Guide de bonnes pratiques de gestion des données et des enregistrements

Contexte

Lors d'une consultation informelle au sujet de l'inspection des bonnes pratiques de fabrication et du guide de gestion du risque dans la fabrication de médicaments organisée par l'Organisation Mondiale de la Santé (OMS) à Genève en avril 2014, une proposition d'un nouveau guide de bonne gestion des données a été discutée et son élaboration a été recommandée. Les participants incluaient des inspecteurs et des spécialistes nationaux des différents sujets qui étaient à l'ordre du jour, mais aussi du personnel du service des inspections de l'équipe de pré-qualification (PQT).

Le Comité OMS d'experts des spécifications aux préparations pharmaceutiques a obtenu des retours de cette consultation informelle pendant sa quarante-neuvième rencontre en octobre 2014. Un document de réflexion du service des inspections de PQT décrivant la structure proposée pour un nouveau document de référence a été discuté de manière détaillée. Le document de réflexion a consolidé des principes normatifs existants et a donné des exemples d'illustration de leurs mises en œuvre. Dans l'appendice du document de réflexion, des extraits des bonnes pratiques et de documents de référence existants ont été combinés pour illustrer les lignes directrices pertinentes courantes en ce qui concerne l'assurance de la fiabilité des données et des sujets BPx (bonnes pratiques [de quelque chose]). Au vu du nombre croissant d'observations faites pendant les inspections qui se rapportent aux pratiques de gestion des données, le Comité a approuvé la proposition.

À la suite de cette approbation, une ébauche de document a été préparée par des membres du service des inspections de PQT et un groupe de travail incluant des inspecteurs nationaux. Cette ébauche a été discutée lors d'une consultation sur la gestion des données, sur la bioéquivalence, sur les bonnes pratiques de fabrication et sur les inspections de médicaments qui a eu lieu du 29 juin au 1er juillet 2015.

Une révision du document de travail a été ensuite préparée par les auteurs en collaboration avec le groupe de travail, sur la base des retours obtenus pendant cette consultation ainsi que durant l'atelier de travail sur la gestion des données organisé par l'OMS après la consultation.

Une collaboration avec d'autres organisations est recherchée pour une convergence future dans ce domaine.

1. Introduction

1.1 Les systèmes de réglementation des médicaments dans le monde entier ont toujours été dépendants de la connaissance des organisations qui développent, fabriquent et conditionnent, testent, distribuent et surveillent les produits pharmaceutiques. La confiance entre le régulateur et le réglementé est implicite dans le processus d'évaluation et de revue quant au fait que l'information soumise dans les dossiers et utilisée dans la prise de décision quotidienne est compréhensible, complète et fiable. Les données sur lesquelles les décisions reposent devraient ainsi être complètes ainsi qu'attribuables, lisibles, enregistrées sur le moment, originales, exactes, communément désigné par l'acronyme « ALCOA ».

1.2 Ces principes ALCOA de base et les exigences de bonnes pratiques associées qui assurent la fiabilité des données ne sont pas récents et beaucoup de guides normatifs de haut et moyen niveau existent déjà. Cependant, ces dernières années, le nombre d'observations faites en ce qui concernent les bonnes pratiques de gestion des données et des enregistrements (BPGDE) pendant les inspections de bonnes pratiques de fabrication (BPF) (1), les bonnes pratiques cliniques (BPC) et les bonnes pratiques de laboratoire (BPL) a augmenté. Les raisons de la préoccupation grandissante des autorités sanitaires en ce qui concerne la fiabilité des données sont sans aucun doute multifactorielles et incluent une sensibilisation réglementaire accrue et des inquiétudes en ce qui concerne les écarts entre les choix de l'industrie et les stratégies de contrôle appropriées et modernes.

1.3 Les facteurs contributifs incluent des échecs de mise en œuvre des systèmes robustes qui inhibent les risques associés aux données par les organisations, afin d'améliorer la détection des situations où la fiabilité des données peut être compromise, et/ou pour enquêter et s'attaquer aux causes fondamentales lorsque des échecs surviennent. Par exemple, les organisations sujettes aux exigences des bonnes pratiques de produit pharmaceutique utilisent des systèmes informatisés validés depuis des décennies mais beaucoup échouent à réviser et à gérer les enregistrements électroniques originaux de manière adéquate et révisent et gèrent à la place souvent des documents imprimés incomplets et/ou non-appropriés. Ces observations soulignent le besoin pour l'industrie de moderniser les stratégies de contrôle et d'appliquer la gestion du risque qualité (QRM) et des principes scientifiques solides aux modèles économiques actuels (tels que l'externalisation et la mondialisation) aussi bien qu'aux technologies utilisées actuellement (tels que les systèmes informatisés).

1.4 Exemples de contrôles qui peuvent nécessiter un développement et un renforcement pour assurer des bonnes stratégies de gestion des données incluent notamment :

- une approche QRM qui assure efficacement la sécurité du patient, la qualité du produit et la validité des données en assurant que la direction ajuste les exigences avec les capacités réelles des procédés. La direction doit assumer la responsabilité pour une bonne gestion des données en fixant en premier lieu des attentes réalistes et atteignables pour les capacités réelles et véritables d'un processus, d'une méthode, d'un environnement, du personnel ou des technologies, entre autres ;

- de la surveillance des processus et de l'allocation des ressources nécessaires par la direction pour assurer et améliorer l'infrastructure, comme requis (par exemple, pour améliorer continuellement les processus et les méthodes, pour assurer une conception et une maintenance adéquates des bâtiments, des installations, des équipements et des systèmes ; pour assurer une puissance et un approvisionnement en eau fiables et adéquats ; pour fournir la formation nécessaire du personnel ; et pour attribuer les ressources nécessaires à la surveillance des sites et des fournisseurs contractants pour assurer que les standards de qualité adéquats soient satisfaits). Un engagement actif de la direction dans ce sens remédie et réduit les pressions et les sources possibles d'erreurs qui peuvent augmenter les risques d'intégrité des données ;

- l'adoption d'une culture de la qualité au sein de l'entreprise qui encourage le personnel à être transparent en ce qui concerne les défaillances de manière à ce que la direction ait une compréhension précise des risques et qu'elle puisse alors fournir les ressources nécessaires pour répondre aux attentes et répondre aux standards de qualité des données : un mécanisme de signalement indépendant de la hiérarchie doit être prévu ;

- la modélisation des processus de données et l'application de QRM moderne et des principes scientifiques solides au cours du cycle de vie des données ;

- l'assurance que tous les personnels du site soient tenus informés de l'application des bonnes pratiques de documentation (BPDoc) pour assurer que les principes BPx d'ALCOA soient compris et appliqués aux données électroniques de la même manière qu'ils l'ont été historiquement appliqués aux enregistrements papier ;

- l'implémentation et la confirmation pendant la validation des systèmes informatisés et le contrôle des modifications ultérieures, que tous les contrôles nécessaires pour les BPDoc pour les données électroniques soient en place et que la probabilité de l'occurrence d'erreurs dans les données soit minimisée ;

- la formation du personnel qui utilise les systèmes informatisés et qui révise les données électroniques pour une compréhension de base du fonctionnement des systèmes informatisés et de la manière de réviser efficacement les données électroniques, qui incluent les métadonnées et les audit-trails ;

- la définition et la gestion des responsabilités et des rôles appropriés pour les accords de qualité et les contrats entre les donneurs et les accepteurs d'ordre, incluant le besoin d'une surveillance basée sur le risque des données générées et réglementées par l'accepteur d'ordre pour le compte du donneur d'ordre ;

- la modernisation des techniques d'inspection d'assurance qualité et la collecte d'indicateurs qualité pour identifier efficacement et réellement les risques et les opportunités d'amélioration des processus de données.

2. Objectifs et missions de ce guide

2.1 Ce guide conforte les principes normatifs existants et propose des exemples détaillés de mise en œuvre pour combler les écarts figurant actuellement dans les textes. De plus, il donne des explications pratiques quant à la signification de ces exigences de haut niveau et quant à la démonstration de la mise en œuvre pour atteindre la conformité.

2.2 Ce guide souligne, et clarifie dans certaines situations, la mise en application des procédures de gestion des données. L'accent est mis sur ces principes qui sont implicites dans les textes existants de l'OMS et qui, s'ils n'étaient pas correctement mis en œuvre, impacteraient la fiabilité et l'intégralité des données et affaibliraient la robustesse de la prise de décision basée sur ces données. Des exemples d'illustration sont fournis sur la manière dont ces principes sont appliqués aux technologies et aux modèles économiques actuels. Ce guide ne définit pas tous les contrôles prévus pour assurer la fiabilité des données et il doit être considéré en relation avec les autres textes existants de l'OMS et avec d'autres références internationales connexes.

2.3 Ce guide est d'une nature évolutive, indicative et il est ainsi sujet à des revues périodiques basées sur l'expérience de sa mise en œuvre et de son utilité, aussi bien que le retour fourni par les parties prenantes, incluant les autorités réglementaires nationales (NRAs).

3. Glossaire

Les définitions données ci-dessous s'appliquent aux termes utilisés dans ce guide. Elles peuvent avoir des significations différentes dans d'autres contextes.

ALCOA. Un acronyme utilisé communément pour « attribuable, lisible, concomitant, original, exact » ; *en Anglais « Attributable, Legible, Contemporaneous, Original and Accurate ».*

ALCOA-plus. Un acronyme utilisé communément pour « attribuable, lisible, concomitant, original, exact » qui de plus met l'accent sur les propriétés suivantes : complet, consistant, durable et disponible – principes ALCOA de base implicites ; en Anglais « complete, consistent, enduring and available ».

Archivage. L'archivage est le processus visant à protéger des enregistrements de la possibilité d'être modifié ultérieurement ou d'être détruit, et de stocker ces enregistrements sous le contrôle d'un personnel indépendant de gestion des données tout au long de la période de conservation requise. Les enregistrements archivés doivent inclure, par exemple, les métadonnées et les signatures électroniques associées.

Archiviste. Selon les bonnes pratiques de laboratoire (BPL), personne indépendante désignée et autorisée par la direction pour être responsable de la gestion des archives, c'est-à-dire : pour les opérations et les procédures d'archivage. Les BPL requièrent un archiviste désigné (par

exemple : un individu), tandis que pour les autres BPx, les rôles et les responsabilités de l'archiviste sont normalement remplis par plusieurs personnes ou groupes de personnes désignés (par exemple : à la fois le personnel de l'assurance qualité en charge du contrôle des enregistrements et les administrateurs système informatique) sans qu'il n'y ait une personne unique assignée à la responsabilité du contrôle comme cela est requis dans BPL. Il est reconnu que dans certaines circonstances, il peut être nécessaire pour l'archiviste de déléguer des tâches d'archivage spécifiques, par exemple, la gestion des données électroniques à un personnel informatique spécifique. Les tâches, les devoirs et les responsabilités doivent être précisés et détaillés dans des procédures opérationnelles (SOP). Les responsabilités de l'archiviste et du personnel auquel les tâches d'archivage sont déléguées incluent – aussi bien pour les enregistrements papier qu'électroniques – l'assurance que l'accès à l'archive est contrôlé, que le stockage et la récupération ordonnée des enregistrements et des matériels sont facilités par un système d'indexation et que la circulation des enregistrements et des matériels dans et en-dehors des archives est adéquatement contrôlé et documenté. Ces procédures et enregistrements doivent être revues périodiquement par un auditeur indépendant.

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

Sauvegarde. Une sauvegarde (*également nommée backup*) correspond à la copie d'un ou plusieurs fichiers électroniques créés en tant que secours dans le cas où le fichier ou le système d'origine seraient perdus ou deviendraient inutilisables (par exemple, dans le cas d'une défaillance du système ou de la corruption d'un disque). Il est important de rappeler que la sauvegarde diffère de l'archivage dans le fait que les copies de sauvegarde d'enregistrements électroniques sont typiquement stockées temporairement à des fins de reprise d'activité et qu'elles peuvent être réécrites périodiquement. Il convient de ne pas se fier

à de telles copies temporaires en tant que mécanisme d'archivage.

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

Stratégie de contrôle. Un ensemble planifié de contrôles établi sur la base du protocole considéré, de l'article ou du produit de test et de la compréhension du processus, qui assure, selon le cas, la conformité avec ce protocole, la performance du processus, la qualité du produit et la fiabilité des données. Les contrôles doivent inclure des paramètres appropriés et des attributs de qualité relatifs aux sujets de l'étude, aux systèmes de test, aux matériaux et aux composants du produit, aux technologies et aux équipements, aux installations, aux conditions de fonctionnement, aux spécifications et aux méthodes associées ainsi qu'à la fréquence de surveillance et de contrôle.

Action préventive et action corrective (**CAPA** – corrective action/preventive action) se réfèrent aux actions conduites pour améliorer les processus d'une organisation et pour éliminer les causes de non-conformités et d'autres situations indésirables. CAPA est un concept commun aux BPx (bonnes pratiques de laboratoire, bonnes pratiques cliniques et bonnes pratiques de fabrication), et à de nombreuses normes ISO industrielles (organisation internationale de normalisation). Le processus se concentre sur la recherche systématique des causes premières des problèmes identifiés ou des risques identifiés afin de prévenir leur répétition (pour l'action corrective) ou leur apparition (pour l'action préventive).

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

Gouvernance des données. La totalité des dispositions prises pour assurer que les données, indépendamment du format dans lequel elles sont générées, enregistrées, traitées, conservées et utilisées pour assurer un enregistrement complet, cohérent et exact tout au long du cycle de vie des données.

Intégrité des données. L'intégrité des données est le degré pour lequel les données sont complètes, cohérentes, exactes, dignes de confiance et fiables et que ces caractéristiques des données sont préservées tout au long du cycle de vie des données. Les données doivent être

collectées et conservées d'une façon sécurisée, de telle manière qu'elles soient attribuables, lisibles, concomitante (c-à-d : enregistrées sur le moment), originales ou une copie conforme, et exacte. Assurer l'intégrité des données requiert des systèmes appropriés de gestion de la qualité et du risque, y compris l'observation de principes scientifiques solides et aux bonnes pratiques de documentation.

Cycle de vie des données. Toutes les phases du processus par lequel les données sont créées, enregistrées, traitées, revues, analysées et rapportées, transférées, stockées, récupérées et surveillées jusqu'à leur retrait et leur destruction. Une approche planifiée doit exister pour évaluer, surveiller, gérer les données et les risques de ces données d'une manière proportionnelle à l'impact potentiel pour la sécurité du patient, la qualité du produit et/ou la fiabilité des décisions prises tout au long des phases du cycle de vie des données.

Format d'enregistrement dynamique. Les enregistrements en format dynamique, tels que les enregistrements électroniques, permettent interaction entre l'utilisateur et le contenu de l'enregistrement. Par exemple, les enregistrements électroniques dans des formats de base de données permettant à l'utilisateur de suivre, d'évaluer des tendances et de faire des requêtes. Ainsi les enregistrements de chromatographie conservés en tant qu'enregistrements électroniques permettent à l'utilisateur (disposant des droits d'accès appropriés) de retraiter les données et d'élargir la ligne de base afin de voir plus clairement l'intégration.

Approche entièrement électronique. Ce terme se réfère à l'utilisation d'un système informatisé dans lequel les enregistrements électroniques originaux sont signés électroniquement.

Bonnes pratiques de gestion des données et des enregistrements (BPGDE). La totalité des mesures organisées qui doivent être en place pour assurer collectivement et individuellement que les données et les enregistrements sont sécurisés, attribuables, lisibles, traçables, permanents, concomitants, originaux et exacts et qui, lorsqu'elles ne sont pas implémentées de manière robuste, peuvent impacter la fiabilité et la complétude des données et affaiblir la robustesse de la prise de décision basée sur ces données.

Bonnes pratiques de documentation. Dans le contexte de ce guide, les bonnes pratiques de documentation sont les mesures qui assurent collectivement et individuellement que la documentation, qu'elle soit au format papier ou électronique, est sécurisée, attribuable, lisible, traçable, permanente, concomitante, originale et exacte.

BPx. Acronyme pour l'ensemble des guides de bonnes pratiques réglementant les activités précliniques, cliniques, de fabrication, de contrôle, de stockage, de distribution et de post-commercialisation pour les produits pharmaceutiques et biologiques et les dispositifs médicaux réglementés, telles que les bonnes pratiques de laboratoire, les bonnes pratiques cliniques, les bonnes pratiques de fabrication, les bonnes pratiques de pharmacovigilance et les bonnes pratiques de distribution.

Approche hybride. Cette approche fait référence à l'utilisation d'un système informatisé dans

lequel il y a une combinaison d'enregistrements électroniques originaux et d'enregistrements papier qui constituent la totalité des enregistrements qui doit être revue et conservée. L'exemple d'une approche hybride est lorsque les analystes de laboratoire utilisent des équipements automatisés qui créent des enregistrements électroniques originaux et qu'ils impriment ensuite un résumé de résultats. L'approche hybride requiert un lien sûr entre tous les types d'enregistrements, incluant les formats papier et électroniques, tout au long de la période de conservation des enregistrements. Là où des approches hybrides sont utilisées, des contrôles appropriés doivent exister pour les enregistrements électroniques, tels que les modèles, les formulaires et les documents maîtres, qui pourraient être imprimés.

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

Indicateurs qualité. Les indicateurs qualité sont des mesures objectives utilisées par le management et les autres parties intéressées pour surveiller l'état général de la qualité, selon le cas, d'une organisation, d'une activité, d'un processus ou d'une conduite d'étude BPx. Elles incluent les mesures pour évaluer le fonctionnement effectif des contrôles du système qualité et de la performance, la qualité et la sécurité des produits pharmaceutiques et la fiabilité des données.

Gestion du risque qualité. Un processus systématique pour l'évaluation, le contrôle, la communication et la revue des risques liés à la qualité du produit pharmaceutique tout au long du cycle de vie du produit.

Direction. Personne(s) qui dirige et contrôle une entreprise ou un site au plus haut niveau avec l'autorité et la responsabilité de mobiliser les ressources au sein de l'entreprise ou du site.

Format d'enregistrement statique. Un format d'enregistrement statique, tel qu'un enregistrement papier ou pdf, est un format qui est fixé et qui ne permet peu ou pas d'interaction entre l'utilisateur et le contenu de l'enregistrement. Par exemple, une fois imprimé ou converti en fichiers « .pdf » statiques, les enregistrements de chromatographie perdent leur capacité à être retraités ou à permettre une vue plus détaillée des lignes de base.

Copie conforme. Une copie conforme (également appelée « vraie copie ») est une copie d'un enregistrement original de données qui a été vérifiée et certifiée pour attester qu'il s'agit d'une

copie exacte et complète préservant l'intégralité du contenu et de la signification de l'enregistrement original, avec, dans le cas de données électroniques, toutes les métadonnées essentielles et le format d'enregistrement original.

4. Principes

4.1 Les BPGDE sont des éléments critiques du système de qualité pharmaceutique, et une approche systématique doit être mise en œuvre pour fournir un niveau élevé d'assurance que, tout au long du cycle de vie du produit, tous les enregistrements et toutes les données BPx sont complets et fiables.

4.2 Le programme d'administration des données doit inclure les politiques et les procédures d'administration qui abordent les principes généraux listés ci-dessous pour un programme de bonne gestion des données. Ces principes sont clarifiés avec des détails supplémentaires dans les sections suivantes.

4.3 **Applicabilité aux données aussi bien papier qu'électroniques**. Les exigences pour BPGDE qui assurent un contrôle solide de la validité des données s'appliquent de manière identique aux données papier et électroniques. Les organisations assujetties aux BPx doivent être pleinement conscientes que revenir à des systèmes manuels ou basés sur le papier en partant de systèmes automatisés ou informatisés n'élimine pas le besoin intrinsèque de contrôles de gestion robustes.

4.4 **Applicabilité aux donneurs d'ordre et aux accepteurs d'ordre**. Les principes de ces directives s'appliquent aux donneurs d'ordre et aux accepteurs d'ordre. Les donneurs d'ordre ont la responsabilité finale de la solidité de toutes les décisions prises sur la base des données BPx, incluant celles prises sur la base des données fournies par les accepteurs d'ordre. Les donneurs d'ordre doivent ainsi effectuer une vérification préalable basée sur le risque pour s'assurer que les accepteurs d'ordre disposent des programmes appropriés en place pour assurer la véracité, l'intégralité et la fiabilité des données fournies.

4.5 **Bonnes pratiques de documentation**. Afin que les décisions prises soient solides, il convient que l'ensemble de données de support soit fiable et complet. Les BPDoc doivent être respectées de manière à s'assurer que tous les enregistrements, papiers et électroniques, permettent la reconstruction intégrale et la traçabilité des activités BPx.

4.6 **Administration de la gouvernance**. Pour établir un bon système de gestion des données solide et durable, il est important que la direction s'assure que des programmes appropriés de gouvernance de la gestion des données soient en place (pour plus de détails, voir chapitre 6).

Les éléments d'une gouvernance efficace doivent inclure :

- l'application des principes modernes de QRM et des principes de bonnes gestion des données qui assurent la validité, l'intégralité et la fiabilité de ces données ;

- l'utilisation d'indicateurs qualité appropriés ;

- l'assurance que le personnel n'est pas soumis à des pressions commerciales, politiques, financières, ou à d'autres pressions ou incitations de la part de l'organisation pouvant nuire à la qualité et à l'intégrité de leur travail ;

- l'allocation des ressources humaines et techniques adéquates de manière à ce que la charge de travail, les heures de travail et les pressions qui s'exercent sur les personnes responsables de la production des données et de la conservation des enregistrements n'augmentent pas les erreurs ;

- la conscience du personnel dans l'importance de son rôle pour garantir l'intégrité des données en relation avec l'assurance de qualité du produit et la protection de la sécurité du patient.

4.7 **Culture de la qualité**. La direction, avec le support de l'unité qualité, doit établir et maintenir un environnement de travail qui minimise le risque d'enregistrements non-conformes et d'enregistrements et de données erronés. Un élément essentiel de la culture de la qualité est que les déviations, les erreurs, les omissions et les résultats aberrants, à tout niveau que ce soit de l'organisation, soient signalés ouvertement et de manière transparente. Des mesures doivent être prises pour prévenir, détecter et corriger des points faibles dans les systèmes et les procédures pouvant conduire à des erreurs de données, afin d'améliorer continuellement la fiabilité du processus de prise de décision scientifique au sein de l'organisation. La direction doit décourager activement toute pratique de gestion dont on peut s'attendre raisonnablement à ce qu'elle nuise au signalement actif et complet de tels problèmes, par exemple, liés aux contraintes hiérarchiques ou à la culture du reproche.

4.8 **Gestion du risque qualité et principes scientifiques solides**. Un processus solide de prise de décision nécessite une qualité adaptée et des systèmes de gestion du risque, ainsi que l'adhésion à des principes scientifiques et statistiques solides, qui doivent être basés sur des données fiables. Ainsi le principe scientifique de l'observation objective et non biaisée des résultats d'analyse d'un échantillon repose sur la capacité à investiguer et à exclure des résultats suspects seulement lorsque leurs causes sont clairement identifiées et attribuables. L'observation des principes de bonne conservation des données et des enregistrements nécessite que tous les résultats rejetés soient enregistrés, conjointement avec une justification documentée de leur rejet et que cette documentation fasse l'objet d'une revue soit conservée.

4.9 **Gestion du cycle de vie des données**. L'amélioration continue des produits pharmaceutiques en vue d'assurer leur sécurité, leur efficacité et leur qualité nécessite une gouvernance permettant la gestion des risques d'intégrité des données tout au long des phases au cours desquelles les données sont créées, enregistrées, traitées, transmises, rapportées, archivées et récupérées. Cette approche de gestion fait l'objet d'une revue régulière. Afin que l'organisation, l'analyse et l'assimilation des données en information facilitent une prise de décision fiable et basée sur des preuves, il convient que la gouvernance des données aborde

les questions de détention des données, de responsabilité pour les processus de traitement des données et de gestion des risques tout au long du cycle de vie des données.

*4.10 Afin que l'organisation, l'analyse et l'assimilation des données dans un format ou une structure facilitent une prise de décision fiable et basée sur des preuves, il convient que la gouvernance des données aborde les questions de détention des données, de responsabilité pour les processus de traitement des données et de gestion des risques tout au long du cycle de vie des données**. [ATTENTION, CECI EST UN DOUBLON]***

4.11 **Conception des méthodes et des systèmes de stockage des enregistrements**. Les méthodes et les systèmes de stockage des enregistrements, que ceux-ci soient sous format papier ou électronique, doivent être conçus de manière à encourager la conformité avec les principes d'intégrité des données.

4.12 Les exemples suivants comprennent, mais ne sont pas restreints à :

- limiter la capacité de modifier l'heure utilisée pour enregistrer des évènements horodatés, par exemple, l'heure des horloges systèmes dans des systèmes électroniques et d'instrumentation des procédés ;

- s'assurer que les formulaires approuvés utilisés pour enregistrer les données BPx (exemple des dossiers de lots papiers, des formulaires papier de rapport d'un évènement et des feuilles de travail de laboratoire) sont accessibles sur les lieux où l'activité se déroule, au moment où elle se déroule, de manière à ce que les données soient enregistrées à ce moment et qu'une transcription ultérieure n'est pas nécessaire ;

- maîtriser l'utilisation de modèles papier vierges pour l'enregistrement de données des activités BPx de manière à ce que tous les formulaires imprimés puissent être réconciliés et comptabilisés ;

- restreindre les droits d'accès d'utilisateur aux systèmes automatisés pour prévenir les modifications de données (ou pour les tracer via l'audit-trail) ;

- s'assurer que les systèmes d'enregistrement (comme les balances) ou d'impression automatique de données soient fixées et raccordées à l'équipement pour assurer l'enregistrement indépendant et opportun des données ;

- s'assurer de la proximité des imprimantes avec le lieu de réalisation des activités correspondantes ;

- s'assurer d'un accès aisé aux points de prise d'échantillons (par exemple les points de prélèvement des systèmes d'eau) pour permettre une exécution efficace et

simple de la prise d'échantillons par les opérateurs et ainsi de réduire la tentation de prendre un raccourci ou de falsifier des échantillons ;

- s'assurer de l'accès aux données électroniques originales pour le personnel en charge de la vérification des données.

4.13 Les données et leurs supports d'enregistrements doivent être durables. L'encre des enregistrements papier doit être indélébile. Les encres thermosensibles, photosensibles et d'autres encres qui s'effacent ne doivent pas être utilisées. Le papier ne doit pas être thermosensible, photosensible ou s'oxyder. Si cela n'est pas entièrement possible (comme par exemple le cas dans des sorties d'imprimantes existantes de balances et d'autres instruments de laboratoire), alors des copies authentiques ou certifiées doivent être disponibles jusqu'à ce que cet équipement soit retiré ou remplacé.

4.14 **Maintenance des systèmes de stockage des enregistrements**. Les systèmes installés et maintenus pour la conservation des enregistrements papiers et électroniques doit prendre en compte le progrès scientifique et technique. Les systèmes, procédures et méthodes utilisées pour enregistrer et stocker les données doivent être revus périodiquement quant à leur efficacité et être mis à jour si nécessaire.

5. Gestion du risque qualité pour s'assurer une bonne gestion des données

5.1 Toutes les organisations réalisant un travail soumis aux BPx sont tenues, de par les directives existantes de l'OMS, d'établir, de mettre en œuvre et de maintenir un système approprié de gestion de la qualité dont les éléments doivent être documentés dans un format prescrit, tel qu'un manuel qualité ou une autre documentation appropriée. Le manuel qualité ou une documentation équivalente doit inclure une déclaration de la politique de qualité de la direction et son engagement d'utiliser un système efficace de gestion de la qualité et des bonnes pratiques professionnelles. Ces règles doivent comprendre un code d'éthique et un code de bonne conduite pour s'assurer de la fiabilité et l'intégralité des données, et comprendre des mécanismes permettant au personnel de rapporter à la direction toute préoccupation ou toute question relative à la gestion de la qualité ou la conformité des opérations.

5.2 Au sein du système de gestion de la qualité, l'organisation doit établir l'infrastructure appropriée, la structure organisationnelle, les règles et les procédures écrites, les processus et les systèmes afin de prévenir et de détecter les situations qui pourraient impacter l'intégrité des données et donc la robustesse scientifique des décisions basées sur une gestion du risque associé à ces données.

5.3 La gestion du risque qualité (QRM) est une composante essentielle d'un programme efficace de validité des données et des enregistrements. L'effort et les ressources attribués à la gestion des données et des enregistrements doivent être proportionnels au risque qualité lié au produit. L'approche basée sur le risque pour la gestion des enregistrements et des données doit garantir que les ressources adéquates sont attribuées et que les stratégies de maîtrise de

l'assurance d'intégrité des données BPx sont proportionnées à l'impact potentiel sur la qualité du produit, la sécurité du patient et la prise de décision associée.

5.4 Les stratégies qui mettent en avant les bonnes pratiques et préviennent les problèmes d'intégrité des enregistrements et des données sont recommandées et sont probablement les plus efficaces et les moins coûteuses. Par exemple, les contrôles d'accès autorisant uniquement les personnes détentrices des autorisations appropriées à modifier une formule ou une étape d'un procédé réduiront la probabilité que des données invalides et aberrantes soient créées. De telles mesures préventives, lorsqu'elles sont mises en œuvre efficacement, réduisent également l'importance de la surveillance requise pour détecter les modifications non-contrôlées.

5.5 Les risques d'altération de l'intégrité des enregistrements et des données doivent être évalués, corrigés, communiqués et revus à travers du cycle de vie des données, selon les principes du QRM. Des exemples d'approches pouvant améliorer la fiabilité des données sont donnés dans ce guide mais doivent être considérés comme des recommandations seulement. D'autres approches peuvent être justifiées et indiquées comme étant aussi efficaces dans l'atteinte d'un niveau de contrôle de risque satisfaisant. Les organisations doivent ainsi concevoir des outils et des stratégies appropriés pour la gestion des risques d'intégrité des données basée sur leurs propres activités BPx, les technologies et les processus employés.

5.6 Un programme de gestion des données développé et mis en œuvre sur la base des principes sûrs du QRM est attendu pour exploiter les technologies existantes selon leur plein potentiel. En retour cela rationalisera les processus de données d'une manière améliorant non seulement la gestion des données mais aussi l'efficience et l'efficacité des processus de gestion, réduisant ainsi les coûts et facilitant l'amélioration continue.

6. Gouvernance de la gestion et des audits de qualité

6.1 Obtenir l'assurance d'une intégrité des données robuste commence avec la direction, qui a la responsabilité générale des opérations techniques et la mise à disposition des ressources pour assurer la qualité requise des activités BPx. La haute direction a la responsabilité ultime d'assurer que le système de qualité effective est en place pour atteindre les objectifs de qualité et que les rôles du personnel, les responsabilités et les autorités, incluant ceux requis pour les programmes effectifs d'administration des données, sont définis, communiqués et implémentés à travers l'organisation. Le rôle de l'encadrement est essentiel pour établir et maintenir dans l'ensemble de l'entreprise un engagement de fiabilité des données en tant qu'élément essentiel du système qualité.

6.2 L'ensemble des éléments constitutifs des comportements, des considérations procédurales et d'ordre politique et de contrôles techniques minimums forme la base de la bonne gouvernance des données, sur laquelle les futures révisions peuvent être établies. Par exemple, un programme de bonne gouvernance des données requiert les dispositions nécessaires prises par la direction pour s'assurer que le personnel n'est pas soumis à des

pressions commerciales, politiques, financières et autres ou à des conflits d'intérêts qui peuvent affecter négativement la qualité de leur travail et l'intégrité de leurs données. La direction doit aussi faire prendre conscience au personnel de la pertinence de l'intégrité des données et de l'importance de son rôle pour la protection de la sécurité de patients et pour la réputation de leur organisation en termes de qualité des produits et des services.

6.3 La direction doit créer un environnement de travail tel que le personnel se trouve encouragé à communiquer les échecs et les erreurs, incluant les enjeux de fiabilité des données, de manière à ce que des actions correctives et préventives puissent être prises et d'améliorer la qualité des produits et des services de l'organisation. Cela comprend la mise en place d'un flux d'information approprié à tous les niveaux du personnel. La direction générale doit activement décourager toute pratique de gestion dont on peut logiquement s'attendre à ce qu'elles freinent le signalement actif, et complet, de tels problèmes, par exemple, les contraintes hiérarchiques et la culture du reproche.

6.4 Les revues de direction et les rapports réguliers des mesures de qualité prises facilitent l'atteinte de ces objectifs. Cela nécessite la désignation d'un responsable qualité qui a un accès direct au plus haut niveau de la direction et qui peut lui communiquer directement les risques, de manière que la direction générale soit informée de tout problème et puisse allouer les ressources pour les résoudre. Pour satisfaire à ce rôle, l'unité qualité doit conduire des revues du risque, formalisées et documentées selon les indicateurs clés de performance du système de gestion de la qualité, et les rapporter à la direction. Cela doit aider à inclure les mesures liées à l'intégrité des données qui aideront à identifier les opportunités d'amélioration. Par exemple :

- le suivi et l'étude des tendances des données invalides et aberrantes peuvent révéler une variabilité inattendue des processus et des procédures précédemment estimés robustes, et peuvent éclairer des opportunités pour améliorer les procédures analytiques et leur validation, la validation des processus, la formation du personnel et l'approvisionnement des matières premières et des articles ;

- une revue adéquate des audit-trails, y compris de ceux examinés en tant qu'étapes-clés de prise de décision (par exemple la libération BPF des lots, l'émission d'un rapport BPL d'étude ou l'approbation des formulaires de rapport d'un évènement), peuvent révéler un traitement incorrect des données, peuvent aider à empêcher la remontée de résultats incorrects et d'identifier le besoin d'une formation additionnelle du personnel ;

- les audits de routine et/ou les auto-inspections des systèmes informatisés peuvent révéler des lacunes dans les contrôles de sécurité qui permet involontairement au personnel d'accéder et potentiellement modifier des horodatages. De telles constatations aident à augmenter la sensibilisation au sein de la direction autour du besoin d'allouer des ressources pour améliorer les contrôles de validation des systèmes informatisés ;

- la surveillance des sous-traitants et le suivi et l'étude des tendances des indicateurs de qualité associés pour ces sites permettent d'identifier les risques pouvant indiquer le besoin d'un engagement plus actif et l'attribution de ressources additionnelles par le donneur d'ordre pour s'assurer que les normes de qualité soient respectées.

6.5 Les audits de qualité des fournisseurs, les auto-inspections et les revues du risque doivent identifier et permettre d'informer la direction des opportunités d'amélioration des fondamentaux des systèmes et des processus ayant un impact sur la fiabilité des données. L'attribution par la direction de ressources pour l'amélioration des systèmes et des processus peut réduire efficacement les risques d'intégrité des données. Par exemple, identifier et résoudre les difficultés techniques avec l'équipement utilisé pour effectuer des opérations BPx multiples peut grandement améliorer la fiabilité des données pour toutes ces opérations. Un autre exemple a trait à l'identification des conflits d'intérêts affectant la sécurité. Allouer un personnel de support technique indépendant pour effectuer l'administration système des systèmes informatisés, incluant la gestion de la sécurité, de la sauvegarde et de l'archivage, réduit les conflits d'intérêts potentiels et peut grandement rationaliser et améliorer l'efficacité de la gestion des données.

6.6 Tous les enregistrements BPx détenus par l'organisation BPx sont soumis aux inspections des autorités de santé compétentes. Ceci comprend les données et métadonnées électroniques originales, telles que les audit-trails stockés dans les systèmes informatisés. La gestion des donneurs d'ordre et des sous-traitants doit permettre de s'assurer que les ressources appropriées sont disponibles et que les procédures relatives aux systèmes informatisés sont disponibles pour ces inspections. Le personnel d'administration des systèmes doit être disponible pour extraire les enregistrements demandés et pour faciliter les inspections.

7. Organisations sous-traitantes, fournisseurs et prestataires de service

7.1 L'accroissement de l'externalisation des tâches BPx à des structures sous-traitantes, par exemple à des organisations de recherche contractuelle, à des fournisseurs et à d'autres prestataires de services, augmente le besoin d'établir et de maintenir fermement les rôles et les responsabilités définis pour s'assurer, au travers de ces relations, de données et d'enregistrements complets et exact. Les responsabilités du donneur d'ordre et du contractant doivent aborder de manière exhaustive les processus de chaque partie devant être suivis pour garantir l'intégrité des données. Ces détails doivent être mentionnés dans le contrat conformément aux BPx de l'OMS applicables au travail externalisé accompli ou aux services fournis.

7.2 L'organisation qui externalise le travail est responsable de l'intégrité de tous les résultats rapportés, incluant ceux fournis par tout sous-traitant ou tout prestataire de services. Ces responsabilités s'étendent à tout prestataire de service informatisé. Lors de l'externalisation des bases de données et de la fourniture de logiciel, le donneur d'ordre doit s'assurer que tous les

sous-traitants se sont mis d'accord et sont inclus dans l'accord de qualité avec l'accepteur d'ordre et qu'ils sont qualifiés et formés de manière appropriée en BDP. Leurs activités doivent être surveillées de manière régulière selon des intervalles définis par une évaluation du risque. Cela s'applique également aux prestataires de services basés dans le ''nuage'' [cloud].

7.3 Pour satisfaire à cette responsabilité, en plus d'avoir leurs propres systèmes de gouvernance, les sociétés sous-traitantes doivent vérifier l'adéquation des systèmes d'administration du contactant par un audit ou tout autre moyen convenable. Cela doit comprendre l'adéquation du contrat des contrôles du contractant sur ses fournisseurs et une liste de tierce-parties significatifs autorisés à travaillant pour le contractant.

7.4 Le personnel qui évalue et apprécie régulièrement la compétence des organisations sous-traitances ou des prestataires de services doivent posséder le niveau d'instruction, les qualifications, l'expérience et la formation appropriés, pour juger leurs systèmes de gouvernance de l'intégrité des données et pour détecter les problèmes de validité. La nature et la fréquence de l'appréciation du contractant et la surveillance continue de leur travail doivent être basées sur l'évaluation documentée du risque. L'évaluation doit inclure une évaluation des processus de données pertinents et de leurs risques.

7.5 Les stratégies attendues pour la maîtrise de l'intégrité des données doivent être insérées, de manière appropriée, dans les accords qualité, le contrat écrit ou les spécifications techniques, établis entre le donneur d'ordre et le contractant. Celles-ci doivent comprendre des dispositions pour que le donneur d'ordre puisse avoir accès aux données pertinentes détenues par le sous-traitant relatives au produit du donneur d'ordre ou aux services ainsi que tous les enregistrements correspondants des systèmes qualité. Cela doit également inclure l'autorisation d'accès par le donneur d'ordre aux enregistrements électroniques - incluant les audit-trails - détenus dans les systèmes informatisés du sous-traitant et tous les rapports imprimés et les autres enregistrements appropriés sous forme papier ou électronique.

7.6 Lorsque la conservation des données et des documents est sous-traitée à un tiers, une attention particulière doit être prêtée pour comprendre comment la propriété et l'extraction des données sont organisées. L'endroit physique où les données sont détenues et l'impact de toute loi applicable à cette localisation doivent aussi être pris en compte. Les accords et les contrats doivent décrire les conséquences, qui doivent être mutuellement acceptées, d'une situation où le sous-traitant rejette, refuse ou limite l'accès du donneur d'ordre aux enregistrements que lui-même détient. Les accords et les contrats doivent également contenir des dispositions pour les actions à entreprendre dans le cas d'une interruption de l'activité ou d'une faillite de la partie tierce pour s'assurer que l'accès reste maintenu et que les données puissent être transférées avant la cessation de toutes les activités commerciales.

7.7 Quand des bases de données sont externalisées, le donneur d'ordre doit s'assurer, si elles sont confiées à nouveau, en particulier à des prestataires de service opérant dans le ''nuage'', qu'ils sont inclus dans l'accord de qualité, qu'ils sont qualifiés et sont formés convenablement en BPGDE. Leurs activités doivent être suivies régulièrement à intervalles définis selon l'évaluation du risque.

8. Formation sur les bonnes pratiques de gestion des données et des enregistrements

8.1 Le personnel doit être formé aux règles d'intégrité des données et doit s'engager à les respecter. La direction doit s'assurer que le personnel est formé pour comprendre et distinguer une bonne d'une mauvaise conduite, incluant la falsification délibérée, et doit être informé des conséquences potentielles.

8.2 De plus, le personnel clé, incluant les directeurs, les superviseurs et le personnel de l'unité qualité, doit être formé aux mesures permettant de prévenir et de détecter les enjeux relatifs aux données. Cela peut nécessiter une formation spécifique dans l'évaluation des paramètres de configuration et la revue des données et métadonnées électroniques, telles que les audit-trails, pour des systèmes informatisés individuels utilisés dans la création, le traitement et le rapport de données. Par exemple, l'unité qualité doit apprendre comment évaluer les paramètres de configuration qui peuvent permettre d'écraser ou de masquer des données, intentionnellement ou non, par l'utilisation de champs cachés ou d'outils d'annotation des données. Les superviseurs en charge de la revue des données électroniques doivent apprendre, dans un système, quels audit-trails suivent les modifications significatives des données et comment il est possible d'accéder à celles-ci le plus efficacement dans le cadre de leur revue.

8.3 La direction doit également s'assurer au moment de l'embauche et si nécessaire à intervalles réguliers ensuite, que tous les personnels sont formés aux procédures de bonnes pratiques de documentation pour les enregistrements papier et électroniques. L'unité qualité doit inclure dans son travail quotidien des vérifications de la conformité aux bonnes pratiques documentaires, aussi bien pour les enregistrements papier et électroniques que pour les audits et les auto-inspections des systèmes et des installations, et doit signaler toutes les opportunités d'amélioration à la direction.

9. Bonnes pratiques de documentation

9.1 Les éléments de base des bonnes pratiques relatives aux données BPx consistent à suivre les bonnes pratiques documentaires et ensuite à gérer les risques relatifs à l'exactitude, à l'intégralité, à la cohérence et à la fiabilité des données tout au long de leur temps d'usage – c'est-à-dire, tout au long du cycle de vie des données. Le personnel doit appliquer les bonnes pratiques documentaires afin d'assurer l'intégrité des données tant pour les enregistrements papier que pour les enregistrements électroniques. Ces principes supposent que la documentation est : attribuable, lisible, concomitante, originale et exacte (parfois désigné par l'acronyme anglais ALCOA). Ces caractéristiques essentielles s'appliquent aussi bien aux enregistrements papier et qu'électroniques.

9.2 **Attribuable** signifie que l'information enregistrée est saisie de manière à ce qu'elle puisse être indubitablement identifiée comme étant créée par l'auteur des données lui-même (par exemple une personne ou un système informatique).

9.3 Les termes **lisible**, **traçable** et **permanent** se réfèrent aux exigences de lisibilité et d'intelligibilité des données et au fait qu'elles permettent une représentation claire du séquençage des étapes ou des évènements de l'enregistrement, de telle manière que toutes les activités BPx conduites puissent être reconstituées intégralement par les personnes examinant ces enregistrements ceci à tout moment pendant la période de conservation des enregistrements posée par les BPx applicables.

9.4 Les données **concomitantes** sont celles enregistrées au moment où elles sont générées ou observées.

9.5 Une donnée **originale** correspond à la première saisie ou à la première acquisition d'une donnée ou d'une information et toutes les données consécutives requises pour reconstituer intégralement l'exécution de l'activité BPx. Les exigences BPx pour les données originales incluent ce qui suit :

- les données originales doivent être revues ;
- les données originales et/ou les copies authentiques ou certifiées qui préservent le contenu et la signification des données originales doivent être conservées ;
- les enregistrements originaux doivent donc être complets, durables et aisément récupérables et lisibles tout au long de la période de conservation de ces enregistrements.

9.6 Le terme « exact » signifie que les données sont correctes, fidèles, complètes, valides et fiables.

9.7 Implicitement, selon les exigences contenues et listées « ALCOA », il convient que les enregistrements soient complets, cohérents, durables et disponibles (pour souligner ces exigences, elles sont parfois désignées par ALCOA-plus).

9.8 Les autres directives destinées à aider à la compréhension des modalités d'application de ces exigences dans chaque cas et les considérations de risques spécifiques qu'il peut être nécessaire de prendre pendant toute mise en œuvre sont fournies dans l'annexe 1.

10. Conception et validation des systèmes pour assurer la qualité et la fiabilité des données

10.1 Les méthodes et les systèmes de conservation des enregistrements, qu'ils soient sous format papier ou électronique, doivent être conçus de telle manière qu'ils encouragent la conformité et assurent la qualité et la fiabilité des données. Toutes les exigences et tous les contrôles nécessaires pour assurer les BPGDE doivent être observés à la fois pour les enregistrements papiers et électroniques.

Validation pour s'assurer des bonnes pratiques de documentation pour les données électroniques

10.2 Afin d'assurer l'intégrité des données électroniques, les systèmes informatisés doivent être validés à un niveau approprié à leur utilisation et leur application. La validation doit mettre en œuvre les contrôles nécessaires pour assurer l'intégrité des données, incluant les données électroniques originales et toute impression ou rapport PDF du système. En particulier, l'approche doit s'assurer que les bonnes pratiques documentaires seront utilisées et que les risques d'intégrité des données seront correctement gérés durant le cycle de vie des données.

10.3 Le « Supplementary guidelines on good manufacturing practices: validation » (WHO Technical Report Series, No. 937, 2006, Annex 4 (2–4)1 fournit une présentation plus complète des aspects liés à la validation. Les aspects clés de la validation permettent d'assurer que les bonnes pratiques documentaires pour les données électroniques incluent, mais ne se limitent pas, aux points suivants.

10.4 Implication de l'utilisateur. Les utilisateurs doivent être impliqués de manière appropriée dans les activités de validation pour définir les données critiques et les contrôles du cycle de vie des données qui assurent l'intégrité des donnés.
Des exemples d'activités impliquant les utilisateurs peuvent inclure : le prototypage, les spécifications utilisateurs des données critiques afin que des contrôles basés sur le risque puissent être appliqués, l'implication de l'utilisateur dans les tests pour en faciliter l'acceptation et celle de la connaissance par l'utilisateur des caractéristiques du système, et autres.

10.5 Maîtrise de la configuration et de la conception. Les activités de validation doivent garantir que les paramètres de configuration et que les contrôles de conception selon les bonnes pratiques de documentation sont autorisés et gérés à travers l'environnement informatisé (incluant aussi bien les environnements d'application logicielle que les environnements de systèmes d'exploitation).

Ces activités comprennent, mais ne sont pas limitées à :

- documenter les spécifications de la configuration des systèmes couramment commercialisés ainsi que, le cas échéant, des systèmes développés pour les utilisateurs ;
- limiter la configuration des paramètres de sécurité et d'administration du système pour les personnes extérieurs lorsque c'est techniquement faisable ;
- désactiver les paramètres de configuration qui permettent d'écraser et de retraiter des données sans en avoir de traçabilité ;
- restreindre les accès à l'horodatage.

Pour les systèmes utilisés dans des essais cliniques, les contrôles de configuration et de conception doivent être en place pour protéger la randomisation en aveugle de l'essai, par exemple en limitant l'accès aux données de randomisation qui peuvent être stockées par voie électronique.

10.6 Cycle de vie des données. La validation doit inclure l'évaluation du risque et les stratégies de réduction des risques qualité pour le cycle de vie des données, en incluant les contrôles pour prévenir et détecter les risques pendant les étapes de :

- création et saisie des données ;
- transmission des données ;
- traitement des données ;
- revue des données ;
- rapport des données, incluant la manipulation des données invalides et atypiques ;
- stockage et récupération des données ;
- élimination des données.

Les activités peuvent comprendre, mais ne sont pas limitées à :

- déterminer l'approche basée sur le risque pour la revue des données électroniques et des audit-trails en s'appuyant sur la compréhension du processus et la connaissance de l'impact potentiel sur les produits et les patients ;

- écrire des procédures (SOPs) définissant la revue des enregistrements électroniques originaux et incluant les métadonnées significatives telles que les audit-trails et la revue de toute impression associée ou d'enregistrements PDF ;

- documenter l'architecture système et le flux des données, incluant le flux de données électroniques et toutes les métadonnées associées, du moment de leur création jusqu'à leur archivage et leur récupération ;

- assurer que la relation entre les données et les métadonnées sont conservées intactes au cours du cycle de vie des données.

10.7 Procédures (SOPs) et formation. Les activités de validation doivent garantir que la formation et les procédures adéquates sont développées avant de permettre l'utilisation du système pour une application BPx. Elles doivent aborder :

- la gestion des systèmes informatisés ;

- l'utilisation des systèmes informatisés ;

- la revue de données électroniques et de métadonnées significatives, telles que les audit-trails, incluant la formation qui peut être nécessaire pour permettre aux

utilisateurs de traiter les données et de réviser les données électroniques et les métadonnées de manière efficiente et efficace.

10.8 D'autres contrôles de validation pour assurer une bonne gestion des données à la fois des données électroniques et des données papier associées doivent être mis en œuvre d'une manière jugée appropriée pour le type de système et son usage prévu.

11. Gestion des données et des enregistrements tout au long du cycle de vie des données

11.1 Les processus de données doivent être conçus pour réduire et contrôler de manière adéquate, et de réviser continuellement, les risques d'intégrité des données associés aux étapes d'acquisition, de traitement, de revue et de rapport des données, aussi bien que le flux physique des données et des métadonnées associées pendant ce processus à travers leur stockage et leur récupération.

11.2 Le QRM du cycle de vie des données nécessite la compréhension scientifique et technologique des processus de données et de leurs limitations inhérentes. Une bonne conception des processus de données, basée sur la compréhension des processus et l'application des principes scientifiques solides, incluant le QRM, est devrait augmenter l'assurance de l'intégrité des données et résulter en un processus d'organisation efficace et efficient.

11.3 Les risques relatifs à l'intégrité des données sont plus susceptibles de survenir et d'être plus élevés lorsque les processus de traitement des données ou des étapes spécifiques de ces processus sont inconstants, subjectifs, biaisés, non-sécurisés, inutilement complexes ou redondants, recopiés, non-définis, mal compris, hybrides, basés sur des suppositions non fondées et/ou ne respectent pas les BPGDE.

11.4 Lorsque cela est possible la bonne conception des processus de données doit prendre en compte, pour chaque étape du processus de données, la vérification et l'amélioration des contrôles de manière à ce que chaque étape soit :

- cohérente ;
- objective, indépendante et sécurisée ;
- simple et rationalisée ;
- bien définie et comprise ;
- automatisée ;
- fondée scientifiquement et statistiquement ;
- correctement documentée selon les BPGDE.

Des exemples de mesures pour chaque phase du cycle de vie des données sont donnés ci-dessous.

11.5 Collecte et enregistrement de données. Toute collecte et tout enregistrement de donnée

doivent se dérouler conformément aux BPGDE et doivent appliquer des contrôles basés sur le risque pour protéger et vérifier les données critiques.

11.6 Les entrées de données, telles que l'identification des échantillons pour les tests de laboratoire ou l'enregistrement de données sources pour l'inclusion d'un patient dans un essai clinique, par exemple, doivent être vérifiées par une deuxième personne ou saisies par des moyens techniques tels que des codes-barres, au plus approprié compte tenu de l'utilisation prévue de ces données. Des contrôles supplémentaires peuvent comprendre le verrouillage de saisies de données après vérification et des revues des audit-trails des données critiques afin de pouvoir détecter si elles ont été modifiées.

11.7 Traitement des données. Pour assurer l'intégrité des données, le traitement des données doit être fait d'une manière objective, non biaisée, selon des protocoles, des processus, des méthodes, des systèmes, des équipements validés/qualifiés ou vérifiés et selon les procédures et les programmes de formation approuvés.

11.8 Autres exemples de mesures. Les organisations BPx doivent prendre des précautions pour décourager l'orientation des essais ou des procédés de données vers un résultat souhaité.

Par exemple :

- pour minimiser le biais potentiel et assurer des traitements de données cohérents, des méthodes de tests doivent avoir spécifié des paramètres d'obtention et de traitement des échantillons, si nécessaire formalisés par défaut dans des fichiers d'acquisition électronique maîtrisés par leur version et dans des fichiers de méthode de traitement. Des modifications de ces paramètres fixés par défaut peuvent être nécessaires pendant le traitement des échantillons, mais ces changements doivent être documentés (qui, quoi, quand ?) et justifié (pourquoi ?) ;

- les tests de conformité d'un système doivent seulement comprendre des substances de référence de concentration connue pour fournir un comparateur approprié pour juger de la variabilité potentielle de l'instrument. Des procédures écrites doivent être établies et suivies si un échantillon (par exemple une substance secondaire bien caractérisée) est utilisé pour vérifier la conformité du système ou pour un essai, et les résultats doivent être inclus dans le processus de revue des données. Le produit analysé ne doit pas être utilisé à des fins d'essais ou pour évaluer la conformité du système ;

- les études cliniques et de sécurité doivent être conçues pour prévenir et détecter les biais statistiques qui peuvent figurer dans des calculs statistiques en raison d'une sélection inappropriée de données.

11.9 Revue et rapports de données. Les données doivent être revues et, si nécessaire, évaluées statistiquement à la fin processus pour déterminer si les résultats sont cohérents et en conformité aux normes établies. L'évaluation doit prendre en considération toutes les données,

y compris les données atypiques, suspectes ou rejetées, conjointement avec les données rapportées. Ceci inclut une revue des enregistrements papier et électroniques originaux.

11.10 Par exemple, lors d'une auto-inspection, certaines questions clés à demander sont : Est-ce que je collecte toutes mes données ? Est-ce que j'examine toutes mes données ? Si j'ai exclu des données de mon processus de prise de décision, quelle en est la justification, et toutes les données sont-elles conservées, incluant aussi bien les données rejetées que rapportées ?

11.11 La démarche de revue du contenu d'enregistrements spécifiques, tels que les champs de données critiques et les métadonnées comme les rayures sur des enregistrements papier et les audit-trails dans les enregistrements électroniques, doit répondre à toutes les exigences réglementaires et doit être basée sur le risque.

11.12 Toute obtention de résultats non-habituels ou atypiques doit faire l'objet d'une enquête. Ceci inclut l'examen et de la détermination des actions correctives et préventives pour les cycles invalidés, les échecs, les répétitions et toute autre donnée atypique. Toutes les données doivent être incluses dans les paquets de données sauf si leur exclusion est documentée et scientifiquement expliquée.

11.13 Pendant le cycle de vie des données, les données doivent, le cas échéant, être soumises à une surveillance continue pour améliorer la compréhension des processus et pour faciliter la gestion de la connaissance et la prise de décision éclairée.

11.14 Exemple de mesure. Pour s'assurer que l'ensemble des données est pris en compte dans les données rapportées, la revue des données électroniques doit inclure des vérifications de tous les endroits où les données peuvent être stockées, y compris les endroits où des données annulées, supprimées, invalidées ou rejetées ont été stockées.

11.15 Conservation et récupération des données. La conservation des enregistrements papier et électroniques est discutée dans la section ci-dessus, qui comprend les mesures de sauvegarde et l'archivage des données électroniques et des métadonnées.

11.16 Exemple de mesure

1) Dans des systèmes autonomes les dossiers de données peuvent ne pas inclure tous les audit-trails ou les autres métadonnées nécessaires pour reconstituer toutes les activités. D'autres métadonnées peuvent être retrouvées dans d'autres dossiers électroniques ou dans les journaux des systèmes d'exploitation. Lors de l'archivage des données électroniques, il est important de s'assurer que les métadonnées associées sont archivées avec le jeu de données correspondant ou sont traçables de manière sécurisée vers le jeu de données à travers la documentation appropriée. La possibilité d'extraire avec succès le jeu de données entier, incluant les métadonnées, à partir des archives, doit être vérifiée.

2) Seuls des systèmes validés sont utilisés pour le stockage de données ; cependant, le

support utilisé pour le stockage des données n'a pas une durée de vie infinie. Il faut prendre en compte la longévité des supports et de l'environnement dans lesquels ils sont stockés. Des exemples comprennent l'effacement des enregistrements sur microfilm, la lisibilité décroissante due au vernis des supports optiques tels que les disques compacts (CDs) et les disques versatiles/vidéos numériques (DVDs), et le fait que ces supports peuvent devenir cassants. De manière similaire, les données historiques stockées sur des supports magnétiques deviendront aussi, du fait de leur détérioration, illisibles dans le temps.

12. Résolution des problèmes de fiabilité des données

12.1 Lorsque des problèmes de validité et de fiabilité sont découverts, il est important que leur impact potentiel sur la sécurité du patient et la qualité du produit et sur la fiabilité de l'information utilisée pour la prise de décision et pour le dépôt de dossier soit examiné comme une priorité de premier ordre. Les autorités sanitaires doivent être notifiées si l'enquête identifie un impact matériel sur des patients, des produits, des informations rapportées ou des dossiers déposés.

12.2 L'enquête doit garantir que les copies de toutes les données sont sécurisées dans un délai convenable pour permettre une revue minutieuse de l'évènement et de tous les processus potentiellement associés.

12.3 Les personnes impliquées doivent être interrogées pour mieux comprendre la nature du problème, comment il s'est produit et ce qui aurait pu être fait pour prévenir ou détecter le problème plus tôt. Cela doit inclure des discussions avec les personnes impliquées dans les questions d'intégrité des données, aussi bien que les superviseurs, le personnel d'assurance qualité et la direction.

12.4 L'enquête ne doit pas être limitée aux problèmes spécifiques identifiés mais doit également considérer l'impact potentiel sur les décisions précédentes basées sur les données et les systèmes trouvés non-fiables maintenant. De plus, il est vital que la cause la plus profonde (c'est-à-dire la(les) cause(s) sous-jacente(s)) du problème soit être prise en compte, en incluant les pressions éventuelles et les incitations de la direction, par exemple, un manque de ressources adéquates.

12.5 Des actions correctives et préventives doivent non seulement aborder le problème identifié, mais aussi les décisions et les jeux de données qui sont impactés, ainsi que les causes les plus profondes et sous-jacentes, comprenant le besoin de rectification des exigences de la direction et l'allocation de ressources supplémentaires pour empêcher que ces risques se reproduisent à l'avenir.

Références et lectures additionnelles

Références

1. WHO good manufacturing practices for pharmaceutical products: main principles. In: WHO Expert Committee on Specifications for Pharmaceutical Preparations: forty-eighth report. Geneva: World Health Organization; 2014: Annex 2 (WHO Technical Report Series, No. 986), également disponible sur CD-ROM et en ligne.

2. Supplementary guidelines on good manufacturing practice: validation. In: WHO Expert Committee on Specifications for Pharmaceutical Preparations: fortieth report. Geneva: World Health Organization; 2006: Annex 4 (WHO Technical Report Series, No. 937).
3. Supplementary guidelines on good manufacturing practice: validation. Qualification of systems and equipment. In: WHO Expert Committee on Specifications for Pharmaceutical Preparations: fortieth report. Geneva: World Health Organization; 2006: Annex 4, Appendix 6 (WHO Technical Report Series, No. 937).

4. Supplementary guidelines on good manufacturing practices: validation. Validation of computerized systems. In: WHO Expert Committee on Specifications for Pharmaceutical Preparations: fortieth report. Geneva: World Health Organization; 2006: Annex 4, Appendix 5 (WHO Technical Report Series, No. 937).

Lectures additionnelles

Computerised systems. In: The rules governing medicinal products in the European Union. Volume 4 : Good manufacturing practice (GMP) guidelines: Annexe 11. Brussels: European Commission (http:// ec.europa.eu/enterprise/pharmaceuticals/eudralex/vol-4/pdfs-en/anx11en.pdf).

Good automated manufacturing practice (GAMP) good practice guide: electronic data archiving. Tampa (FL): International Society for Pharmaceutical Engineering (ISPE); 2007.

Good automated manufacturing practice GAMP good practice guide: A risk-based approach to GxP compliant laboratory computerized systems, 2nd edition. Tampa (FL): International Society for Pharmaceutical Engineering (ISPE); 2012.

MHRA GMP data integrity definitions and guidance for industry. London: Medicines and Healthcare Products Regulatory Agency; March 2015 (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/412735/Data_integrity_definitions_and_guidance_v2.pdf).

OECD series on principles of good laboratory practice (GLP) and compliance monitoring. Paris: Organisation for Economic Co-operation and Development (http://www.oecd.org/chemicalsafety/

testing/oecdseriesonprinciplesofgoodlaboratorypracticeglpandcompliancemonitoring.htm).

Official Medicines Control Laboratories Network of the Council of Europe: Quality assurance documents: PA/PH/OMCL (08) 69 3R – Validation of computerised systems – core document (https://www.edqm.eu/sites/default/files/medias/fichiers/Validation_of_Computerised_Systems_Core_Document.pdf) and its annexes:

- PA/PH/OMCL (08) 87 2R – Annex 1: Validation of computerised calculation systems: example of validation of in-house software (https://www.edqm.eu/sites/default/files/medias/fichiers/NEW_Annex_1_Validation_of_ computerised_calculation.pdf).
- PA/PH/OMCL (08) 88 R – Annex 2: Validation of databases (DB), laboratory information management systems (LIMS) and electronic laboratory notebooks (ELN) (https://www.edqm.eu/sites/default/files/medias/fichiers/NEW_Annex_2_Validation_of_ Databases_DB_Laboratory_.pdf).

PA/PH/OMCL (08) 89 R – Annex 3: Validation of computers as part of test equipment (https://www.edqm.eu/sites/default/files/medias/fichiers/NEW_Annex_3_Validation_of_computers_as_part_of_tes.pdf).

Title 21 Code of Federal Regulations (21 CFR Part 11): Electronic records; electronic signatures. US Food and Drug Administration. The current status of 21 CFR Part 11 Guidance is located under Regulations and Guidance at : http://www.fda.gov/cder/gmp/index.htm — see background: http://www.fda.gov/ OHRMS/DOCKETS/98fr/03-4312.pdf.

PIC/S guide to good manufacturing practice for medicinal products annexes: Annex 11 – Computerised systems. Geneva: Pharmaceutical Inspection Co-operation Scheme.
PIC/S PI 011-3 Good practices for computerised systems in regulated GxP environments. Geneva: Pharmaceutical Inspection Co-operation Scheme.

WHO good manufacturing practices for active pharmaceutical ingredients. In: WHO Expert Committee on Specifications for Pharmaceutical Preparations: forty-fourth report. Geneva: World Health Organization; 2010: Annex 2 (WHO Technical Report Series, No. 957).

WHO good practices for pharmaceutical quality control laboratories. In: WHO Expert Committee on Specifications for Pharmaceutical Preparations: forty-fourth report. Geneva: World Health Organization; 2010: Annex 1 (WHO Technical Report Series, No. 957).

Appendice 1

Exigences et exemples de gestion du risque spécifique à la mise en œuvre des principes ALCOA (-plus) (ALCOA : Attribuable, lisible, concomitant, original, exact / ALCOA-plus : complet, cohérent, durable, disponible) dans les systèmes papiers et électroniques. Les organisations devraient suivre les bonnes pratiques de documentation (BPDoc) afin d'assurer l'exactitude, l'exhaustivité, la cohérence et la fiabilité des enregistrements et des données au cours de la totalité de leur période d'utilisation – c'est-à-dire : tout au long du cycle de vie des données. Ces principes requièrent que la documentation soit attribuable, lisible, concomitante, originale et exacte (propriétés parfois désignées par l'acronyme ALCOA).

Les tableaux de cet appendice fournissent des indications supplémentaires quant à l'implémentation des exigences générales ALCOA à la fois pour les enregistrements papier et électroniques ainsi que pour les systèmes. De plus, des exemples particuliers de gestion du risque et plusieurs exemples indicatifs sont fournis sur la manière dont ces mesures sont généralement implémentées. Ces exemples indicatifs sont fournis pour aider à la compréhension des concepts et de la manière de réaliser avec succès une implémentation basée sur le risque. Ces exemples ne doivent pas être considérés comme établissant de nouvelles exigences normatives.

Attribuable

Attribuable signifie que l'information est saisie dans l'enregistrement de manière à ce qu'elle soit identifiée de manière unique comme ayant été exécutée par l'auteur des données (par exemple : une personne ou un système informatique).

Exigences pour les enregistrements papier	**Exigences pour les enregistrements électroniques**
L'attribution des actions pour les enregistrements papier doit avoir lieu, selon le cas, au moyen : • de paraphes ; • de la signature manuscrite complète ; • du sceau personnel ; • de la date et, si nécessaire, de l'heure.	L'attribution des actions dans des enregistrements électroniques doit avoir lieu, selon le cas, au moyen : • de connexions utilisateur uniques qui font le lien entre l'utilisateur et les actions de création, de modification ou de suppression des données ; • de signatures électroniques uniques (pouvant être soit biométriques soit non-biométriques) ; • d'un audit-trail qui devrait contenir l'identifiant de l'utilisateur (ID) et être horodaté ; • de signatures, qui doivent être liées de manière sûre et permanente à l'enregistrement signé.

Indications relatives à la gestion du risque pour les contrôles visant à assurer que les actions et les enregistrements sont attribués à un individu unique

- Pour des signatures juridiquement contraignantes, il doit y avoir un lien sûr et vérifiable entre la personne (courante) unique et identifiable qui signe et l'exécution de la signature. Les signatures doivent être liées en permanence à l'enregistrement faisant l'objet de la signature. Les systèmes qui utilisent une application pour signer un document et une autre application pour stocker le document faisant l'objet de la signature doivent garantir que le document et la signature deux restent liés de manière à assurer que le lien (attribution) ne soit pas rompu.
- Les signatures doivent être exécutées et les sceaux personnels doivent être utilisés concomitamment à la revue ou à la réalisation de l'évènement ou de l'action devant être enregistrée.
- L'utilisation d'un sceau personnel pour signer des documents nécessite des contrôles supplémentaires de gestion du risque, tels que des dates manuscrites et des procédures qui requièrent le stockage du sceau dans un endroit sûr avec un accès limité uniquement à l'individu assigné, ou équipé d'autres moyens de prévention d'un abus potentiel.
- L'utilisation d'images numérisées de la signature manuscrite d'une personne pour signer un document n'est pas acceptable. Cette pratique compromet la confiance relative à l'authenticité de ces signatures lorsque de telles images sauvegardées ne sont pas conservées dans un endroit sûr, dont l'accès est limité uniquement à l'individu auquel la signature est assignée ou équipé d'autres moyens pour prévenir les abus potentiel, et sont placées, au lieu de cela, dans des documents et des courriels où elles peuvent être aisément copiées et réutilisées par d'autres. Des signatures manuscrites juridiquement contraignantes doivent être datées au moment de la signature et les signatures électroniques doivent inclure l'horodatage de la signature afin d'enregistrer la concomitance de l'exécution de la signature.
- L'utilisation de systèmes hybrides est déconseillée, mais lorsque des systèmes anciens sont en attente de remplacement, des contrôles de limitation des risques doivent être mis en place. L'utilisation d'identifiants de connexion partagés et génériques doit être évitée afin de garantir que les actions documentées dans les enregistrements électroniques sont attribuable à un individu unique. Cela s'applique tant au niveau de l'application logicielle qu'à l'ensemble des environnements réseau où le personnel peut effectuer des actions (par exemple le système d'exploitation du poste de travail ou du serveur). Là où de tels contrôles techniques ne sont pas disponibles ou réalisables, par exemple, dans des systèmes électroniques anciens où une déconnexion fermerait une application ou arrêterait le processus en cours, une combinaison d'enregistrements papier et électroniques doit être utilisée pour répondre aux exigences d'attribution des actions aux individus concernés. Dans de tels cas, les enregistrements originaux générés au cours des activités BPx doivent être complets et doivent être maintenus tout au long de la période de conservation des enregistrements

d'une manière qui permet la reconstruction complète des activités BPx.

- Tant qu'un niveau adéquat de sécurité peut être maintenu, une approche hybride peut être utilisée de manière exceptionnelle pour signer des enregistrements lorsque le système ne dispose pas de fonctionnalité de signature électronique. L'approche hybride est probablement plus fastidieuse qu'une approche entièrement électronique ; c'est pourquoi l'utilisation de signatures électroniques est recommandée chaque fois que cela est possible. Par exemple, la signature manuscrite d'un enregistrement électronique peut être réalisée par le biais d'un moyen simple qui créerait un formulaire contrôlé d'une page associé aux procédures écrites régissant l'utilisation du système et la revue des données. Le document doit lister les jeux de données électroniques revus ainsi que toutes les métadonnées sujettes à la revue et il doit fournir des champs afin que l'auteur, le relecteur et/ou l'approbateur du jeu de données puissent insérer leur signature manuscrite. Cet enregistrement papier avec les signatures manuscrites doit alors être lié de manière sûre et traçable au jeu de données électroniques, soit au moyen de procédure, tel que l'utilisation d'index d'archives détaillés, ou par des moyens techniques, tels que l'intégration d'une copie conforme d'une image scannée de la page de signature dans le jeu de données électroniques.
- Le remplacement des systèmes hybrides doit être une priorité.
- L'utilisation d'un transcripteur pour enregistrer une activité pour le compte d'un autre opérateur doit uniquement être considéré à titre exceptionnel et doit uniquement avoir lieu lorsque :
  - l'action d'enregistrement met en péril le produit ou l'activité, par exemple : documentation des interventions sur ligne des opérateurs de la zone aseptique ;
  - pour s'adapter aux différences culturelles ou pour atténuer les limitations d'alphabétisation / de langues de l'équipe, par exemple, lorsque l'activité est accomplie par un opérateur, mais constatée et enregistrée par un superviseur ou un agent.
- Dans les deux cas, l'enregistrement par le superviseur doit être généré concomitamment à la tâche effectuée et il doit identifier aussi bien la personne effectuant la tâche observée que la personne générant l'enregistrement. Dans la mesure du possible, la personne effectuant la tâche observée doit contresigner l'enregistrement, même s'il est accepté que cette étape de contresignature soit rétrospective. Le processus de génération de la documentation par un superviseur (transcripteur) doit être décrit dans une procédure approuvée qui doit également spécifier les activités auxquelles le processus s'applique.

Lisible, traçable et permanent

Les termes lisible, traçable et permanent se réfèrent aux exigences que les données soient lisibles, compréhensibles et permettent une vision claire du déroulement des étapes ou des évènements documentés dans l'enregistrement de manière à ce que toutes les activités BPx réalisées puissent être reconstruites intégralement par les personnes examinant ces enregistrements à n'importe quel moment de la période de conservation des enregistrements, fixées par les BPx applicables.

Exigences pour les enregistrements papier	**Exigences pour les enregistrements électroniques**
Les contrôles assurant que les enregistrements papier sont lisibles, traçables et permanents incluent mais ne sont pas limités à : • l'utilisation d'une encre indélébile, permanente ; • la non-utilisation de crayon de papier ou de gomme ; • rayer d'une ligne simple les enregistrements nécessitant modification, avec la mention du nom, de la date et du motif (c'est-à-dire l'équivalent papier de l'audit-trail) ; • la non-utilisation de liquide correcteur opaque ou de toute occultation de l'enregistrement ; • l'émission contrôlée de cahiers reliés, paginés avec des pages numérotées consécutivement (c'est-à-dire qui permettent la détection de page manquante ou sautée) ; • l'émission contrôlée de copies numérotées consécutivement de formulaires vierges (c'est-à-dire qui permettent de comptabiliser tous les formulaires émis) ; • l'archivage des enregistrements papier dans des archives papier sécurisées et contrôlées par un personnel indépendant désigné (archiviste est le terme utilisé pour ces personnels dans le cadre du contrôle qualité, des bonnes pratiques de laboratoire (BPL) et des bonnes pratiques	Les contrôles assurant que les enregistrements papier sont lisibles, traçables et permanents incluent mais ne sont pas limités à : • la conception et la configuration de systèmes informatisés et l'écriture des procédures opérationnelles standards (SOPs) requises, qui imposent l'enregistrement des données électroniques concomitamment à l'activité et avant de procéder à la prochaine étape de la séquence d'évènement (par exemple des contrôles qui interdisent la génération, le traitement et la suppression de données dans une mémoire temporaire et qui, au lieu de cela, imposent l'enregistrement des données dans une mémoire durable concomitamment à l'activité et avant de passer à la prochaine étape de la séquence) ; • l'utilisation d'audit-trails sécurisés horodatés qui enregistrent de manière indépendante les actions de l'opérateur et qui attribuent les actions à l'individu connecté ; • un paramétrage de la configuration qui limite l'accès aux droits d'accès avancés (tels que le profil d'administrateur système qui peut être utilisé pour potentiellement désactiver les audit-trails et permettre l'écrasement ou la suppression de données), uniquement

cliniques (BPC)). – Dans le cadres des bonnes pratiques de fabrication (BPF), ce rôle est habituellement attribué spécifiquement à un ou plusieurs individus au sein de l'unité d'assurance qualité ; – la préservation de papier/d'encre qui s'estompe au cours du temps lorsque leur utilisation est inévitable.	aux personnes indépendantes de celles qui sont responsables du contenu des enregistrements électroniques ; • un paramétrage de la configuration et les SOPs comme requis, pour bloquer et interdire la capacité d'écraser des données, y compris l'interdiction de l'écrasement de données préliminaires et intermédiaires ; • un paramétrage de la configuration strictement contrôlé et l'utilisation d'outils d'annotation de données d'une manière qui prévient que des données soient masquées dans les affichages et les impressions ; • la sauvegarde validée des enregistrements électroniques pour assurer le plan de reprise d'activité ; l'archivage validé des enregistrements électroniques dans des archives électroniques sécurisées et contrôlées par un ou plusieurs archivistes indépendants désignés.

Indications relatives à la gestion du risque pour assurer l'enregistrement lisible, traçable et permanent de données BPx

- Lorsque des systèmes informatisés sont utilisés pour générer des données électroniques, il doit être possible d'associer toutes les modifications des données aux personnes qui effectuent ces modifications ; ces modifications doivent être horodatées et, le cas échéant, la raison de la modification doit être enregistrée. La traçabilité des actions des utilisateurs doit être documentée au moyen d'audit-trails générés par le système informatisé ou dans d'autres champs de métadonnées ou au moyen de fonctionnalités du système qui répondent à ces exigences.

- Les utilisateurs ne doivent pas être capables de modifier ou de désactiver les audit-trails ou les autres moyens permettant de fournir la traçabilité des actions des utilisateurs.

- La nécessité d'implémenter des fonctionnalités d'audit-trail appropriées doit être envisagée pour tous les nouveaux systèmes informatisés. Lorsqu'un système informatisé existant ne dispose pas d'audit-trails générés par le système, le personnel peut utiliser, dans le cadre de contrôles procéduraux, des moyens alternatifs tels que

des cahiers de route (logbooks), le contrôle de changement, le contrôle des versions des enregistrements ou d'autres combinaisons d'enregistrements papier et électroniques pour satisfaire aux exigences réglementaires BPx relatives à la traçabilité afin de documenter le quoi, qui, quand et pourquoi d'une action. Les contrôles procéduraux devraient inclure des procédures écrites, des programmes de formation, des revues d'enregistrements, d'audits et des auto-inspections des processus de gouvernance.

- Lorsque des enregistrements électroniques sont archivés, le processus d'archivage doit être exécuté d'une manière contrôlée afin de préserver l'intégrité des enregistrements. Les archives électroniques doivent être validées, sécurisées et conservées dans un état maîtrisé tout au long du cycle de vie des données. Les enregistrements électroniques archivés manuellement ou automatiquement doivent être enregistrés dans des archives sécurisées et contrôlées, accessibles uniquement par des archivistes indépendants désignés ou par leurs délégués approuvés.

- Une séparation appropriée des fonctions doit être établie de manière à ce que les détenteurs de processus métier ou d'autres utilisateurs qui pourraient avoir un conflit d'intérêt, ne puissent pas disposer de droits d'accès étendus à quelque niveau du système que ce soit (par exemple : système d'exploitation, application, base de données). En outre, les comptes d'administrateurs système avec les droits d'accès élevés doivent être réservés aux personnels techniques désignés, par exemple les personnels du service informatique, qui sont complètement indépendants du personnel responsable du contenu des enregistrements, puisque ces types de comptes utilisateur peuvent inclure la capacité de changer les paramètres pour écraser, renommer, supprimer, déplacer des données, changer les paramètres d'heure et de date, de désactiver les audit-trails et d'effectuer d'autres actions de maintenance du système qui désactivent les contrôles relatifs aux bonnes pratiques de gestion des données et des enregistrements (BPGDE) assurant la lisibilité et la traçabilité des données électroniques. Lorsqu'il n'est pas possible d'assurer l'indépendance de ces rôles de sécurité, d'autres stratégies de contrôle devraient être utilisées pour réduire les risques relatifs à la validité des données.

Pour éviter les conflits d'intérêts, ces permissions d'accès étendu au système doivent uniquement être octroyées à un personnel ayant des rôles concernant la maintenance du système (par exemple : l'informatique, la métrologie, le contrôle des enregistrements, l'ingénierie), qui sont complètement indépendants du personnel responsable du contenu des enregistrements (par exemple les analystes de laboratoire, la direction du laboratoire, les investigateurs cliniques, les directeurs d'étude, les opérateurs de production et la direction de la production). Lorsqu'il n'est pas possible d'assurer l'indépendance de ces rôles de sécurité, d'autres stratégies de contrôle devraient être utilisées pour réduire les risques relatifs à la validité des données.

Il est crucial que les individus avec des droits d'accès étendus comprennent bien l'impact de tout changement qu'ils réalisent en utilisant ces privilèges. Les personnels disposant de droits d'accès étendus devraient ainsi être formés aux principes d'intégrité des données.

Concomitant (enregistré sur le moment)

Les données enregistrées sur le moment (concomitamment) sont des données enregistrées au moment où elles sont générées ou observées.

Exigences pour les enregistrements papier	**Exigences pour les enregistrements électroniques**
L'enregistrement concomitant des actions dans des documents papier doit avoir lieu, selon le cas, par le biais : • de procédures écrites, de contrôles réalisés dans le cadre de formations, de revues, d'audits et d'auto-inspections, qui assurent que le personnel enregistre les données et les informations directement dans des documents contrôlés officiellement (par exemple : les cahiers de laboratoire, les dossiers de lot, les formulaires de rapport) concomitamment à l'activité ; • de procédures requérant que les activités soient enregistrées dans des documents papier avec la date de l'activité (ainsi que l'heure, si l'activité a une contrainte temporelle) ; • d'une bonne conception documentaire, qui encourage les bonnes pratiques : les documents doivent être conçus de manière appropriée et la disponibilité des formulaires / documents vierges dans lesquels les activités sont enregistrés doit être assurée ; • de l'enregistrement de la date et de l'heure des activités en utilisant des sources de temps synchronisées (pendules dans les locaux, horloge des systèmes informatisé) qui ne peuvent pas être modifiées par un personnel non-autorisé. Lorsque cela est possible, l'enregistrement de la date et de l'heure des activités manuelles (par exemple les pesées) devrait être fait automatiquement.	L'enregistrement concomitant des actions dans des documents électroniques doit avoir lieu, selon le cas, par le biais : • du paramétrage de la configuration, de SOPs et de contrôles qui imposent que les données enregistrées dans une mémoire temporaire soient enregistrées durablement à l'achèvement d'une étape ou d'un événement et avant de procéder à la prochaine étape de la séquence d'évènement ; • de l'horodatage fiable par le système qui ne peut être modifié par le personnel ; • de procédures et de programmes de maintenance qui garantissent que les horodatages sont synchronisés tout au long des opérations BPx ; • de contrôles qui permettent de déterminer l'ordre des activités les unes par rapport aux autres (par exemple : gestion des fuseaux horaires) ; • de la disponibilité du système pour l'utilisateur au moment de l'activité.

Indications relatives à la gestion du risque pour assurer la concomitance des enregistrements de données BPx

Les programmes de formation aux BPDoc (bonnes pratiques documentaires) doivent souligner qu'il est inacceptable d'enregistrer initialement des données dans des documents informels (non officiels) (par exemple sur un morceau de papier) et de transférer ultérieurement les données dans un document officiel (par exemple le cahier de laboratoire). Au lieu de cela, la donnée originale doit être enregistrée directement dans des documents formels, tels que des formulaires de travail analytiques approuvés, immédiatement au moment de l'activité BPx.

Les programmes de formation doivent souligner qu'il est inacceptable d'antidater ou de prédater un enregistrement. Au lieu de cela, la date enregistrée doit être la date réelle de la saisie de la donnée. Des saisies tardives doivent être indiquées comme telles avec à la fois la date de l'activité et la date de la saisie. Si une personne fait une erreur sur un document papier, elle doit procéder à des corrections en rayant d'un seul trait, en signant et datant, en mentionnant les raisons de la modification et en conservant cet enregistrement avec l'ensemble des enregistrements.

Si les utilisateurs de systèmes informatisés autonomes bénéficient de la totalité des droits d'accès de l'administrateur au niveau du système d'exploitation du poste de travail, sur lesquels les enregistrements électroniques originaux sont stockés, cela pourrait, de manière inopportune, de permettre aux utilisateurs de renommer, copier ou supprimer les fichiers stockés localement sur le système et de modifier l'horodatage. Pour cette raison, la validation des informatisé autonomes doit assurer la mise en œuvre de véritables restrictions des accès afin de protéger la configuration de l'heure et de la date de manière à garantir l'intégrité des données dans la totalité de l'environnements informatique, incluant le système d'exploitation du poste de travail, l'application et, le cas échéant, tout autre environnement réseau.

Original

Les données originales incluent la saisie initiale ou la capture initiale des données ou de l'information et toutes les données résultantes (subséquentes) requises pour une reconstitution intégrale du déroulement des activités BPx. Les exigences BPx concernant les données originales incluent les points suivants :

- les données originales doivent être revues ;
- les données originales et/ou les copies authentiques ou certifiées qui préservent le contenu et la signification des données originales doivent être conservées ;
- en tant que tel, les enregistrements originaux doivent être complets, durables et aisément récupérables ainsi que lisibles tout au long de la période de conservation des enregistrements.

Des exemples de données originales incluent des données électroniques originales et des métadonnées dans les systèmes informatisées autonomes des instruments de laboratoire (par exemple la spectrophotométrie ultraviolette/visible (UV/Vis), la spectroscopie infrarouge à transformée de Fourier (FT-IR), électrocardiogramme (ECG), la chromatographie liquide couplée à la spectrométrie de masse (LC/MS/MS), les analyseurs d'hématologie et de chimie), les données électroniques originales et les métadonnées des systèmes automatisés de production (par exemple : les testeurs automatisés d'intégrité de filtre, les systèmes de contrôle, de surveillance et d'acquisitions de données (SCADA), les systèmes de contrôle-commande (SNCC)), les données électroniques originales et les métadonnées dans des systèmes de bases de données en réseaux (par exemple : système de gestion de l'information de laboratoire (LIMS), les progiciels de gestion intégré (ERP), les systèmes de gestion des processus industriels (MES), les formulaires électroniques de rapport de cas / les captures électroniques de données (eCRF/EDC), les bases de données de toxicologie, et les bases de données des écarts ainsi que des actions correctives et préventives (CAPA)), les informations manuscrites de préparation des échantillons enregistrées dans des cahiers papier, les tickets de pesée imprimés, les archives médicales électroniques et les dossiers de lot papier.

Revue des enregistrements originaux

Exigences pour les enregistrements papier	**Exigences pour les enregistrements électroniques**
Des contrôles pour la revue des enregistrements papier originaux incluent, mais ne sont pas limités : • aux procédures écrites, aux contrôles réalisés dans le cadre de formations, de revues, d'audits et d'auto-inspections, qui assurent que le personnel conduit une	Des contrôles pour la revue des enregistrements électroniques originaux incluent, mais ne sont pas limités : • aux procédures écrites, aux contrôles réalisés dans le cadre de formations, de revues, d'audits et d'inspections, qui assurent que le personnel conduit une revue adéquate des enregistrements

revue adéquate des enregistrements papier originaux et les approuve, y compris ceux ayant servi à l'enregistrement concomitant de l'information ; • aux procédures de revue des données décrivant la revue des métadonnées pertinentes. Par exemple : les procédures écrites de revue devraient requérir que le personnel évalue les modifications apportées aux informations originales sur des enregistrements papier (telles que les modifications documentées en rayant ou en corrigeant des données) pour garantir que ces modifications sont documentées de manière appropriée, justifiées au moyen de preuve probante et, le cas échéant, examinées ; • à la documentation de la revue des données. Pour les enregistrements papier, cela signifie généralement que les documents papier, qui ont été revus, sont signés. Lorsque l'approbation des enregistrements fait l'objet d'un processus séparé, cette approbation devrait également être signée. Les procédures écrites de revue des données doivent clarifier la signification de la revue et des signatures d'approbation afin de s'assurer que les personnes concernées comprennent leur responsabilité en tant que réviseurs et approbateurs pour garantir l'intégrité, l'exactitude, la et cohérence des enregistrements papier sujets à la revue et à l'approbation ainsi que leur conformité avec les règles établies ; • à une procédure décrivant les mesures à prendre si la revue des données identifie une erreur ou une omission. Cette procédure devrait permettre la correction des données ou les clarifications nécessaires d'une manière conforme aux BPx, en assurant la lisibilité de	électroniques originaux et les approuve, y compris les enregistrements initiaux lisibles des enregistrements électroniques ; • aux procédures de revue des données décrivant la revue des données électroniques originales et des métadonnées pertinentes. Par exemple : les procédures écrites de revue devraient requérir que le personnel évalue les modifications apportées aux informations originales dans les enregistrements électroniques (telles que les modifications documentées dans les audit-trails, ou les champs d'historiques ou tout autre métadonnée pertinente) pour garantir que ces modifications sont documentées de manière appropriée, justifiées au moyen de preuve probante et, le cas échéant, examinées ; • à la documentation de la revue des données. Pour les enregistrements électroniques, cela signifie généralement que les enregistrements électroniques, qui ont été revus, sont signés électroniquement. Les procédures écrites de revue des données doivent clarifier la signification de la revue et des signatures d'approbation afin de s'assurer que les personnes concernées comprennent leur responsabilité en tant que réviseurs et approbateurs pour garantir l'intégrité, l'exactitude, la et cohérence des enregistrements électroniques sujets à la revue et à l'approbation ainsi que leur conformité avec les règles établies ; • à une procédure décrivant les mesures à prendre si la revue des données identifie une erreur ou une omission. Cette procédure devrait permettre la correction des données ou les clarifications nécessaires d'une manière conforme aux BPx, en assurant la lisibilité de l'enregistrement original et la traçabilité

l'enregistrement original et la traçabilité de la correction de manière documentée, en utilisant les principes ALCOA.	de la correction au moyen d'un audit-trail, en utilisant les principes ALCOA.

Indications relatives à la gestion du risque pour la revue des enregistrements originaux

Les risques relatifs à l'intégrité des données peuvent survenir lorsque les personnes choisissent de se fier uniquement aux impressions papier ou aux rapports PDF issus de systèmes informatisés sans répondre aux attentes réglementaires applicables pour les enregistrements originaux. Les enregistrements originaux devraient être revus – cela inclut les enregistrements électroniques. Si le réviseur revoit uniquement le sous-ensemble de données fourni en tant qu'impression ou PDF, les risques peuvent passer inaperçus et des dommages peuvent survenir.

Bien que les enregistrements originaux doivent être revus, et que tous les personnels impliqués sont pleinement responsables de l'intégrité et de la fiabilité des décisions ultérieures prises sur la base des enregistrements originaux, une revue basée sur le risque du contenu des enregistrements originaux est recommandée.

Les systèmes incluent typiquement de nombreux champs de métadonnées ainsi que les audit-trails. Il est attendu que, lors de la validation du système – sur la base d'une évaluation du risque documentée et justifiée – l'organisation définisse la fréquence, les rôles et les responsabilités ainsi que l'approche devant être suivie pour revoir les différents type de métadonnées pertinentes telles que les audit-trails. Par exemple : sous certaines conditions, une organisation peut justifier de la revue périodique des audit-trails qui tracent les activités de maintenance du système, tandis que les audit-trails qui tracent les modifications des données BPx critiques, ayant un impact direct sur la sécurité du patient ou la qualité du produit, seront examinées lorsque le jeu de données associé est revu et approuvé – et avant chaque prise de décision. Certains aspects concernant la définition du processus de revue des audit-trails (par exemple la fréquence de revue) peuvent être formalisés pendant la validation et ensuite ajustés au cours du cycle de vie du système, sur la base des revues du risque et afin d'assurer une amélioration continue.

Une approche de revue des données basée sur le risque nécessite une compréhension du processus et une connaissance des risques-clés relatifs à la qualité dans le processus donné qui peut avoir un impact sur les patients, les produits, la conformité ainsi que sur l'exactitude, la cohérence et la fiabilité générales des prises de décision BPx. Lorsque les enregistrements originaux sont électroniques, une approche basée sur le risque de la revue des données électroniques originales requière de comprendre le système informatisé, les données et les métadonnées et les flux de données.

Lors de la définition d'une approche, basée sur le risque, de revue des audit-trails de systèmes informatisés BPx, il est important de noter que certains développeurs de logiciels peuvent concevoir des mécanismes pour tracer les actions des utilisateurs relatives aux données BPx les plus critiques en utilisant des fonctionnalités de métadonnées, bien que celles-ci ne soient peut-être pas dénommées « audit-trail », et en revanche ces développeurs peuvent utiliser le terme « audit-trail » pour documenter d'autres activités de maintenance de l'ordinateur ou des fichiers. Par exemple, des modifications de données scientifiques peuvent parfois être plus facilement visualisées en effectuant diverses requêtes dans les bases de données ou en visualisant des champs de métadonnées marqués comme « fichiers d'historique » ou par la revue de rapports du système définis et validés, tandis que les fichiers désignés par le développeur de logiciel comme étant des audit-trails peuvent être d'une valeur limitée pour une revue effective. La revue basée sur le risque des données électroniques et des métadonnées, telles que les audit-trails, nécessite une compréhension du système et du processus scientifique gouvernant le cycle de vie des données, de manière à ce que les métadonnées pertinentes soient sujettes à la revue, indépendamment des conventions de nommage utilisées par le développeur du logiciel.

Les systèmes peuvent être conçus pour faciliter la revue des audit-trails par différents moyens ; par exemple : la conception du système peut permettre de revoir les audit-trails sous la forme d'une liste de données pertinentes ou par un processus validé de rapport d'exception.

Des procédures écrites pour la revue des données doivent définir la fréquence, les rôles et les responsabilités et l'approche de la revue des métadonnées significatives, comme les audit-trails. Ces procédures doivent également décrire la manière dont des données aberrantes doivent être traitées si elles sont trouvées au cours d'une revue. Le personnel qui conduit de telles revues doit avoir une formation adéquate et appropriée dans le processus de revue aussi bien que dans les systèmes logiciels contenant le sujet des données à réviser. L'organisation doit prendre les dispositions nécessaires pour que le personnel révisant les données puisse accéder au système (aux systèmes) contenant les données électroniques et les métadonnées.

L'assurance de la qualité doit également réviser un échantillon des audit-trails pertinents, de données brutes et de métadonnées en tant que partie de l'auto-inspection pour assurer la conformité continue avec la politique de gouvernance des données et des procédures.

Toute variation significative des résultats prévus doit être enregistrée complètement et examinée.

Dans l'approche hybride, qui n'est pas l'approche privilégiée, des impressions papier des enregistrements électroniques originaux des systèmes informatisés peuvent être utiles en tant que rapports sommaire si les exigences pour les enregistrements électroniques originaux sont également respectées. Pour se fier à ces sommaires de résultats imprimés pour des prises de décision futures, une deuxième personne doit réviser les données électroniques originales et toute métadonnée pertinente telles que les audit-trails, pour vérifier que le sommaire imprimé est représentatif de tous les résultats. Cette vérification sera alors documentée et l'impression pourrait être utilisée pour la prise de décision ultérieure.

L'organisation BPx peut choisir une approche complètement électronique pour permettre une revue simplifiée des enregistrements, plus efficace et la conservation des enregistrements. Cela exigerait que des signatures électroniques authentifiées et sécurisées soient implémentées pour la signature des enregistrements le cas échéant. Cela, en retour, nécessiterait la préservation des enregistrements électroniques originaux, ou une copie certifiée, ainsi que le logiciel et le matériel nécessaire ou d'autres équipements de lecture adaptés pour voir les enregistrements pendant la période de conservation des enregistrements.

La conception du système et la manière de capturer les données peuvent influencer significativement la facilité avec laquelle la cohérence des données peut être assurée. Par exemple, et le cas échéant, l'utilisation de vérifications des modifications programmées ou des caractéristiques telles que les menus déroulants, les cases à cocher ou la ramification des questions ou des champs de données basées sur les entrées, sont utiles dans l'amélioration de la cohérence des données.

Les données et leurs métadonnées doivent être conservées de telle manière qu'elles soient disponibles pour la revue par des individus autorisés, et dans un format qui est adapté à la revue aussi longtemps que les exigences de conservation des données s'appliquent. Il est souhaitable que les données soient conservées et disponibles dans le système original dans lequel elles ont été générées pendant la période de temps la plus longue possible. Lorsque le système original est retiré ou désactivé, la migration des données vers d'autres systèmes ou d'autres moyens de préserver les données doivent être utilisés de manière à préserver le contexte et la signification des données, permettant aux étapes pertinentes d'être reconstruites. Les contrôles de l'accessibilité des données archivées, indépendamment de leur format, et incluant les métadonnées pertinentes, doivent être entrepris pour confirmer que les données soient durables et continuent d'être disponibles, lisibles et compréhensibles par un être humain.

Conservation des enregistrements originaux ou des copies conformes

Exigences pour les enregistrements papier	**Exigences pour les enregistrements électroniques**
Les contrôles pour la conservation des enregistrements papier originaux et des copies conformes des enregistrements papier originaux incluent, mais ne sont pas limités : • aux lieux de stockage contrôlés et sécurisés, incluant les archives, pour les enregistrements papier ; • à un archiviste (à des archivistes) papier désigné(s) qui est(sont) indépendant(s)	Les contrôles pour la conservation des enregistrements électroniques originaux et des copies conformes des enregistrements électroniques originaux incluent, mais ne sont pas limités : • à des copies de sauvegarde de routine des enregistrements électroniques originaux stockés à un autre emplacement les protégeant en cas d'un désastre qui causerait la perte des

des opérations BPx est requis par les directives BPL ; pour les autres BPx, les rôles et les responsabilités pour archiver les enregistrements BPx doivent être définis et surveillés (et devraient normalement être sous la responsabilité de la fonction assurance qualité ou d'une unité indépendante de contrôle de la documentation) ; • à l'indexation des enregistrements pour permettre leur récupération rapide ; • à des tests périodiques, à des intervalles appropriés basés sur l'évaluation du risque, pour vérifier la capacité de récupération des enregistrements papier ou sous un format statique archivés ; • à la disponibilité, le cas échéant, d'équipement de lecture adapté, tels que des lecteurs de microfiches ou de microfilms si l'archivage des enregistrements papier originaux est réalisé au moyen de copies conformes sur des microfilms ou des microfiches ; • aux procédures écrites, aux formations, aux revues et audits et aux auto-inspections des processus définissant, selon les besoins, la conversion d'un enregistrement papier original en une copie conforme et qui devraient inclure les étapes suivantes : – réalisation d'une copie / de copies de l'enregistrement(s) papier original, en préservant le format d'enregistrement original, le format statique, comme requis (par exemple photocopie, scan), – comparaison de la copie / des copies avec l'enregistrement original (les enregistrements originaux) pour déterminer si la copie préserve l'intégralité du contenu et la signification de l'enregistrement original, que les métadonnées sont inclues, et qu'aucune donnée ne	enregistrements électroniques originaux ; • aux zones de stockage contrôlées et sécurisées, y compris les archives, des enregistrements électroniques ; • à un (des) archiviste(s) électronique(s) désigné(s) tel que requis dans les directives BPL et qui est (sont) indépendant(s) des opérations BPx (le personnel désigné devrait être dûment qualifié et avoir une expérience pertinente et une formation appropriée pour mener à bien ses tâches) ; • à l'indexation des enregistrements pour permettre leur récupération rapide ; • à des tests périodiques afin de vérifier la capacité à récupérer les données électroniques depuis les lieux de stockage. La capacité à récupérer des données électroniques archivées à partir des emplacements de stockage devrait être testée au cours de la validation de l'archive électronique. Après la validation, la capacité à récupérer les données électroniques archivées à partir des emplacements de stockage devrait être reconfirmée périodiquement, y compris pour la récupération depuis un stockage tiers ; • à la disponibilité, le cas échéant, d'équipement de lecture adapté, tel que les logiciels, le système d'exploitation et des environnements virtualisés, pour la consultation des données électroniques archivées lorsque cela est nécessaire ; • aux procédures écrites, aux formations, aux revues et audits et aux auto-inspections des processus définissant, selon les besoins, la conversion d'enregistrements électroniques originaux en une copie conforme et qui devraient inclure les étapes suivantes : – réalisation d'une copie / de copies du jeu de données électroniques original, en préservant le format

manque dans la copie. La manière dont le format de l'enregistrement est préservé est importante pour la signification de l'enregistrement si la copie doit répondre aux exigences d'une copie conforme de l'enregistrement papier original (des enregistrements papier originaux), – documentation de la vérification par le vérificateur au moyen d'un lien sûr attestant que la (les) copie(s) est une copie conforme ou au moyen d'un certificat.	d'enregistrement original, le format dynamique, comme requis (par exemple la copie d'archivage du jeu complet des données électroniques et des métadonnées faites en utilisant un processus de sauvegarde validé), – comparaison par une deuxième personne vérificatrice ou au moyen d'un processus de vérification technique (tel que l'utilisation de sommes de contrôle (hash)) confirmant le succès de la sauvegarde au cours de laquelle une comparaison de la copie d'archivage avec le jeu de données électroniques originales pour confirmer que la copie préserve l'intégralité du contenu et la signification de l'enregistrement original (c'est-à-dire que toutes les données et toutes les métadonnées sont incluses, qu'aucune donnée ne manque dans la copie, que tout format d'enregistrement dynamique qui est important pour la signification et l'interprétation de l'enregistrement est préservé et que le fichier n'a pas été corrompu pendant l'exécution du processus de sauvegarde validé), – documentation de la vérification par le vérificateur ou par le processus technique au moyen d'un lien sûr attestant que la (les) copie(s) est une copie conforme.

Indications relatives à la gestion du risque pour la conservation des enregistrements originaux et/ou des copies conformes

Les dispositions concernant la conservation des données et des documents devraient garantir la protection des enregistrements d'une modification délibérée ou involontaire ou de leur perte. Les contrôles sécurisés devraient être en place pour garantir l'intégrité des données de

l'enregistrement tout au long de la période de conservation. Le cas échéant, les processus d'archivage devraient être définis dans des procédures écrites et validées.

Les données collectées ou enregistrées (manuellement et/ou par des dispositifs d'enregistrement ou des systèmes informatisés) pendant un processus ou une procédure devraient montrer que toutes les étapes définies et requises ont été effectuées et que le rendement en termes de quantité et de qualité est tel qu'attendu. Les données collectées devraient permettre une traçabilité complète de l'historique du processus ou des matières et elles devraient être conservées d'une manière compréhensible et accessible. C'est-à-dire que les enregistrements originaux et/ou les copies conformes devraient être complètes, cohérentes et durables.

Une copie conforme des enregistrements originaux peut seulement être conservée à la place des enregistrements originaux si la copie a été comparée aux enregistrements originaux et s'il a été vérifié qu'elle contenait l'intégralité du contenu et de la signification des enregistrements originaux, y compris les métadonnées et les audit-trails concernés.

Si des copies conformes des enregistrements papier originaux sont faites en scannant le papier original et en le convertissant en une image électronique, telle qu'un PDF, alors des mesures additionnelles pour protéger l'image électronique contre des altérations supplémentaires sont requises (par exemple : le stockage dans un emplacement réseau protégé avec un accès limité uniquement au personnel d'archivage électronique, ainsi que des mesures pour contrôler l'utilisation potentielle d'outils d'annotation ou d'autres moyens de prévention d'une altération ultérieure de la copie).

Il faut prendre en considération la conservation, le cas échéant, de l'intégralité du contenu et de la signification des enregistrements papier originaux signés à la main, en particulier lorsque la signature manuscrite représente un aspect important et général de l'intégrité et de la fiabilité de l'enregistrement et en accord avec la valeur du enregistrement au cours du temps. Par exemple, dans un essai clinique, il peut être important de préserver les formulaires originaux de consentement renseignés et signés à la main tout au long de la durée de vie de cet enregistrement en tant qu'aspect essentiel de l'essai et de l'intégrité du dossier de demande concerné.

Les copies conformes d'enregistrements électroniques devraient préserver le format dynamique des données électroniques originales car il est essentiel de préserver la signification des données électroniques originales, par exemple lorsque l'ancien logiciel ou l'ancien équipement est mis hors service. Par exemple : les fichiers spectraux électroniques dynamiques originaux créés par des instruments tels que les FT-IR, les UV/Vis, les systèmes de chromatographie ou autres peuvent être réévalués tandis qu'un fichier PDF ou une impression sont fixes ou statiques et la capacité d'étendre les lignes de base, de voir le spectre complet, de réévaluer et d'interagir dynamiquement avec le jeu de données est perdue avec le PDF ou l'impression. Un autre exemple concerne la préservation du format dynamique des données d'études cliniques collectées dans un système eCRF qui permet la recherche et l'interrogation des données, tandis qu'un fichier PDF des données eCRF, même s'il inclut un fichier PDF contenant les audit-

trails, perdrait cet aspect du contenu et de la signification des données eCRF originales. Les investigateurs cliniques doivent avoir accès aux enregistrements originaux au cours de l'étude et tout au long de la période de conservation des enregistrements d'une manière qui préserve l'intégralité du contenu et de la signification de l'information initiale. Il peut être décidé de maintenir des copies complètes des données électroniques ainsi que des sommaires PDF / imprimés de ces données électroniques dans les archives afin de limiter les risques d'une perte de capacité totale à facilement consulter les données si le logiciel et le matériel devaient être mis hors service. Cependant, dans ces circonstances, en particulier pour les données qui soutiennent des prises de décision critique, même si des sommaires PDF / imprimés sont conservés, les copies complètes des données électroniques devraient continuer à être conservées tout au long de la période de conservation des enregistrements afin de permettre des enquêtes qui pourraient être nécessaires dans des circonstances inattendues, telles que des enquêtes concernant l'intégrité des dossiers de demande.

La préservation des données électroniques originales sous format électronique est aussi importante car les données dans des formats dynamiques simplifient l'utilisation de ces données dans des processus ultérieurs. Par exemple, la conservation électronique des données d'un enregistreur de température simplifie le suivi, la tendance et la surveillance des températures dans des graphiques servant à la maîtrise statistique des procédés.

En plus de l'option de créer des copies conformes des données électroniques originales en tant que copies de sauvegarde vérifiées qui sont alors sécurisées dans des archives électroniques, une autre option pour la création d'une copie conforme de données électroniques originales serait de migrer les données électroniques originales d'un système à un autre et de vérifier et de documenter que le processus validé de migration des données préserve l'intégralité du contenu, incluant toutes les métadonnées significatives, ainsi que la signification des données électroniques originales.

Les informations relatives aux signatures électroniques doivent être conservées comme partie intégrante de l'enregistrement électronique original. Elles devraient rester liées à l'enregistrement et être lisibles tout au long de la période de conservation, indépendamment du système utilisé pour l'archivage des enregistrements.

Exactitude

Le terme « exact » signifie que les données sont correctes, véridiques, complètes, valides et fiables.

Aussi bien pour les enregistrements papier que pour les enregistrements électroniques, l'obtention de données exactes nécessite l'adéquation des procédures, des processus, des systèmes et des contrôles qui constituent le système de gestion de la qualité. Le système de gestion de la qualité doit être approprié à l'étendue de ses activités et basé sur le risque.

Les contrôles qui garantissent l'exactitude des données pour les enregistrements papier et les enregistrements électroniques incluent, mais ne se limitent pas :

- à la qualification, l'étalonnage et la maintenance des équipements, tels que les balances et les pH-mètres, qui génèrent des impressions ;
- à la validation des systèmes informatisés qui génèrent, traitent, conservent, distribuent ou archivent des données électroniques ;
  - les systèmes doivent être validés pour garantir leur intégrité pendant la transmission entre les / au sein des systèmes informatisés ;
- la validation des méthodes analytiques ;
- la validation des processus de production ;
- la revue des enregistrements BPx ;
- l'examen des écarts et des résultats douteux et des résultats non-conformes (OOS) ; et
- bien d'autres contrôles de gestion du risque dans le cadre du système de gestion de la qualité.
-

Des exemples de ces contrôles appliqués au cycle de vie des données sont fournis ci-dessous.

Indications relatives à la gestion du risque pour assurer des enregistrements BPx exacts

- La saisie de données critiques dans un ordinateur par une personne autorisée (par exemple : la saisie d'une formule maître d'un processus) nécessite une vérification additionnelle de l'exactitude des données saisies manuellement. Cette vérification peut être faite par une vérification et une libération pour utilisation indépendantes par une deuxième personne autorisée ou par des moyens électroniques validés. Par exemple, pour détecter et gérer les risques associés aux données critiques, les procédures nécessiteraient la vérification par une deuxième personne, telle qu'un membre du personnel de l'unité qualité : des formules de calcul saisies dans des tableurs ; des données maître saisies dans un LIMS telles que les champs des gammes de spécifications utilisées pour signaler des valeurs non-conformes aux spécifications sur les certificats d'analyse ; et, le cas échéant, d'autres données maître critiques. En outre, une fois vérifiés, ces champs de données critiques devraient être verrouillés pour prévenir des modifications ultérieures, lorsque cela est faisable et approprié, et ils doivent être uniquement modifiés dans le cadre d'un processus formel de gestion des changements.
- La validité du processus de saisie des données est fondamentale pour assurer que

des données de grande qualité soient produites.

- Là où ils sont utilisés, des dictionnaires standards et des thésaurus, des tables (par exemple d'unités et d'échelles) devraient être contrôlés.
- Le processus de transfert de données entre des systèmes doit être validé.
- La migration des données dans des systèmes et l'export de données à partir de systèmes requièrent que des tests et des contrôles spécifiques soient planifiés.

Le temps peut ne pas être critique pour toutes les activités. Lorsque l'activité est critique dans le temps, les enregistrements imprimés devraient afficher l'horodatage.

Par exemple : Afin d'assurer l'exactitude des pesées d'échantillons enregistrées sur une impression papier à partir de la balance, la balance devrait être étalonnée de manière appropriée avant son utilisation et elle devrait être entretenue correctement. En outre, la synchronisation et le verrouillage du paramétrage des métadonnées de la balance pour la configuration de l'heure / de la date assurerait des enregistrements exacts de l'heure / la date sur l'impression de la balance.

Acknowledgement

The translation of this Annex has been produced with the financial assistance of the European Union.