

**ansm**

Agence nationale de sécurité du médicament  
et des produits de santé

# Focus sur l'intégrité des données

Réunion d'information à destination des opérateurs  
« matières premières à usage pharmaceutique »

DIRECTION DE L'INSPECTION



Engagement



Transparence



Impartialité



Compétence

**NABIL BEZZENINE**

Inspecteur - Pôle inspection des matières premières  
Direction de l'inspection

23 Novembre 2017  
ANSM (Saint-Denis)

## Sommaire :

- ❑ Pourquoi est-ce une préoccupation majeure du moment ?
- ❑ Exemples d'écarts relevés lors des inspections
- ❑ Qu'est-ce que l'intégrité des données ? Principes ALCOOA (+)
- ❑ Rappels réglementaires – Convergence internationale
- ❑ Notions de base concernant l'intégrité des données / Attentes de l'Ansm :
  - ➔ Contrôle des formulaires vierges
  - ➔ Données « Statiques » versus « Dynamiques »
  - ➔ Restrictions d'accès aux systèmes informatisés
  - ➔ Revue de l' « Audit trail »
  - ➔ Sauvegarde des données électroniques
  - ➔ Considérations pour les activités sous-traitées
- ❑ Conclusions

## Pourquoi est-ce une préoccupation majeure du moment ?

**Augmentation significative** du nombre et des types de problèmes liés à l'intégrité des données lors des dernières années



**Lettres d'injonction**  
(site internet de l'ANSM)  
**Rappel à la loi**

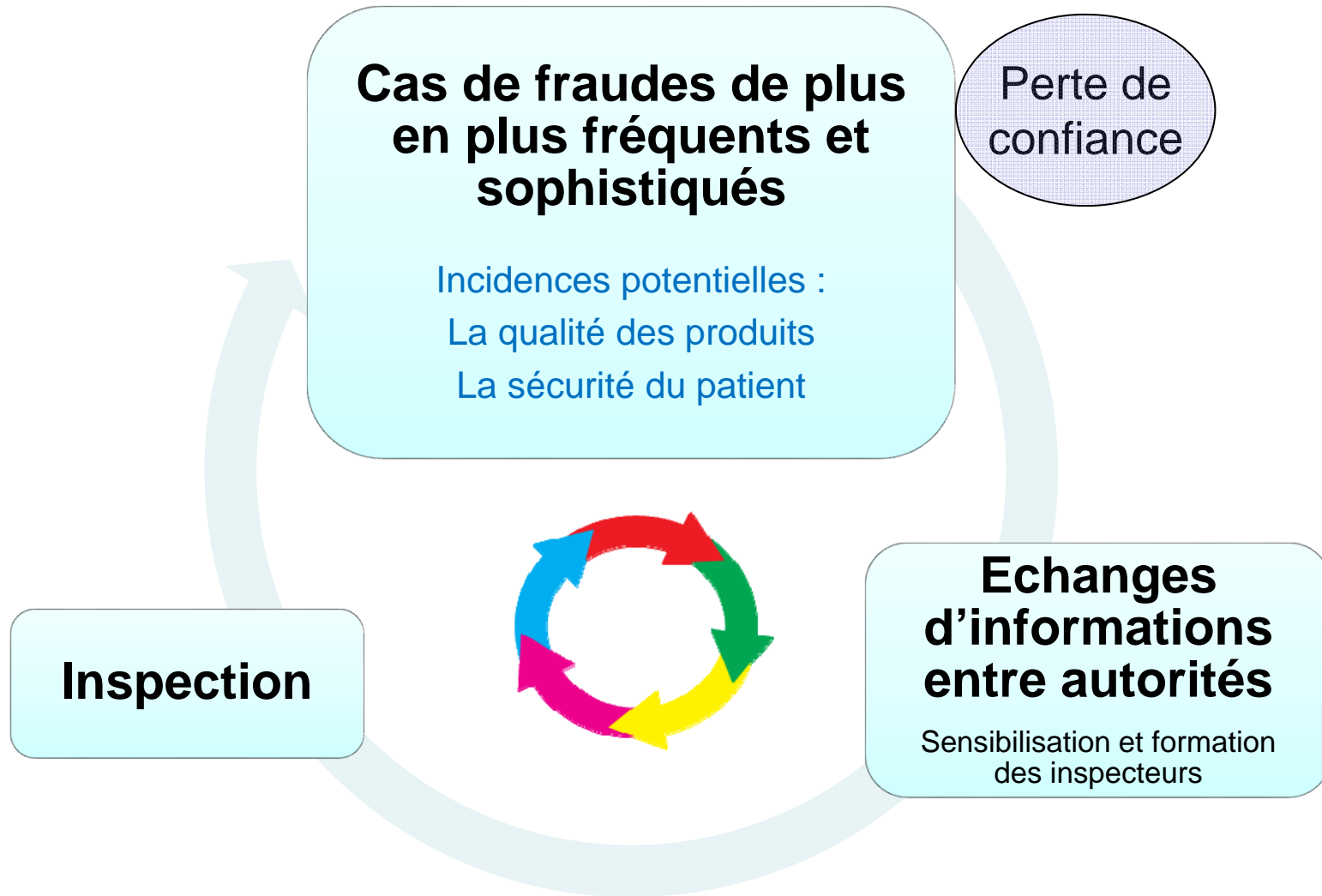


**Rapports de non-conformité  
aux BPF**  
(EudraGMDP)



« **Warning Letters** »  
(Site internet de l'US-FDA)

# Pourquoi est-ce une préoccupation majeure du moment ?



## Exemples d'écarts relevés lors des inspections



### Type n°1 :

- ◆ Données analytiques, de production et réglementaires falsifiées :
  - ❑ Données existantes enregistrées comme étant nouvelles
  - ❑ Données fabriquées
  - ❑ Données manipulées (NC ⇒ C)
- ◆ Origine de la substance active falsifiée

## Exemples d'écart relevés lors des inspections



### Type n°2 :

- ◆ Gestion des formulaires vierges non maîtrisée
  - ❑ Enregistrements réécrits (avec ou sans modifications)
  - ❑ Formulaires vierges partiellement remplis mis au rebut
- ◆ Données non enregistrées en temps réel
- ◆ Enregistrements antidatés
- ◆ Enregistrements non remplis par la personne ayant réalisée l'action
- ◆ Enregistrements de contrôle ou dossiers de lots de production non disponibles

## Exemples d'écart relevés lors des inspections



Type n°3 :

- ◆ Des systèmes informatisés mal conçus et/ou mal contrôlés :
  - ❑ Absence de système de gestion des profils d'utilisateurs :
    - ✓ Pas d'identifiant ni de mot de passe,
    - ✓ Profil partagé,
    - ✓ Profil administrateur disponible pour tout le personnel
  - ❑ Absence d'« audit trail » ou « audit trail » inactivé
  - ❑ Absence de protection contre la suppression des données
  - ❑ Absence de sauvegarde des données

## Exemples d'écart relevés lors des inspections



Type n°4 :

- ◆ Analyses non officielles des échantillons CQ  
☞ « **Echantillon test** »
- ◆ Ré-analyses jusqu'à l'obtention de résultats acceptables  
☞ « **Analyse orientée vers un résultat cible** »
- ◆ Données enregistrées incomplètes  
☞ « **Rapport sélectif** »
- ◆ Intégration manuelle erronées des pics chromatographiques



## Qu'est-ce que l'intégrité des données ?

### Définition :

C'est la mesure dans laquelle toutes les données doivent être **complètes, cohérentes** et **précises** tout au long de leur *cycle de vie*.

( Générées )



① **Système papier ;**

② **Systèmes informatisés :**

- Appareils simples  
⇒ **Système hybride**
- Equipements connectés à un système informatisé complexe  
⇒ **Système électronique**

## Qu'est-ce que l'intégrité des données ?

*Pas une nouvelle réglementation*

Une nouvelle approche dans la gestion et le contrôle des données

Observations lors des inspections

Evolution technologique

Textes réglementaires  
BPF/ICH

Intégrité des données

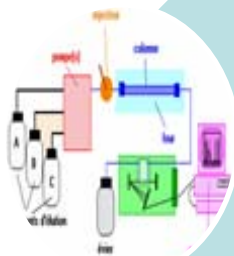
## Qu'est-ce que l'intégrité des données ?



### Attention:



L'intégrité des données n'est pas toujours associée aux falsifications / fraudes

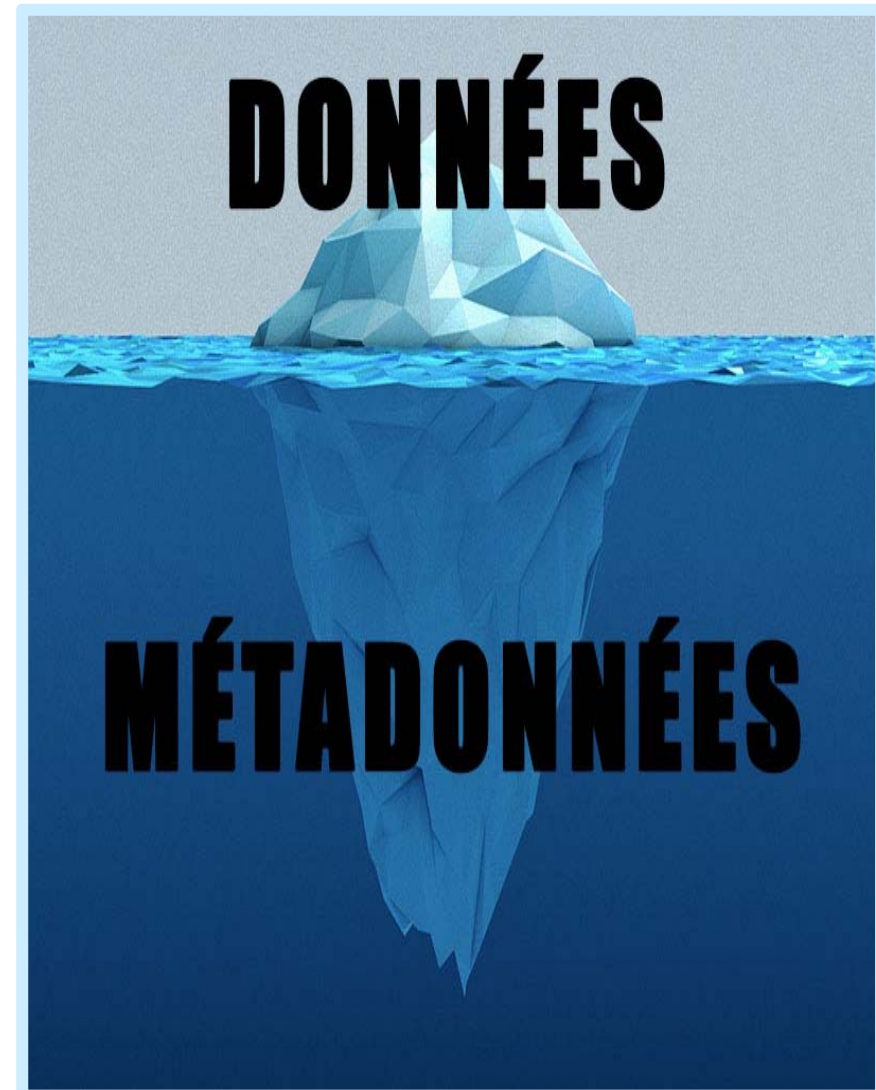


L'intégrité des données ne concerne pas uniquement les systèmes chromatographiques du CQ

## Qu'est-ce que les « métadonnées » ?

Les «**Métadonnées**» sont des données sur les données.

☞ Elles fournissent le contexte et la relation avec les données primaires préservant ainsi l'exactitude, l'exhaustivité, le contenu et la signification.





## Qu'est-ce que l'intégrité des données ?

### Principes **ALCOA+**

<b>A</b> ttributable ( <i>Attribuable</i> )	<b>C</b> omplete ( <i>Complète</i> )
<b>L</b> egible ( <i>Lisible</i> )	<b>C</b> onsistent ( <i>Cohérente</i> )
<b>C</b> ontemporaneous ( <i>Contemporain</i> )	<b>E</b> nduring ( <i>Durable</i> )
<b>O</b> riginal ( <i>Originale</i> )	<b>A</b> vailable ( <i>Disponible</i> )
<b>A</b> ccurate ( <i>Précise</i> )	



## Comment la criticité des données peut-elle être évaluée ?

**Q1** : Quel type de décision les données peuvent influencer ?

**Q2** : Quel est l'impact des données sur la qualité ou la sécurité des produits ?





## Comment les risques associés aux données peuvent-ils être évalués et atténués ?

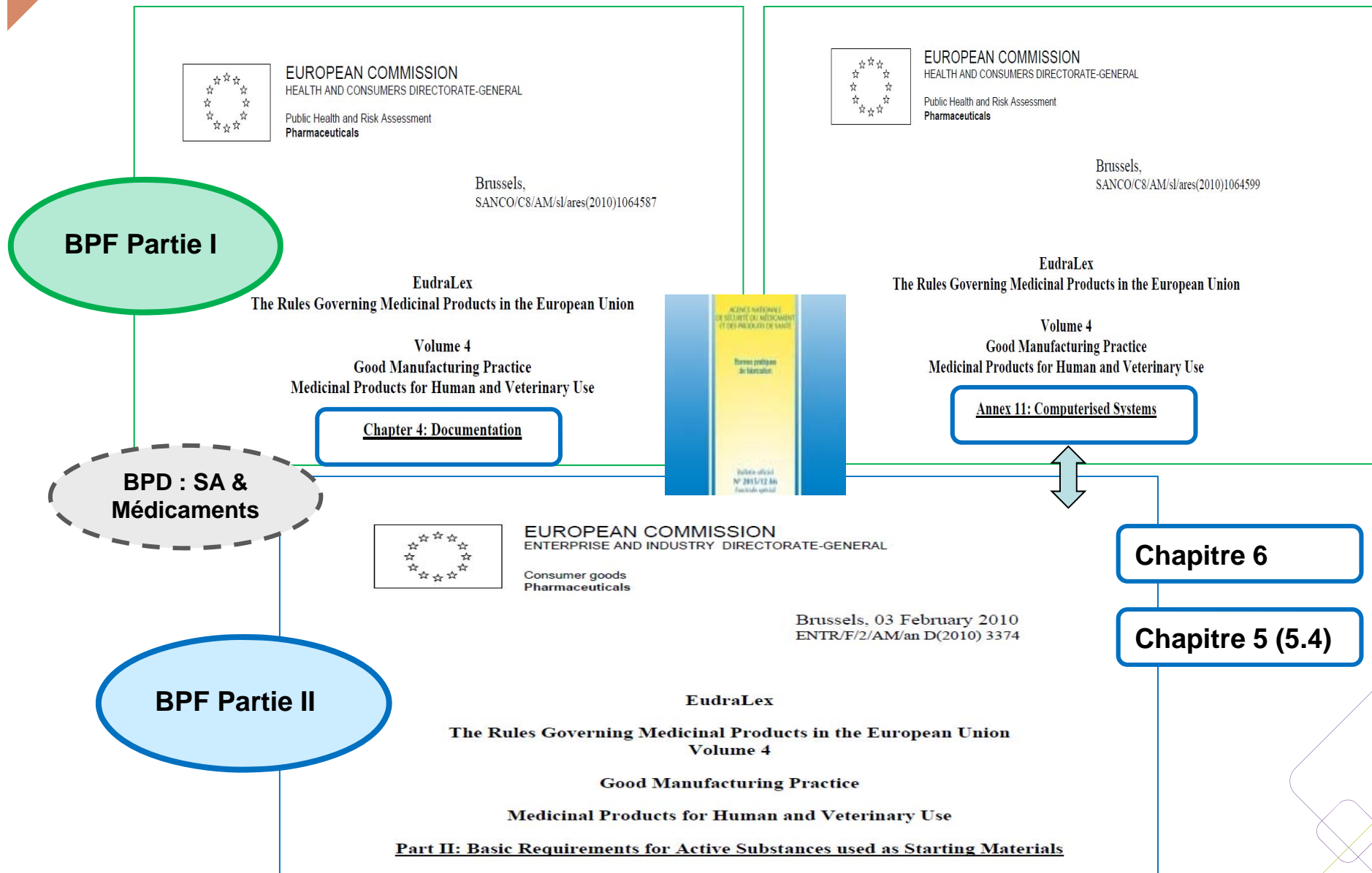
### Evaluation des risques

- Tenir compte de la **vulnérabilité** des données
- Tenir compte des processus et non uniquement des fonctionnalités des systèmes informatisés

### Atténuation des risques

- mesures de contrôle pour :
  -  empêcher une activité non autorisée
  -  augmenter la détectabilité

# Rappels réglementaires





## Exemples de correspondance entre les principes « ALCOA » et les références BPF partie II et annexe 11

<b>ALCOA</b>	<b>BPF Part II</b>	<b>Annex 11</b>
<b>Attributable</b> ( <i>Attribuable</i> )	[5.43], [6.14], [6.18], [6.52]	[2], [12.1], [12.4], [15]
<b>Legible</b> ( <i>Lisible</i> )	[6.11], [6.14], [6.15], [6.50]	[4.8], [7.1], [7.2] [8.1], [9], [10], [17]
<b>Contemporaneous</b> ( <i>Contemporain</i> )	[6.14]	[12.4], [14]
<b>Original</b> ( <i>Originale</i> )	[6.14], [6.15], [6.16]	[8.2], [9]
<b>Accurate</b> ( <i>Précise</i> )	[5.40], [5.42], [5.45], [5.46], [5.47], [6.6]	[Paragraph "Principles"] [4.8], [5], [6], [7.2], [10], [11]



## Convergence internationale

- ◆ **EMA** Questions and answers: Good Manufacturing Practice - Data Integrity (August 2016)
- ◆ **PIC/S** Guidance PI 041-1: Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments – Draft version, August 2016
- ◆ **FDA** Guidance for Industry: Data Integrity and Compliance with CGMP – Draft version, April 2016
- ◆ **WHO** Technical Report Series No. 996, 2016 - Annex 5: Guidance on Good Data and Record Management Practices
- ◆ **MHRA** GxP Data Integrity Definitions and Guidance for Industry - Draft version for consultation, July 2016.



## Comment les formulaires vierges doivent être émis et contrôlés?

- ◆ L'émission doit être contrôlée par une procédure écrite.
  - ❑ **Qui et Quand ?**
  - ❑ **Comment?** (Mise à disposition)
    - Par exemple :
      - ✓ Identifiant unique enregistré pour chaque formulaire
      - ✓ Tampon sécurisé, code couleur papier non disponible dans les zones de travail etc.
  - ❑ Les **formulaires incomplets ou erronés** doivent être **conservés avec une justification formalisée** de leur remplacement.
  - ❑ **Réconciliation** (le cas échéant)



## Qu'est ce qu'une donnée originale - Donnée « Statique » versus « Dynamique » ?

- ◆ Une donnée originale est la première capture d'information, qu'elle soit enregistrée
  - ❑ sur papier ou une image électronique (**statique**) ou
  - ❑ électroniquement (généralement **dynamique**, selon la complexité du système).  
Par exemple : un chromatogramme enregistré sous forme dynamique permet de vérifier le retraitement des données
- ◆ Les informations capturées à l'origine dans un état dynamique doivent rester disponibles dans cet état.



## Comment définir les restrictions d'accès aux systèmes informatisés concernés par les BPF?

- ◆ **Liste des personnes autorisées** et de leurs **privilèges d'accès** pour chaque système électronique utilisé :  
ségrégation stricte des droits
- ◆ **Identifiants et mots de passe** de connexion **individuels** doivent être configurés et assignés
- ◆ **Déconnexion automatique** doit être mise en place
- ◆ L'octroi de **droits d'accès administrateur** pour exécuter les applications critiques doit être strictement contrôlé :  
Indépendant des utilisateurs exécutant la tâche



## Qu'est-ce qu'un « Audit trail » ? Quand et comment il doit être revu ?

Reconstituer le cours des événements relatifs à la création, à la modification ou à la suppression d'un enregistrement électronique.

Doit inclure pour chaque événement :

**Quoi, Qui, Quand et pourquoi** (le cas échéant)

- ◆ Les fonctionnalités doivent être :
  - ❑ vérifiées lors de la validation du système
  - ❑ configurées pour enregistrer tous les processus initiés manuellement liés aux données critiques
  - ❑ activées et verrouillées
- ◆ Le système doit être en mesure d'émettre un rapport électronique dans un format compréhensible



## Qu'est-ce qu'un « Audit trail » ? Quand et comment il doit être revu ? (Suite)

- ◆ Une procédure décrivant le processus d'examen des « Audit trails » doit-être mise en place :
  - ❑ **Fréquence en fonction de la criticité** des données.
    - ✓ L'examen des « audit trails » doit faire partie de la revue des données de routine du processus d'approbation
  - ❑ **Rôles et responsabilités : comment** passer en revue des « audit trails », **que chercher, comment exécuter des recherches** etc.
- ◆ Cette activité doit être documentée et enregistrée
- ◆ Toute déviation significative doit être entièrement examinée et enregistrée



## Comment les données électroniques doivent être sauvegardées ?

- ◆ **Sauvegardes régulières** conformément à une procédure approuvée.
- ◆ Les données sauvegardées doivent :
  - ❑ inclure toutes les données et métadonnées d'origine, y compris les « Audit trails », à l'aide d'un processus sécurisé et validé
  - ❑ avoir un **contrôle approprié** afin d'interdire l'accès non autorisé, les modifications et la suppression de données ou leur altération





## Quel sont les considérations pour l'intégrité des données des activités sous-traitées ?

- ◆ Une **qualification** initiale et périodique robuste des sous-traitants doit inclure une **vérification adéquate des données et des métadonnées** en utilisant une **approche de gestion des risques de qualité**. Cela peut être réalisé par des mesures telles que :
  - ❑ Audit sur site
  - ❑ Analyse interne versus certificat d'analyse reçu
  - ❑ Examen des données à distance, etc.



## Conclusion

Il est de votre responsabilité de mettre en place une organisation et un système qualité robustes, basés sur une approche de gestion du risque, permettant de prévenir et de détecter les vulnérabilités d'intégrité des données

- ◆ Identifier les systèmes et les données critiques
- ◆ Sélectionner des systèmes informatisés ayant une configuration permettant d'assurer l'intégrité, la traçabilité et la fiabilité des données
- ◆ Sensibiliser le personnel aux problèmes d'intégrité des données
  - 👉 Formation à la détection des problèmes
  - 👉 Formation aux systèmes informatisés



## Conclusion (suite)

- ◆ Intégrer la vérification de l'intégrité des données dans le cadre du programme des audits internes et des procédures de qualification des sous-traitants
- ◆ Informer la direction de l'entreprise en mettant en place un mécanisme interne de signalement des problèmes graves liés à l'intégrité des données.

### **Avertissement**

- Lien d'intérêt : personnel salarié de l'ANSM (opérateur de l'Etat).
- La présente intervention s'inscrit dans un strict respect d'indépendance et d'impartialité de l'ANSM vis-à-vis des autres intervenants.
- Toute utilisation du matériel présenté, doit être soumise à l'approbation préalable de l'ANSM.

### **Warning**

- Link of interest: employee of ANSM (State operator).
- This speech is made under strict compliance with the independence and impartiality of ANSM as regards other speakers.
- Any further use of this material must be submitted to ANSM prior approval.