ANNEXE 11 :

SYSTEMES INFORMATISES

Principe

Cette annexe s'applique à toutes les formes de systèmes informatisés utilisés dans le cadre d'activités relevant des BPF. Un système informatisé est un ensemble de logiciels et matériels qui remplissent ensemble certaines fonctionnalités.

L'application doit être validée et l'infrastructure informatique doit être qualifiée.

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

Généralités

1. **Gestion du risque**

La gestion du risque doit être appliquée tout au long du cycle de vie du système informatisé, en prenant en compte la sécurité des patients, l'intégrité des données et la qualité du produit. Dans le cadre d'un système de gestion du risque, les décisions relatives à l'étendue de la validation et aux contrôles d'intégrité des données doivent être basées sur une évaluation justifiée et documentée des risques liés au système informatisé.

2. **Personnel**

Il doit y avoir une coopération étroite entre l'ensemble des personnels impliqués, tels que le détenteur du processus, le détenteur du système, les personnes qualifiées et le service informatique. Tout le personnel doit avoir les qualifications appropriés, leurs niveaux d'accès et leurs responsabilités doivent être clairement définies, afin d'effectuer les tâches qui lui sont assignées.

3. **Fournisseurs et prestataires de services**

3.1. Lorsque le fabricant fait appel à un tiers (par exemple : des fournisseurs, des prestataires de services) qui interviendrait, par exemple, dans l'approvisionnement, l'installation, la configuration, l'intégration, la validation, la maintenance (par exemple via un accès à distance), la modification ou la conservation d'un système informatisé, ou tous services associés ou pour le traitement de données, un contrat formel doit être établi entre le fabricant et les tierces parties. Ces contrats doivent intégrer un énoncé clair des responsabilités de la tierce partie. Les services informatiques doivent être considérés de manière similaire.

3.2. La compétence et la fiabilité d'un fournisseur sont des facteurs essentiels à prendre en compte lors de la sélection d'un produit ou d'un prestataire de service. La nécessité d'un audit doit être basée sur une évaluation du risque.

3.3. La documentation accompagnant les produits standards du commerce doit être attentivement examinée par les utilisateurs soumis à la réglementation pharmaceutique, afin de s'assurer qu'ils satisfont aux exigences attendues.

3.4. Les informations relatives au système qualité et à l'audit des fournisseurs ou des développeurs de logiciels ainsi que les systèmes installés doivent être disponibles, à

la demande des inspecteurs.

Phase du projet

4. **Validation**

4.1. La documentation et les rapports de validation doivent couvrir les étapes pertinentes du cycle de vie. Les fabricants doivent être capables de justifier leurs standards, leurs protocoles, leurs critères d'acceptation, leurs procédures et leurs enregistrements, sur la base de leur évaluation du risque.

4.2. La documentation de validation doit inclure, le cas échéant, les enregistrements relatifs à la maîtrise des changements et les rapports de toutes les déviations observées durant le processus de validation.

4.3. Un inventaire à jour de tous les systèmes concernés et leurs fonctionnalités BPF doit être disponible.

Pour les systèmes critiques, une description à jour du système détaillant les dispositions physiques et logiques, les flux de données et les interfaces avec d'autres systèmes ou processus, les prérequis concernant les matériels et les logiciels, ainsi que les mesures de sécurité, doit être disponible.

4.4. Les spécifications utilisateurs (« User Requirements Specifications » - URS) doivent décrire les fonctions requises du système informatisé et être basées sur une évaluation documentée du risque et de l'impact BPF. Les exigences de l'utilisateur doivent être traçables tout au long du cycle de vie.

4.5. L'utilisateur soumis à la réglementation pharmaceutique doit prendre toutes les mesures raisonnables permettant de s'assurer que le système informatisé a été développé conformément à un système approprié de gestion de la qualité. Le fournisseur doit être évalué de manière adéquate.

4.6. Pour la validation de systèmes informatisés sur mesure ou personnalisés, un processus doit être mis en place afin de garantir une évaluation formelle et des retours d'information sur la qualité et les mesures de performance, et ce, pour toutes les étapes du cycle de vie du système.

4.7. L'adéquation des méthodes et des scénarii de tests doit être démontrée. En particulier, les limites des paramètres du système (processus) et des données et le traitement des erreurs, doivent être pris en considération. L'adéquation des outils automatisés et des environnements de test doit faire l'objet d'une évaluation documentée.

4.8. Si des données sont transférées dans un autre format ou vers un autre système, la validation doit intégrer des vérifications garantissant que la valeur et/ou la signification des données ne sont pas altérées durant le processus de migration.

Phase opérationnelle

5. **Données**

Les systèmes informatisés qui échangent des données électroniques avec d'autres systèmes doivent disposer de contrôles intégrés garantissant la sécurité et l'exactitude des entrées et des traitements des données et ce, afin de minimiser les risques.

6. **Contrôle d'exactitude**

Pour les données critiques introduites manuellement, il est nécessaire de prévoir un contrôle supplémentaire pour vérifier l'exactitude des données. Ce contrôle peut être effectué par

un deuxième opérateur ou par des moyens électroniques validés. La criticité et les conséquences potentielles de données erronées ou incorrectement saisies dans un système doivent être couvertes par la gestion du risque.

7. **Stockage des données**

7.1. Les données doivent être protégées d'éventuels dommages par des moyens physiques et électroniques. Les données stockées doivent être vérifiées en terme d'accessibilité, la lisibilité et l'exactitude. L'accès aux données doit être garanti tout au long de la période de conservation.

7.2. Des sauvegardes régulières des données pertinentes doivent être réalisées. L'intégrité et l'exactitude des données sauvegardées, et la capacité à restaurer les données, doivent être vérifiées pendant la validation et contrôlées périodiquement.

8. **Sorties imprimées**

8.1. Il doit être possible d'obtenir des copies imprimées claires des données stockées électroniquement.

8.2. Pour les données nécessaires à la libération des lots, Il doit être possible de générer des impressions indiquant si l'une ou plusieurs d'entre elles ont été modifiées depuis leur saisie initiale.

9. **Traçabilité des modifications**

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

10. **Maîtrise des changements et de la configuration**

Toute modification d'un système informatisé, y compris relative à sa configuration, ne peut être réalisée que de façon maîtrisée et conformément à une procédure définie.

11. **Evaluation périodique**

Les systèmes informatisés doivent périodiquement faire l'objet d'une évaluation afin de s'assurer qu'ils restent dans un état validé et conforme aux BPF. Ces évaluations doivent inclure, le cas échéant, la gamme en cours de fonctionnalités, les enregistrements des déviations, les incidents, les problèmes, l'historique des mises à jour et les rapports de performance, de fiabilité, de sécurité et de validation.

12. **Sécurité**

12.1. Des moyens physiques et/ou logiques doivent être mis en place afin de restreindre l'accès des systèmes informatisés au seul personnel autorisé. Des méthodes adéquates pour éviter des accès non autorisés au système informatisé peuvent consister en l'utilisation de clés, de badges, de codes personnels associés à des mots

de passe, de la biométrie, d'accès limités aux zones où sont situés les équipements informatiques et les stockages des données.

12.2. L'étendue des contrôles de sécurité dépend de la criticité du système informatisé.

12.3. La création, la modification et l'annulation des autorisations d'accès doivent être enregistrées.

12.4. Les systèmes de gestion des données et des documents doivent être conçus pour enregistrer l'identité des utilisateurs impliqués dans la saisie, la modification, la confirmation ou la suppression de données, y compris la date et l'heure.

13. **Gestion des incidents**

Tous les incidents, pas seulement ceux liés aux défaillances du système et aux erreurs de données, doivent être rapportés et évalués. L'origine d'un incident critique doit être identifiée et constituer la base d'actions correctives et préventives.

14. **Signature électronique**

Les enregistrements électroniques peuvent être signés électroniquement. Les signatures électroniques doivent :

a. avoir la même valeur, au sein de l'entreprise, qu'une signature manuscrite;
b. être définitivement liées aux documents auxquels elles se rapportent;
c. comprendre l'heure et la date de leur application.

15. **Libération des lots**

Lorsqu'un système informatisé est utilisé pour enregistrer la certification et la libération de lot, il doit être conçu de manière à ce que seules les personnes qualifiées puissent certifier la libération des lots, et à permettre l'enregistrement et l'identification claire de la personne libérant ou certifiant les lots. Cette opération doit être réalisée à l'aide d'une signature électronique.

16. **Continuité opérationnelle**

Pour la disponibilité des systèmes informatisés abritant des procédés critiques, des dispositions doivent être prises afin d'assurer le bon fonctionnement de ces procédés lors de panne (par exemple, un système manuel ou système alternatif). Le temps nécessaire à la mise en place de ces arrangements alternatifs doivent être basés sur une étude des risques et être appropriés à ce système particulier et à l'activité concernée. Ces arrangements alternatifs doivent être correctement documentés et testés.

17. **Archivage**

Les données peuvent être archivées. L'accessibilité, la lisibilité et l'intégrité de ces données doivent être vérifiées. Si des modifications significatives du système doivent être faites (par exemple, un changement d'équipement informatique ou de logiciel), alors la capacité à récupérer les données archivées doit être garantie et testée.

Glossaire

Application: Logiciel installé sur une plateforme/ équipement défini(e) et fournissant une fonction spécifique.

Cycle de vie: Toutes les phases de vie d'un système, de l'expression initiale des besoins jusqu'à sa mise hors service, et incluant la conception, les spécifications, la programmation, les tests, l'installation, l'exploitation et la maintenance.

Détenteur du processus: Personne responsable du processus commercial.

Détenteur du système: Personne responsable de la disponibilité et de la maintenance d'un système informatisé, ainsi que de la sécurité des données conservées par le système.

Infrastructure informatique: Ensemble des équipements et logiciels, tels que des logiciels réseau et des systèmes d'exploitation, permettant le bon fonctionnement de l'application.

Logiciel standard du commerce: Logiciel disponible dans le commerce et conçu pour être utilisé par un large spectre d'utilisateurs.

Système informatisé sur mesure ou personnalisé: Système informatisé conçu de manière unique afin de convenir à un processus spécifique.

Tiers: Entités qui ne sont pas sous la responsabilité directe du détenteur de l'autorisation de fabrication et/ou d'importation.