Conformité aux exigences de la réglementation "21 CFR Part 11" de la FDA

Définition de la réglementation 21 CFR partie 11

Au cours de la dernière décennie, l'industrie pharmaceutique a très rapidement reconnu que la mise en oeuvre de systèmes informatisés au niveau des opérations des unités de production offraient un grand nombre d'avantages, notamment:

- La rapidité accrue des échanges d'informations
- Une meilleure approche dans l'intégration, l'établissement de
- tendances et la recherche de données
- La réduction des erreurs et de la variabilité
- Et enfin, la réduction des coûts liés au stockage des données.

En réaction à la demande des différentes secteurs industriels pour une uniformisation et acceptation des systèmes informatisés, la réglementation finale de la Food and Drug Administration (FDA) des Etats-Unis sur les dossiers et signatures électroniques, connue sous le nom de **21 CFR § 11** partie **11** ou **21 CFR** partie **11** ou "la réglementation", a été promulguée en mars 1997.

Définition de la réglementation ***21 CFR partie 11***
*La réglementation **21 CFR** partie **11** définit les critères selon lesquels les dossiers et signatures électroniques seront considérés comme équivalents à des dossiers sur support papier et des signatures manuscrites. La réglementation s'applique aux dossiers sous forme électronique, qui sont créés, modifiés, maintenus, archivés, récupérés ou transmis dans le cadre des exigences liées à tout dossier décrit dans la réglementation de la FDA.*

La compréhension de l'importance de ces règles sous-jacentes de la FDA ou règles prédicats est critique pour le développement de solutions de conformité à la partie **11**. En outre, la partie **11** s'applique aux dossiers électroniques soumis à la FDA même ceux qui ne sont pas explicitement mentionnées dans les réglementations.
Il faut néanmoins noter que la partie **11** ne s'applique pas aux dossiers sur support papier transmis par des moyens électroniques.

Définitions importantes dans la réglementation 21 CFR partie 11

Dossier électronique:
Toute combinaison de texte, de schémas, données, informations audio, graphiques ou toute autre information représentée sous forme numérique créée, modifiée, maintenue, archivée, récupérée ou distribuée par un système informatique.

Signature électronique:
Une compilation de données informatiques de tout symbole ou série de symboles validée, adoptée ou autorisée par un individu constituant un engagement légal équivalent à la signature manuscrite d'un individu.

Signature manuscrite:
Le nom ou la marque légale sous forme de trace manuscrite d'un individu, écrite à la main par cet individu et validée ou adoptée avec l'intention d'authentifier des écrits sous une forme permanente.

Signature numérique:
Une signature électronique basée sur des méthodes cryptographiques d'authentification du signataire, calculée à partie d'un ensemble de règles et de paramètres, afin que l'identité du signataire et l'intégrité des données puissent être vérifiées.

Biométrie:
Une méthode permettant de vérifier l'identité d'un individu, en fonction de mesures de caractéristiques physiques ou d'actions répétables de l'individu, dans la mesure où ces caractéristiques et/ou actions sont à la fois propres à cet individu et mesurables.

Système fermé:
Un environnement dans lequel l'accès au système est contrôlé par des personnes responsables du contenu des dossiers électroniques du système.

Système ouvert:
Un environnement dans lequel l'accès au système n'est pas contrôlé par des personnes responsables du contenu des dossiers électroniques du système.

Spécifications de la réglementation *21 CFR partie 11*

Un certain nombre d'exigences doivent être satisfaites, pour que la conformité des organisations à la partie **11** soit reconnue. Ces exigences concernent, en général, l'authenticité, l'intégrité et la confidentialité des dossiers et signatures électroniques.

Tout système informatique, qui utilise des dossiers et signatures électroniques doit être validé pour s'assurer de sa précision, fiabilité, de la constance de ses performances et de sa capacité à discerner des enregistrements erronés ou modifiés.

Le système doit être en mesure de générer des copies sous forme lisible (c'est à dire sous forme de texte en clair) et électronique qui soient exactes et complètes.
Plusieurs types de vérifications doivent être intégrées dans les systèmes conformes à la partie **11**, y compris des vérifications d'autorité pour déterminer qui a accès au système et à quel niveau, ainsi que des vérifications des unités pour déterminer la validité des sources de données introduites dans le système.

Une autre exigence importante pour les systèmes conformes à la partie **11** est leur capacité à générer une piste de vérification, définie comme un enregistrement montrant qui a accédé au système de vérification et quelles opérations il ou elle a effectuées au cours d'une période donnée.
Un telle piste de vérification doit répondre aux critères suivants:

- doit être sécurisée, générée par ordinateur et horodatée
- ne doit pas obscurcir des données modifiées précédemment
- doit mentionner le responsable des modifications
- doit contenir les donnée originales et modifiées
- et doit être accessible pour être examinée et copiée par la FDA.

Contrôles pour les systèmes ouverts et fermés

La partie **11** exige qu'un certain nombre de procédures et de contrôles soient mis en place sur les systèmes de dossiers électroniques fermés.
La principale de ces exigences est que les systèmes soient validés pour s'assurer de leur précision, fiabilité, de la constance de leurs performances et de leur capacité à discerner des enregistrements erronés ou modifiés.
La FDA exige que les systèmes fermés soient également en mesure de générer des copies exactes et complètes sous forme lisible (c'est à dire sous forme de texte en clair) et électronique, afin que la FDA puisse inspecter, examiner et copier ces enregistrements, le cas échéant.
Les dossiers électroniques doivent également être protégés pour permettre une récupération précise et facile pendant la période de rétention des dossiers requise soit par la FDA ou toute autre organisme fédéral ou par les procédures ou les modalités spécifiques à l'organisation de l'utilisateur.

Système à accès limité: Filières de vérification précises

Les organisations qui utilisent des dossiers électroniques doivent également limiter l'accès du système aux seules personnes accréditées et prévoir des limites de temps imparti en cas d'inactivité.
La génération et l'utilisation de pistes de vérification sont des éléments critiques de la partie **11**. Ces filières de vérification doivent être sécurisées, générées par ordinateur et horodatées, afin de consigner indépendamment la date et l'heure des entrées et actions des opérateurs, qui créent, modifient ou suppriment des enregistrements électroniques.
Les modifications apportées aux enregistrements dans des systèmes fermés ne doivent pas obscurcir des informations enregistrées précédemment. Toute documentation d'une filière de vérification doit être conservée pendant une période au moins aussi longue que celle requise pour les dossiers électroniques de l'objet en question, et doit être accessible pour être examinée et copiée par la FDA.

Vérifications d'autorité

La réglementation exige également que certaines vérifications soient mises en place sur les systèmes fermés. Il s'agit notamment de l'utilisation de vérifications d'autorité, afin de s'assurer que seuls les personnes accréditées puissent utiliser le système, signer électroniquement un enregistrement, accéder aux unités d'entrée ou de sortie du système d'opérations ou du système informatique, modifier un enregistrement ou exécuter l'opération immédiatement, ainsi que de vérifications des unités pour déterminer la validité de la source d'entrée des données ou des directives opérationnelles.

Personnel spécialisé et qualifié

Comme pour la plupart des réglementations de la FDA, la partie **11** exige que les personnes qui développent, maintiennent ou utilisent des systèmes de dossiers et de signatures électroniques aient le niveau d'étude, les qualifications et l'expérience nécessaires pour effectuer les tâches qui leur incombent. Les organisations qui utilisent des systèmes de dossiers et signatures électroniques fermés doivent établir et respecter des procédures écrites, qui rendent leurs employés comptables et responsables des actions entreprises sous leur signature électronique, afin de décourager toute falsification de dossiers et de signatures. Ils doivent également exercer des contrôles appropriés sur la documentation des systèmes, dans le domaine de la ventilation, de l'accès à la documentation et de son utilisation pour la maintenance et l'exploitation des systèmes. Des procédures de contrôle des révisions et modifications doivent être mises en place pour maintenir une filière de vérification, qui documente chronologiquement le développement et les modifications de la

documentation du système de dossiers électroniques. D'autres procédures et modalités sont nécessaires pour la protection des dossiers: période de rétention des dossiers, limitation de l'accès au système, niveau d'études et formation, et contrôles des révisions et modifications.

Contrôles dans les systèmes ouverts par rapport aux systèmes fermés

La FDA exige que les mêmes contrôles soient appliqués aux systèmes ouverts et fermés. Mais, les systèmes ouverts doivent également être soutenus par des procédures et contrôles pour assurer l'authenticité, l'intégrité et la confidentialité des dossiers électroniques créés, modifiés, maintenus ou transmis sur ces systèmes.
Ces procédures et contrôles peuvent comprendre des mesures comme l'utilisation de techniques cryptographiques pour les documents et des normes sur les signatures électroniques.

Signatures électroniques

La partie **11** impose un ensemble d'exigences générales obligatoires sur les organisations qui ont l'intention d'utiliser des signatures électroniques.
Chaque signature électronique utilisée doit être unique pour chaque individu et ne peut être réutilisée ou affectée à un autre individu. Les organisations doivent vérifier l'identité de l'individu avant de lui attribuer une signature électronique. Elles doivent également certifier par écrit (sur support papier) à la FDA qu'elles souhaitent utiliser leur signature électronique comme l'équivalent légal de leur signature manuscrite, et, le cas échéant, soumettre des attestations supplémentaires de leur intention à la FDA.

Signatures biométriques et non biométriques

Les signatures électroniques doivent présenter certaines caractéristiques selon qu'elles sont biométriques ou non biométriques. Les signatures électroniques biométriques doivent être conçues pour qu'elles ne puissent pas être utilisées par quiconque d'autre que leur propriétaire légitime.
Les signatures électroniques non biométriques doivent au moins comprendre deux éléments d'identification distincts (ex.: identification de l'utilisateur et mot de passe), ne doivent être utilisées que par leur propriétaire légitime, et doivent être gérées et validées, de telle manière que deux ou plusieurs personnes sont nécessaires pour dupliquer la signature.
Un autre enjeu lié à l'utilisation de signatures électroniques non biométriques est celui des périodes d'accès contrôlé. Si, au cours d'une seule période d'accès contrôlé, un individu utilise plusieurs fois sa signature, il doit utiliser tous les composants de sa signature électronique pour la première signature, et au moins un élément secret pour toutes les signatures suivantes. Si, par contre, les signatures ne sont pas toutes "apposées" au cours d'une seule période d'accès contrôlé, chacune d'elle doit comprendre tous les éléments de la signature.

Présence et liens des signatures

La FDA exige que les enregistrements à signature électronique mentionnent clairement le nom du signataire, la date et l'heure de la signature, et la raison de la signature.
Ces enregistrements doivent être soumis aux mêmes contrôles que les enregistrements électroniques, et doivent également être mis à la disposition de la FDA pour être examinés et copiés.
Les signatures électroniques et manuscrites appliquées à des enregistrements électroniques doivent être rattachées à leurs enregistrements électroniques respectifs, pour s'assurer que les signatures ne peuvent être extraites, copiées ou transférées de quelque manière que ce soit pour falsifier un enregistrement électronique par des moyens ordinaires (ex.: par un simple couper et coller).

Signatures en utilisation continue

La partie **11** permet des périodes d'utilisation continue où les dossiers électroniques peuvent être signés en utilisant un seul jeton de contrôle. Ceci permet, lorsqu'une personne accède initialement au système ou se "connecte" et peut ensuite "apposer" plusieurs signatures, en exécutant au moins un jeton de contrôle de la signature électronique, dans des conditions contrôlées, d'éviter qu'une autre personne n'usurpe l'identité du signataire légitime.
Afin de répondre aux exigences d'utilisation continue, il est vital de mettre en place des contrôles stricts pour éviter toute usurpation d'identité. Ces contrôles couvrent notamment:

- L'obligation d'un individu à rester à proximité du poste de travail pendant toute la session de signature.
- Des mesures de déconnexion automatique de la personne connectée en cas d'inactivité, si aucune saisie ou action n'est effectuée dans un délai imparti.
- L'obligation qu'un seul élément nécessaire pour d'autres signatures ne soit connu et ne puisse être utilisé que par la personne accréditée.

En dehors de l'utilisation d'un seul jeton de contrôle pour la signature, toutes les autres exigences liées aux signatures électroniques sont applicables au cours d'une période d'utilisation continue, ce qui nécessite que l'opérateur soit informé que sa signature est en cours de validation, et que la signification de la signature est claire.

Application des séquences d'opérations

Une meilleure approche pour une saisie précise des données peut nécessiter deux signatures pour la validation d'un dossier électronique. La première signature permet d'identifier la personne qui saisit les données, alors que la seconde identifie la personne qui a vérifié que les données saisies sont correctes. Dans certains cas, plus de deux signatures peuvent également s'avérer nécessaires.