Article 16 Protection/sécurité des données

Type de document : ART
Version : 2
En vigueur de : 01.07.2025

Nouvel article

16.1. Protection des données

Les SRTS sont tenus de mettre en oeuvre les exigences relatives au respect de la loi sur la protection des données.

16.2. Sécurité des données

16.2.1. Systèmes assistés par ordinateur

Lorsque des systèmes informatisés sont utilisés, les logiciels, le matériel et les procédures de sauvegarde doivent être régulièrement contrôlés afin de garantir leur fiabilité. Pour les systèmes critiques, il convient de disposer d'une description actualisée du système, dans laquelle sont définis
les flux de données physiques et logiques et les interfaces avec d'autres systèmes ou processus, toutes les conditions matérielles et logicielles ainsi que les mesures de sécurité.

16.2.2. **Validation et tests**

Les systèmes informatisés doivent être évalués avant d'être utilisés, selon une approche documentée fondée sur les risques. Sur la base de cette évaluation, les systèmes doivent être validés, le cas échéant, et maintenus dans un état validé. Des méthodes et des scénarios de test appropriés doivent être définis et documentés. Les limites des paramètres du système (du processus), les bornes de données et le traitement des erreurs doivent être pris en compte. Les évaluations, les tests, l'évaluation du caractère adéquat doivent être documentés. Les systèmes informatisés qui échangent des données par voie électronique avec d'autres systèmes devraient comporter des contrôles intégrés appropriés pour la saisie et le traitement corrects et sûrs des données, afin de réduire les risques au minimum. L'intégrité et la précision de la sauvegarde des données, ainsi que la capacité à restaurer les données, devraient être vérifiées lors de la validation et faire l'objet d'un suivi régulier. Les changements pertinents dans les systèmes informatisés doivent être évalués et notés au préalable. Selon la classification, ils doivent être validés.

16.2.3. **Systèmes informatisés sur mesure - Spécifiques au client**

Pour la validation des systèmes informatisés sur mesure ou personnalisés, il convient de disposer d'une procédure garantissant l'évaluation formelle et la documentation des mesures de qualité et de performance pour toutes les phases du cycle de vie du système.

16.2.4. **Autorisations**

Le matériel et les logiciels doivent être protégés contre toute utilisation ou modification non autorisée. Il doit exister une hiérarchie d'accès utilisateur autorisé pour la saisie, la modification, la lecture ou l'impression des données.

16.2.5. **Gestion des risques**

La gestion des risques doit être appliquée tout au long du cycle de vie du système informatisé, en tenant compte de la sécurité du donneur, de la sécurité du patient, de l'intégrité des données et de la qualité du produit. L'utilisateur doit prendre toutes les mesures raisonnables pour s'assurer que le système a été développé conformément à un système de gestion de la qualité approprié. Le fournisseur devrait être évalué de manière appropriée.
Toutes les mesures nécessaires doivent être prises pour la protection des données. Ces mesures garantissent que des précautions prises contre l'ajout, le transfert d'informations, la suppression ou la modification non autorisés de données, afin d'éliminer les incohérences dans les données et d'empêcher la divulgation non autorisée de ces informations.

16.2.6. **Intégrité des données**

Les systèmes informatisés qui échangent des données par voie électronique avec d'autres systèmes devraient comporter des contrôles intégrés appropriés pour la saisie et le traitement corrects et sûrs des données, afin de réduire au minimum les risques de transmission erronée.
Si des données doivent transférées dans un autre format, il faut s'assurer que la valeur initiale et/ou le message ne soient pas modifiés au cours du processus de migration.

16.2.7. **Saisie manuelles**

Pour les données critiques qui sont saisies manuellement, un contrôle supplémentaire de l'exactitude des données devrait effectué. Ce contrôle peut être effectué par un deuxième collaborateur ou par des moyens électroniques validés. La criticité et les conséquences potentielles pour un système de données erronées ou mal saisies devraient être couvertes par une gestion des risques.

16.2.8. **Maintenance / mises à jour**

Les systèmes devraient être correctement entretenus à tout moment. Des plans de maintenance pour les systèmes informatisés devraient être établis si nécessaire et mis en œuvre de manière documentée.

16.2.9. **Sauvegardes**

Des copies de sauvegarde de toutes les données pertinentes devraient effectuées régulièrement.

16.2.10. **Garantir la disponibilité des données**

Des précautions devraient être prises pour éviter la perte et/ou l'endommagement des données en cas d'arrêt, prévu ou non, ou de dysfonctionnement du système informatique. Pour les systèmes informatisés qui soutiennent des processus critiques, des dispositions devraient être prise pour assurer la continuité de la prise en charge de ces processus en cas de défaillance du système (par exemple, un système manuel ou alternatif).

Le temps nécessaire à la mise en place des dispositifs alternatifs devrait être basé sur le risque et être adapté au système concerné et au processus opérationnel qu'il soutient. Ces mesures doivent être documentées et testées de manière appropriée.

16.2.11. **Documentation des modifications**

Lors de la création, de la suppression ou de la modification d'applications informatiques, la documentation utilisateur doit être révisée et le personnel concerné doit être formé en conséquence avant qu'une modification soit introduite dans les opérations de routine. Les tests utilisateurs utilisés doivent démontrer que le système répond à toutes les exigences, aussi bien lors de la première installation qu'après chaque modification du système.

16.2.12. **Archivage des données**

Les données qui doivent être archivées en vertu de dispositions légales devraient protégées contre les dommages et les pertes. L'accessibilité, la lisibilité, l'exactitude et l'exhaustivité des données archivées devraient être vérifiées. L'accès aux données devrait être garanti pendant toute la période d'archivage.
Si des modifications importantes sont apportées au système (par exemple, équipement informatique ou programmes), il convient de s'assurer que les données peuvent être récupérées et de procéder à des tests. Il faut également définir les autorisations, par exemple pour la suppression ou la destruction de données.

16.2.13. Validation des systèmes informatiques concernés

Les systèmes informatiques conçus pour contrôler les décisions relatives aux stocks et à la libération des composants sanguins doivent empêcher la libération de sang ou de composants sanguins considérés comme impropres à la libération. Des mécanismes doivent être en place pour empêcher le prélèvement et la libération des composants d'un futur don provenant d'un donneur contre-indiqué.