutions proposées seront efficaces.
- Un responsable du service concerné : ayant la connaissance de l'ensemble du processus, celui-ci peut évaluer l'impact d'un changement sur les processus en amont et en aval du changement.

Ensemble, les différents membres de l'équipe analyseront le document directement sur le terrain afin de s'assurer de comprendre comment celui-ci est utilisé par les différents intervenants. Afin de faciliter cette analyse, il peut être nécessaire de diviser un même document en plusieurs sections (chacune correspondant à une salle/zone).

.

Les questions ci-dessous sont nécessaires mais non exhaustives à l'évaluation de ces systèmes :

- Identification :
    - Ce document possède-t-il tous les attributs nécessaires à son identification ?

      Chaque page doit posséder les éléments suivants :
        - L'identifiant unique du document
        - La version du document
        - Un numéro unique d'impression
        - Une pagination sous la forme "x" sur "y"
    - Ce document, ou n'importe quelle partie de ce document, peut-il provenir d'un scan, photocopie ou impression non contrôlée ?

- Enregistrements :
    - Les métadonnées sont-elles présentes et suffisantes pour donner un sens à la donnée ?

- Les unités sont-elles enregistrées selon le système ISU (par exemple s = seconde) ?
- La donnée est-elle transcrite dans un document intermédiaire avant d'être enregistré dans son document final ?
- Le support d'enregistrement se dégrade-t-il avec le temps ?
- Des abréviations non procédurées sont-elles utilisées ?
- Une encre indélébile est-elle utilisée ?
- En cas de copies, sont-elles certifiées conformes à l'original, tant sur le fond que la forme, par le biais d'un commentaire manuscrit ou d'un tampon ? Chaque page doit être attestée séparément.

- Heures et dates :
    - Le document est-il conçu pour permettre l'enregistrement de la date/heure dans le format requis par les procédures locales ?
    - La date/heure est-elle enregistrée au moment de l'action associée ?
    - L'horloge est-elle facilement visible à l'endroit où l'enregistrement de l'activité à lieu ?

- Calculs :
    - Les étapes du calcul sont-elles clairement définies sur le document ou dans la procédure associée ?
    - La revue d'un calcul critique est-il réalisé avant qu'une action ou décision ne soit prise sur la base du résultat de ce calcul ?
    - Le format du document permet-il d'appliquer les arrondis et d'enregistrer la donnée avec le bon nombre de décimales ?

- Signatures :
    - Le document est-il rempli à l'endroit de l'activité ?
    - La personne signant le document est-elle la personne ayant réalisé l'activité ?
    - En cas d'utilisation de scribe, la procédure décrit-elle ce rôle ?
    - Les signatures requises pour une étape sont-elles enregistrées avant de passer à l'étape suivante ?
    - L'utilité d'une seconde signature/vérification 4 yeux est-elle clairement indiquée sur le document ?

- Champs libres :
    - Existe-t-il un espace réservé aux commentaires ?

Chaque document ainsi évalué doit faire l'objet d'un rapport consignant l'ensemble des réponses obtenues, des éventuels commentaires ainsi que des actions proposées pour limiter le risque d'erreur.

2. Evaluation des systèmes informatisés

En complément de l'évaluation des systèmes documentaires papier, une évaluation des systèmes informatisés doit être réalisée.

Afin d'optimiser l'utilisation des ressources matérielles et humaines à disposition, une classification des systèmes selon le risque potentiel d'impact sur les données, peut être appliquée :

- Haute priorité : Système ayant des comptes partagés ou étant stand-alone
- Priorité modérée : Petits équipements de laboratoire
- Faible priorité : Systèmes ayant des comptes individuels et connectés au réseau d'entreprise

L'équipe chargée de l'évaluation du système devra être composée, à minima, d'un expert Data Integrity, d'un expert du terrain et d'un automaticien spécialiste de l'équipement. Ensembles, ceux-ci devront vérifier directement sur l'équipement (et à l'aide des documents de validation) si celui-ci est conforme aux requis réglementaires. Lors de cette évaluation, il est conseillé d'opposer la théorie présente sur les documents de validation à la pratique terrain en essayant d'utiliser le système afin de déceler d'éventuelles failles dans la validation du système.

Les questions ci-dessous sont nécessaires mais non exhaustives à l'évaluation de ces systèmes :

- Accès et sécurité :
    - L'accès au système/logiciel est-il contrôlé par des identifiants uniques ?
    - Le système dispose-t-il d'une fermeture de session automatisée en cas de période d'inactivité prolongée ?
    - En cas d'accès à distance par le personnel ou le fournisseur, cet accès est-il contrôlé de manière appropriée ?

- Existe-t-il un processus documenté qui assure que seuls les utilisateurs formés et qualifiés ont accès au système/logiciel et que leur accès est supprimé dès lors qu'il n'est plus nécessaire ?
- Les utilisateurs ont-ils uniquement accès aux fonctions appropriées et nécessaires à leur travail ?
- Une personne ayant un potentiel conflit d'intérêt peut-elle modifier ou supprimer les données ?
- Une personne ayant un potentiel conflit d'intérêt peut-elle modifier la configuration/recette/paramètres critiques/alarmes critiques/paramètres validés/méthode ?
- Les niveaux d'accès au système sont-ils documentés dans un document approuvé ?
- Si des comptes administrateurs existent, leur nombre est-il limité au minimum nécessaire ?
- Le système permet-il de visualiser la liste actuelle et passée des utilisateurs ainsi que leur niveau d'accès ou existe-t-il une procédure contenant ces informations ?

- Enregistrements des données :
  - Existe-t-il un propriétaire responsable des données générées/conservées par le système ?
  - Si la même information est enregistrée plus d'une fois, la donnée originale est-elle désignée par un document validé ?
  - La donnée utilisée pour prendre une décision qualité provient-elle de la source la plus appropriée (source la plus complète et précise) ?
  - Si un rapport papier ou PDF provenant du système est utilisé pour prendre une décision qualité, existe-t-il un document validé démontrant que le contenu du rapport est similaire à la donnée format électronique ?

- Les données sont-elles enregistrées et sauvegardées au moment de leur création ?
- Les données sont-elles sauvegardées automatiquement au sein du système par un processus validé (ne pas avoir besoin d'une sauvegarde manuelle) ?
- Le système sauvegarde-t-il toutes les métadonnées nécessaires à la compréhension des données ?
- Est-il possible de répéter un test ou une action dans le but d'arriver au résultat espéré ou de modifier une donnée afin d'avoir un résultat conforme ? Si la répétition est possible, existe-il des contrôles permettant de détecter cette action ?
- Les horloges du système (heure et date) utilisées pour l'horodatage sont-elles ajustées par synchronisation automatique ou de manière procédurée ?

- Revue des enregistrements :
    - Existe-il une procédure décrivant la revue et l'approbation des enregistrements de données (données brutes, métadonnées, modifications des enregistrements) ?
    - Si les données électroniques sont modifiables, un audit trail est-il mis en place (qui/quand/raison du changement/sauvegarde de la précédente donnée) ?
    - Si des données peuvent être créées, ces données sont-elles attribuables à la personne réalisant l'action génératrice de données ?
    - Les audits trails sont-ils sécurisés de manières à ce qu'ils ne puissent pas être désactivés/modifiés/supprimés ?
    - Si une revue de l'audit trail est nécessaire, les personnes responsables de cette revue sont-elles formées ?

- Validation du système :

    - Les paramètres du système sont-ils définis et testés/validés afin de s'assurer qu'ils ne puissent être modifiés ?

    - Si les données sont sauvegardées ou transférées sur un système externe, la sauvegarde/transfert est-elle validée ?

    - Les changements de configuration/paramètre validé/méthode sont-ils uniquement autorisés après une procédure de change control/revue par l'assurance qualité ?

- Stockage et archivage :

    - Existe-t-il des procédures définissants les périodes de stockage des données au sein du système et le système est-il en accord avec ces procédures ?

    - Les données sont-elles sauvegardées/copiées automatiquement ou de façon procédurée afin de minimiser le risque de perte ?

    - En cas de backup, sont-ils sécurisés de façon à empêcher toute modification/suppression ?

    - Si un système d'archivage est en place, peut-on retrouver et lire une donnée archivée pendant toute sa durée d'archivage ?

    - Si les données sont archivées chez un tiers, la propriété et le processus de récupération sont-ils bien définis et documentés ?

Chaque système ainsi évalué doit faire l'objet d'un rapport consignant l'ensemble des réponses obtenus, des éventuelles stratégies de mitigation du risque mises en place ainsi que des actions proposées pour limiter le risque d'erreur.

La nécessité de revoir l'audit-trail d'un équipement devant être documentée, celle-ci doit être évaluée et basée sur le risque d'une éventuelle modification pouvant altérer les données. Si en théorie la revue de l'ensemble des audit trails à chaque lot produit

peut-être un choix judicieux, il s'avère que dans la pratique cette activité est fortement chronophage et parfois peu pertinente.

Attention cependant, ceux-ci doivent être correctement paramétrés afin de seulement remonter les informations essentielles à l'évaluation de la qualité de produit pour ne pas que leur revue soit fastidieuse.

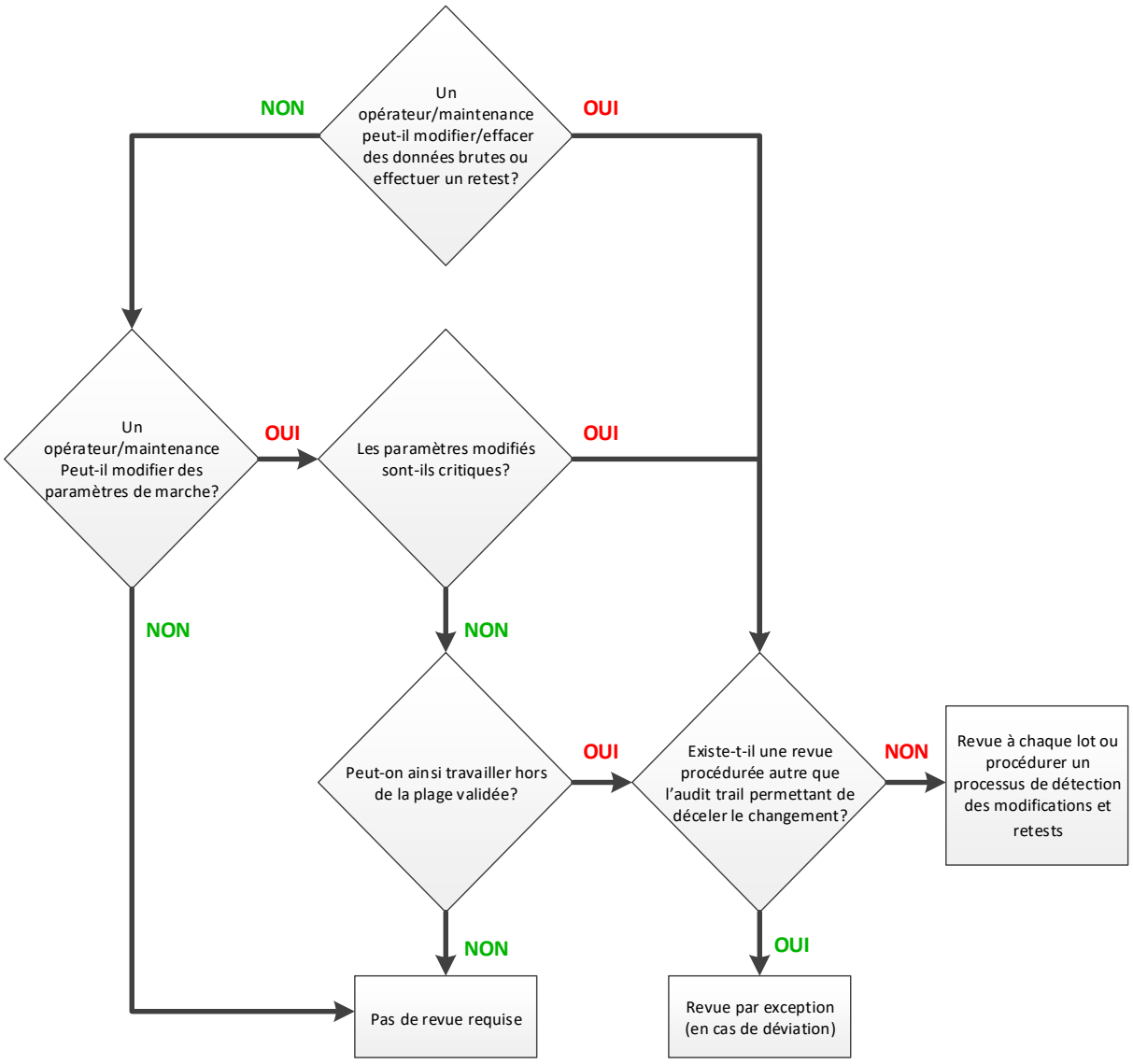


Figure 20 : Exemple d'évaluation de la nécessité de revoir l'audit-trail

3. Mise en place d'actions correctives et préventives

Suite à l'évaluation des systèmes papier et électroniques, les éventuels risques détectés doivent faire l'objet d'actions correctives et préventives (CAPA). Ces actions ont pour but d'atténuer ou d'annuler le risque mais aussi d'aligner les pratiques au sein des différents services. Ces CAPA sont prises en concertation avec les

différents acteurs en fonction du risque actuel du système sur les données générées et des moyens mis à disposition pour agir sur ce risque.

De manière générale, quatre grands types d'actions peuvent être entreprises :

- Modification de document
- Modification de configuration de système
- Réorganisation des pratiques
- Achat de nouveau matériel

Afin de ne pas remplacer du jour au lendemain l'ensemble du parc technique d'une entreprise, il est conseillé d'évaluer l'impact qu'une modification d'organisation ou de configuration pourrait avoir sur les données. Ainsi, si une telle modification permet de réduire significativement le risque qualité, le remplacement des équipements peut faire l'objet d'une action long terme.

Gap n°	Description du Gap	Gravité du Gap	Action court terme	Gravité du Gap suite à l'action court terme	Action long terme	Gravité du Gap suite à l'action long terme
1	Tout le monde utilise le compte administrateur car l'équipement ne permet pas de créer plus de 10comptes.	Critique	Créer un compte par niveau d'accès, configurer les accès et procédurer la gestion des accès	Mineure	Remplacement de l'équipement par un équipement permettant de créer des comptes individuels	Nulle

Figure 21 : Exemple d'évaluation d'impact

Chaque système doit alors faire l'objet de son propre « plan CAPA » détaillant l'ensemble des actions à mettre en œuvre, la personne responsable de cette mise en œuvre ainsi qu'une date limite de mise en œuvre. Il est alors conseillé de faire mensuellement un état des lieux avec chaque intervenant de l'avancée des actions

entreprises dans leur secteur afin de ne pas avoir d'oubli ni de blocage sur la résolution d'éventuels problèmes.

4. Mapping et optimisation des flux de données

Après analyse des déviations, une forte proportion de celles-ci concerne la perte de données, imputables à leur mauvaise gestion. Afin de palier à ce problème, une analyse des flux critiques doit être réalisée pour définir où, quand et pourquoi une donnée risque de ne plus être ALCOE+.

De même que pour l'analyse des systèmes, une équipe pluridisciplinaire composée de membres de chaque service impacté, de la qualité mais aussi de l'automation doit être formée afin de pouvoir retracer l'ensemble du cycle de vie d'une donnée, de sa création à sa destruction.

L'analyse du flux de chaque donnée générée sur un site s'avérant être une tâche colossale, il est conseillé de réaliser cet exercice sur les données contenues au sein des différents dossiers de lots.

L'exemple ci-dessous permet d'illustrer cette optimisation des flux.

Cas avant optimisation :

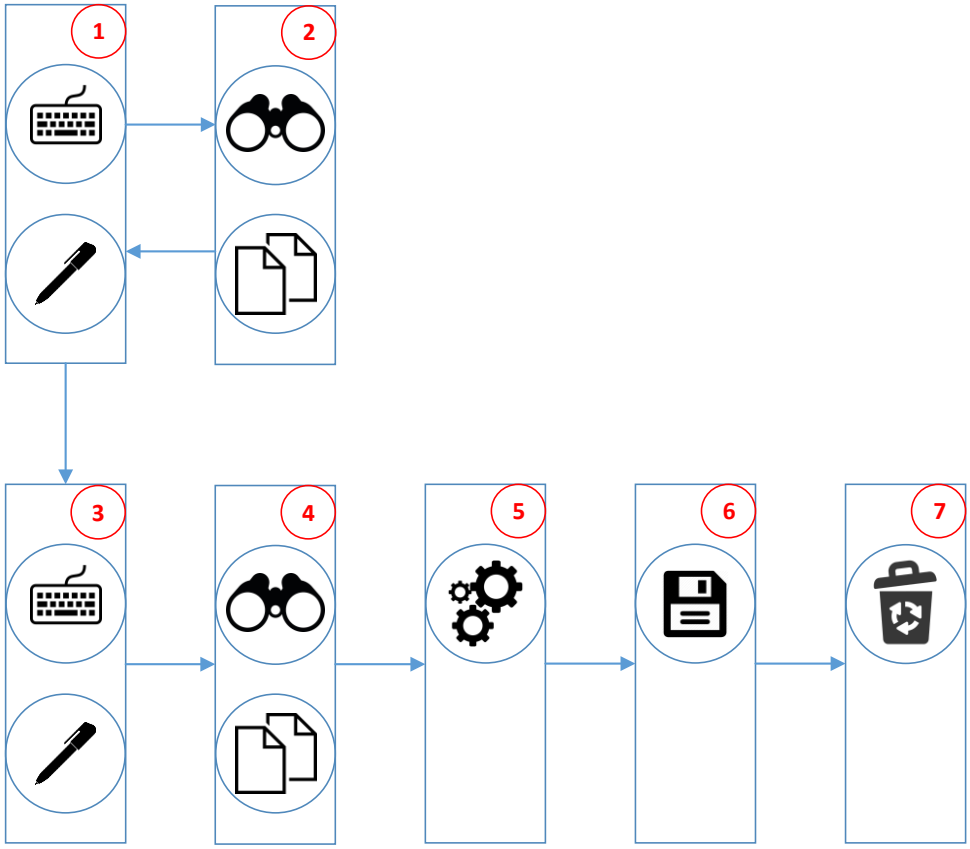


Figure 22 : Exemple de flux avant optimisation

Etape 1 : Le service de production débute son lot et complète le dossier de lot papier en y annexant des impressions de copies d'écrans des appareils. Le dossier est donc constitué de données papiers mais il existe des données brutes électroniques qui ne sont pas conservées.

Etape 2 : Après transfert au département d'assurance qualité production, ce dernier participe à la revue des données de l'étape 1 et réalise une photocopie qu'elle conserve.

Etape 3 : Le dossier de lot repart en production afin qu'il soit transmis au service de packaging. De même qu'à l'étape 1, les données papier sont utilisées mais toutes les données brutes électroniques ne sont pas conservées.

Etape 4 : Après transfert au département d'assurance qualité packaging, l'ensemble du dossier de lot est revu et une seconde copie est réalisée pour conservation au sein du département.

Etape 5 : Le dossier de lot complet est ensuite envoyé au service de libération des lots où une décision est prise.

Etape 6 : Suite à la décision, le dossier est envoyé au service d'archivage où il sera stocké.

Etape 7 : En fin de vie, un prestataire chargé de la destruction du document sera appelé.

Dans ce cas de nombreux problèmes d'intégrité des données peuvent être repérés.

- A chaque étape de production il y a une perte des données dynamiques électroniques due à une utilisation du format papier.
- Les services d'assurance qualité génèrent des copies ce qui accroit l'effort de certification de ces copies. Devenant des documents GxP elles nécessitent ç leur tour un effort de stockage.
- La multiplication des services spécialisés entraine une multiplication des transferts de documents et donc une élévation signification du risque de perte du dossier de lot. L'un des points critiques se trouve entre l'étape 2 et l'étape 3 : pourquoi le document doit-il être envoyé à la production s'il ne fait qu'y transiter vers le service packaging ?
- L'appel à un prestataire pour la destruction nécessite de s'assurer que celui-ci répond aux critères de l'intégrité des données.

Suite à l'étude de ce cas, un projet d'optimisation des flux a été proposé.

Cas après optimisation :

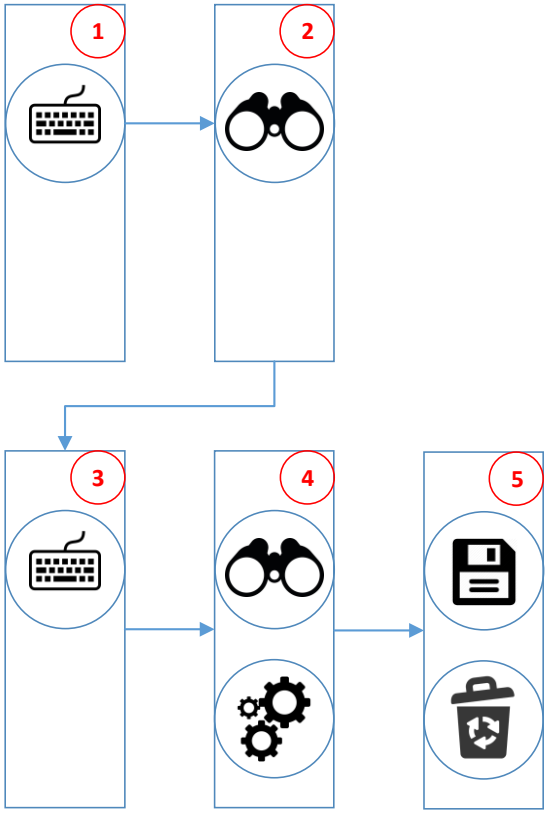


Figure 23 : Exemple de flux après optimisation

Etape 1 : Le service de production débute son lot et complète le dossier de lot électronique. Le dossier de lot étant électronique, il est directement conservé sur le réseau : il n'y a donc pas d'étape de transfert entre les services.

Etape 2 : Le service d'assurance qualité production revoit les données de l'étape 1.

Etape 3 : Après revue, le service packaging est libre de réaliser ses actions.

Etape 4 : L'ensemble des actions étant réalisé, le service de libération de lot est libre de revoir le dossier de lot complet et de prendre une décision.

Etape 5 : Après prise de décision, le service chargé de l'archivage participe au stockage du dossier ainsi qu'à son éventuelle destruction.

Cette optimisation des flux permet de résoudre les nombreux problèmes soulevés par le premier cas, participant ainsi à consolider la culture d'intégrité des données de l'entreprise.

5. Création d’un processus de suivi des bonnes pratiques

Une fois l’ensemble du personnel formé, des systèmes évalués et des actions de correction/prévention entreprises, il est nécessaire de s’assurer que les bonnes pratiques soient respectées au quotidien dans l’ensemble des services. A ce titre, différents moyens peuvent être mis en œuvre :

- **L’oversight:** Un membre de l’équipe qualité du secteur concerné suit quotidiennement (ou de façon la plus fréquente possible) ses équipes afin d’observer les pratiques. En cas de dérive, il intervient directement pour expliquer l’erreur et les bonnes pratiques associées. Ce processus n’a pas pour vocation de sanctionner un service ou une équipe mais plutôt de pérenniser les bonnes pratiques tout en dialoguant avec les équipes afin de pouvoir soulever d’éventuelles complications.

- **L’Auto-inspection :** Chaque service doit être en mesure d’autoévaluer ses activités. Il est ainsi conseillé à chaque service d’analyser de façon annuelle la qualité de ses données sur un processus choisi en prenant en compte l’ensemble des facteurs (personnel et matériel). Le but de l’auto-inspection est de proposer des axes d’amélioration pour les services et chaque écart détecté doit faire l’objet d’un plan d’actions.

- **Les audits internes** : Outil indispensable du système de management de la qualité, l’audit interne permet à des spécialistes de vérifier qu’un secteur répond aux attentes des autorités. Le responsable Data Integrity devra s’assurer que les auditeurs intègrent l’analyse des données au sein de chaque audit.

CONCLUSION :

Cœur des préoccupations du monde pharmaceutique mais aussi cœur du système qualité d'une entreprise, le développement d'un programme d'intégrité des données au sein d'un laboratoire pharmaceutique doit prendre en compte les contraintes humaines et matérielles. Qu'il s'agisse d'un simple ticket de pesée ou d'un dossier de lot, chaque donnée générée sur un site pharmaceutique doit faire l'objet d'une évaluation détaillée menée par différents acteurs de la qualité mais aussi de la production.

Si une modification des systèmes informatisés permet une rapide progression de la fiabilisation des données, atteindre cet objectif n'est que pleinement possible grâce l'adoption de la culture de la qualité par chacun. Ainsi, la direction pharmaceutique se doit de montrer l'exemple et de favoriser un climat de transparence où chacun se sente libre de remonter tout évènement indésirable.

Mener à bien ce programme peut s'avérer délicat car une évolution des mentalités n'est pas perceptible du jour au lendemain et nécessite un travail de tous les jours, cependant les données sont aujourd'hui le reflet direct du produit. Sans données de qualité, il est inenvisageable d'espérer un produit de qualité.

Bibliographie :

1. Gantz et Reinsel - THE DIGITAL UNIVERSE IN 2020 Big Data, Bigger Dig.pdf [Internet]. [cité 27 avr 2018]. Disponible sur: https://www.emc.com/collateral/analyst-reports/idc-the-digital-universe-in-2020.pdf

2. 2008 - WHO Expert Committee on specifications for pharmac.pdf [Internet]. [cité 20 avr 2018]. Disponible sur: http://www.who.int/medicines/areas/quality_safety/quality_assurance/Guidance-on-good-data-management-practices_QAS15-624_16092015.pdf

3. Purdie - Data Integrity and Compliance With CGMP Guidance f.pdf [Internet]. [cité 20 avr 2018]. Disponible sur: https://www.fda.gov/downloads/drugs/guidances/ucm495891.pdf

4. European Medicines Agency - Good manufacturing practice - Questions and answers: Good manufacturing practice [Internet]. [cité 20 avr 2018]. Disponible sur: http://www.ema.europa.eu/ema/index.jsp?curl=pages/regulation/q_and_a/q_and_a_detail_000027.jsp&mid=WC0b01ac05800296ca#section18

5. PI_041_1_DRAFT_2_GUIDANCE_ON_DATA_INTEGRITY.pdf [Internet]. [cité 20 avr 2018]. Disponible sur: http://academy.gmp-compliance.org/guidemgr/files/PI_041_1_DRAFT_2_GUIDANCE_ON_DATA_INTEGRITY.PDF

6. MHRA_GxP_data_integrity_guide_March_edited_Final.pdf [Internet]. [cité 25 avr 2018]. Disponible sur: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/687246/MHRA_GxP_data_integrity_guide_March_edited_Final.pdf

7. EUR-Lex - 31991L0356 - FR [Internet]. Journal officiel n° L 193 du 17/07/1991 p. 0030 - 0033; édition spéciale finnoise: chapitre 13 tome 20 p. 0206 ; édition spéciale suédoise: chapitre 13 tome 20 p. 0206 ; [cité 20 avr 2018]. Disponible sur: https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:31991L0356&from=FR

8. EUR-Lex - 32003L0094 - FR [Internet]. Journal officiel n° L 262 du 14/10/2003 p. 0022 - 0026; [cité 20 avr 2018]. Disponible sur: https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32003L0094&from=FR

9. Guidance for Industry - Part 11, Electronic Record.pdf [Internet]. [cité 20 avr 2018]. Disponible sur: https://www.fda.gov/downloads/RegulatoryInformation/Guidances/ucm125125.pdf

10. Withdrawn_MHRA_GxP_Data_Integrity_Definitions_and_Guidance_for_Industry.pdf [Internet]. [cité 20 avr 2018]. Disponible sur: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/697047/Withdrawn_MHRA_GxP_Data_Integrity_Definitions_and_Guidance_for_Industry.pdf

11. ISPE GAMP® Guide: Records and Data Integrity. :152.

12. 18016_TOC.pdf [Internet]. [cité 24 avr 2018]. Disponible sur: https://store.pda.org/TableOfContents/18016_TOC.pdf

Liste des abréviations et acronymes :

WHO: World Health Organization (Organisation mondiale de la santé = OMS)

MHRA: Medicines and Healthcare Products Regulatory Agency (Agence de santé britannique)

FDA : Food and Drug Administration (Agence de santé américaine)

EMA : European Medicines Agency (Agence de santé européenne)

PIC/S : Pharmaceutical Inspection Co-operation Scheme (Regroupement des auditeurs)

GMP : Good Manufacturing Practices (= Bonnes Pratiques de Fabrication)

GxP : Good X Practices (Ensemble des bonnes pratiques)

CQA : Critical Quality Attributes (Caractéristique physique, chimique ou microbiologique d'un produit permettant de s'assurer de son niveau de qualité)

ALCOA : Attributable, Legible, Contemporaneous, Original, Accurate

ALCOE : Attribuable, Lisible, Concomitante, Originale, Exacte

Liste des figures :

Définitions :

Audit-trail : Moyen de suivre et de contrôler chaque activité réalisée sur un système informatisé (rapport contenant l'enregistrement de chaque action).

Backup : Réalisation d'une copie des données numériques afin de conserver celles-ci en cas de désastre (par exemple : crash du système).

Copie certifiée : Copie certifiée identique à l'original en contenu et en sens par une seconde personne. Elle peut remplacer l'original.

Document maître : Premier exemplaire d'un document destiné à être distribué en plusieurs exemplaire.

Donnée : Représentation d'une information, elle est le résultat d'une observation ou d'une expérience.

Donnée brute : Donnée conservée dans son état d'origine. Elle n'est pas directement exploitable mais permet d'être lue après traitement.

Donnée traitée : Donnée ayant subie une étape de traitement dans le but de la rendre lisible et compréhensible par tous.

Format dynamique : Est à opposer avec le format statique. Dans ce format la donnée peut subir une étape de traitement pour obtenir un résultat.

Format statique : Format dans lequel une donnée ne peut à nouveau subir une étape de traitement. Il s'agit le plus souvent du format PDF.

Gemba : Fait d'aller directement sur le terrain pour observer les pratiques.

Identification biométrique : L'authentification biométrique fait appel aux caractéristiques biologiques uniques d'un individu (empreinte digitale, reconnaissance du visage ou de l'iris) pour vérifier son identité.

Intégrité des données : Ensemble des moyens permettant de garantir qu'une donnée est fiable tout au long de son cycle de vie.

Métadonnées : Ensembles des données conférant un sens et un contexte à la donnée centrale. Elles sont essentielles à sa compréhension. Dans l'exemple suivant les métadonnées sont en italique et la donnée centrale en gras :

Chlorure de sodium Lot 1234, **3.5** *mg. J.Smith 01-Juin-2014*

Période de rétention : Période pendant laquelle une donnée doit être conservée et peut être demandée par une agence de santé ou un client.

Réconciliation documentaire : Processus de comparaison du nombre de documents distribués et du nombre de documents retournés.

Répétition de tests: Fait de réaliser de nombreux tests successifs dans le but d'avoir un résultat conforme. Cette pratique n'est pas tolérée.

Stand-Alone : Equipement non connecté au réseau de l'entreprise, limitant ainsi le transfert et la sauvegarde des données.

Université de Lille

FACULTE DE PHARMACIE DE LILLE

DIPLOME D'ETAT DE DOCTEUR EN PHARMACIE

Année Universitaire 2016/2017

Nom : DELPLANQUE

Prénom : THIBAUT

Titre de la thèse :

Développement d'une politique d'intégrité des données sur un site de production pharmaceutique

Mots-clés : Data Integrity, Qualité, Cycle de vie des données, ALCOE+, Bonnes Pratiques Documentaires, Système papier, Système Informatisé

Résumé :

Le volume des données manuscrites et électroniques générées dans le monde connait une croissance exponentielle, passant de 0.13 zetaoctets (10^{21}) par an en 2005 à une prévision de 160 zetaoctets en 2025 La multiplication de ces données entraine alors un besoin de s'assurer de leur fiabilité et de leur pérennité. C'est dans ce contexte que des principes réglementaires émis dans les années 1990 refont aujourd'hui surface pour devenir l'un des requis essentiels des différentes autorités de santé : l'intégrité des données générées.

<u>Membres du jury</u> :

Président :

Pr. Anne Gayot : Professeur à la Faculté de Pharmacie de Lille

Membre(s) extérieur(s) :

Mme. Hélène Zentar: Manager Affaires Réglementaires GSK SAE

M. Yannic Lepage : QA & RA Manager Minakem Mont-Saint-Guibert