NOTE DE SYNTHESE

« Etat des lieux de la conformité des fabricants de médicaments à usage humain (médicaments chimiques et biologiques) et de substances actives ainsi que des laboratoires sous-traitants d'analyses physico-chimiques et/ou microbiologiques(1) au regard des exigences relatives à l'intégrité des données électroniques ».

(1) désignés sous le terme de sous-traitants d'analyses dans l'ensemble du document.

Remerciements

Nous tenons à remercier les trois pôles suivants de la Direction de l'Inspection (ANSM) :

- Pôle d’inspection des matières premières ;
  (***insmp@ansm.sante.fr***)
- Pôle d’inspection des produits pharmaceutiques et lutte contre les fraudes ;
  (***ipplf@ansm.sante.fr***)
- Pôles d’inspection des produits biologiques.
  (***insbio1@ansm.sante.fr***).

Pour leur grande contribution à l’élaboration de cette note de synthèse.

Nous remercions également les établissements qui ont répondu à l'enquête réalisée par l’ANSM sur l’intégrité des données électroniques au laboratoire de contrôle qualité. Leurs réponses détaillées ont permis d'enrichir cette étude.

Sommaire

REMERCIEMENTS 2

RESUME 4

1. INTRODUCTION 5

1.1. Contexte et enjeux de l'intégrité des données 5

1.2. Objectifs de la note de synthèse 5

1.3. Méthodologie de collecte et d'analyse des données 6

2. ANALYSE DES DONNÉES COLLECTÉES 7

2.1. Données recueillies lors de l'enquête conduite par l'ANSM 7

2.1.1. Renseignements sur les établissements ayant répondu à cette enquête 7

2.1.2. Résultats des inspections internationales, des audits clients ou donneurs d'ordre et des audits internes ayant couvert des aspects liés à l'intégrité des données électroniques générées au laboratoire de contrôle qualité 9

2.1.3. Etat des lieux, problème rencontrés et moyens mis en œuvre pour assurer la conformité aux exigences réglementaires des données électroniques générées dans les laboratoires de contrôle qualité 11

2.2. Données recueillies lors de la campagne d'inspections réalisées par l'ANSM20

2.2.1. Présentation générale des résultats d'inspection, mettant en évidence le nombre et la criticité des écarts par domaine d'inspection 21

2.2.2. Identification des domaines de défaillance et analyse de tendance.....22

2.2.3. Analyse des domaines problématiques 23

2.2.3.1. Gestion du risque 23

2.2.3.2. Personnel 23

2.2.3.3. Validation 24

2.2.3.4. Stockage des données 25

2.2.3.5. Traçabilité des modifications 26

2.2.3.6. Evaluation périodique 27

2.2.3.7. Sécurité 28

3. RECOMMANDATIONS 29

4. CONCLUSION..... 31

5. BIBLIOGRAPHIE 32

Résumé

Ce document dresse un état des lieux de la conformité et des difficultés rencontrées par les fabricants de substances actives, les fabricants de médicaments à usage humain (médicaments chimiques et biologiques) et les sous-traitants d'analyses situés sur le territoire national par rapport à la maîtrise de l'intégrité des données électroniques dans les laboratoires de contrôle qualité. Cette étude s'appuie sur :

- une revue de la réglementation applicable incluant les guides et les questions/réponses publiées par les autorités de santé sur cette thématique ;
- les résultats d'une campagne d'inspections
- les réponses des opérateurs à une enquête menée par l'ANSM sur ce sujet.

Des rappels concernant les Bonnes Pratiques de Fabrication (BPF) relatives à cette thématique et des recommandations basées sur une évaluation des risques ont également été intégrés à cette étude.

1. INTRODUCTION

1.1. Contexte et enjeux de l'intégrité des données

Les inspections réalisées par les autorités de santé nationales et internationales auprès des fabricants et distributeurs de substances actives (SA) et de médicaments à usage humain (médicaments chimiques et biologiques) sont nécessaires pour évaluer la conformité de ces établissements aux Bonnes Pratiques de Fabrication (BPF) et aux Bonnes Pratiques de Distribution (BPD). La vérification de l'intégrité des données est un élément important dans ce processus d'inspection car la qualité et la sécurité des produits fabriqués dépendent notamment de la fiabilité des données.

La bonne gestion des données relève de la responsabilité du fabricant, et du distributeur le cas échéant. Ce dernier doit évaluer régulièrement son processus de gestion des données pour identifier les vulnérabilités potentielles et mettre ainsi en place des pratiques de gouvernance des données solides afin de garantir l'intégrité des données. Ces données doivent respecter les principes de l'« ALCOA+ » en étant attribuables, lisibles, contemporaines, originales, fiables, complètes, cohérentes, durables et disponibles.

La maitrise de l'intégrité des données est devenue, depuis quelques années, une préoccupation majeure pour les autorités de santé à l'échelle mondiale dans la mesure où une augmentation significative des écarts liés à cette thématique a été observée lors des inspections. Ces manquements ont entraîné différentes mesures réglementaires telles que des déclarations de non-conformité aux BPF européennes, des lettres d'avertissement, des alertes d'importation de l'« U.S Food and Drug Administration » et des lettres d'injonction émises par l'ANSM.

Afin de standardiser les pratiques, plusieurs guides et questions/réponses ont été élaborés ces dernières années par les autorités de santé témoignant d'une collaboration importante sur ce sujet ; ces travaux ayant pour principal objectif de clarifier les attentes des autorités en matière d'intégrité des données.

1.2. Objectifs de la note de synthèse

L'objectif de cette note de synthèse est :

1) d'établir un état des lieux de la conformité des fabricants de substances actives, de médicaments à usage humain (médicaments chimiques et biologiques) ainsi que des laboratoires sous-traitants d'analyses au regard des exigences relatives à l'intégrité des données électroniques. En raison de la vaste portée de ce sujet, le périmètre de cette note de synthèse a été restreint aux données électroniques produites, traitées et enregistrées dans un laboratoire de contrôle qualité par les systèmes informatisés utilisés pour :
    - la gestion des activités de contrôle et de certification/libération des lots, tels que les progiciels et les systèmes d'information de laboratoire ;
    - le pilotage des équipements d'analyse. Il est à noter que les « systèmes hybrides » qui permettent de générer à la fois des

données sur des supports papiers et électroniques ont été inclus dans le champ de cette note de synthèse ;

2) d'élaborer des recommandations en matière de bonne gestion des données destinées aux fabricants de substances actives, de médicaments à usage humain (médicaments chimiques et biologiques) ainsi qu'aux laboratoires sous-traitants d'analyses.

Cette note de synthèse n'a pas pour objectif de définir les principes généraux de l'intégrité des données ni de proposer une méthodologie pour la mise en œuvre d'une politique de maîtrise de l'intégrité des données dans les laboratoires de contrôle de la qualité.

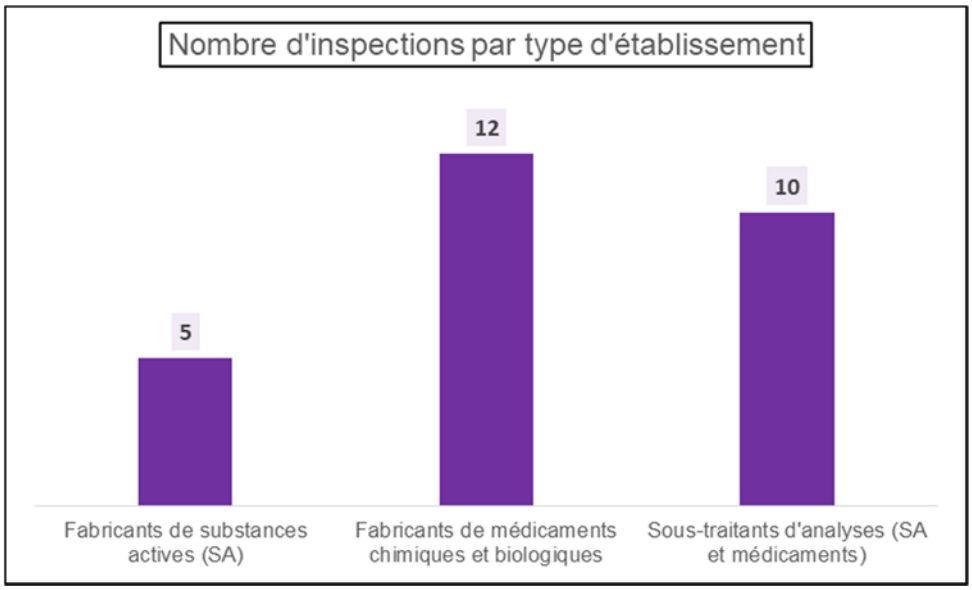
1.3. Méthodologie de collecte et d'analyse des données

Deux types de données d'entrée ont été utilisés pour l'élaboration de cette note de synthèse :

1) Les informations collectées lors de l'enquête réalisée en ligne par l'ANSM, sur la gestion de l'intégrité des données électroniques générées dans les laboratoires de contrôle qualité. L'ensemble des établissements impliqués dans la fabrication de substances actives et/ou de médicaments à usage humain (médicaments chimiques et biologiques), y compris les laboratoires sous-traitants d'analyses situés sur le territoire national, ont été invités à répondre à cette enquête. Cette enquête a été ouverte aux opérateurs entre le 06 mars 2023 et le 31 avril 2023. Au total, 239 établissements ont répondu à ce questionnaire. Le questionnaire correspondant comprenait une vingtaine de questions réparties dans les trois thèmes suivants :
   - Renseignement sur les établissements ayant répondu à cette enquête ;
   - Résultats des inspections internationales, des audits clients ou donneurs d'ordre et des audits internes ayant couvert des aspects liés à l'intégrité des données électroniques générées au laboratoire de contrôle qualité ;
   - Etat des lieux, problèmes rencontrés et moyens mis en œuvre pour assurer la conformité des données électroniques générées au laboratoire de contrôle qualité, aux exigences réglementaires ;

2) Les écarts et les informations recueillis lors d'une campagne d'inspections portant sur l'intégrité des données électroniques au laboratoire de contrôle réalisée par l'ANSM entre juillet 2019 et juillet 2022. Pour cette campagne d'inspections, des établissements de différentes tailles et de différents niveaux de conformité aux Bonnes Pratiques de Fabrication (BPF) ont été sélectionnés. Au total 27 établissements ont été inspectés sur le territoire national parmi lesquels :
   - 9 ont été inspectés par le pôle d'inspection des matières premières [INSMP] : 5 fabricants de substances actives et 4 sous-traitants d'analyses (dont 3 ayant le statut d'établissement pharmaceutique) ;

- 18 par les pôles d'inspection des produits biologiques [INSBIO1] et d'inspection des produits pharmaceutiques et lutte contre les fraudes [IPPLF] : 12 fabricants de médicaments et 6 sous-traitants d'analyses ayant tous le statut d'établissement pharmaceutique. Le nombre d'inspections par type d'établissement est mentionné dans le graphique 1.



Graphique 1

2. ANALYSE DES DONNÉES COLLECTÉES

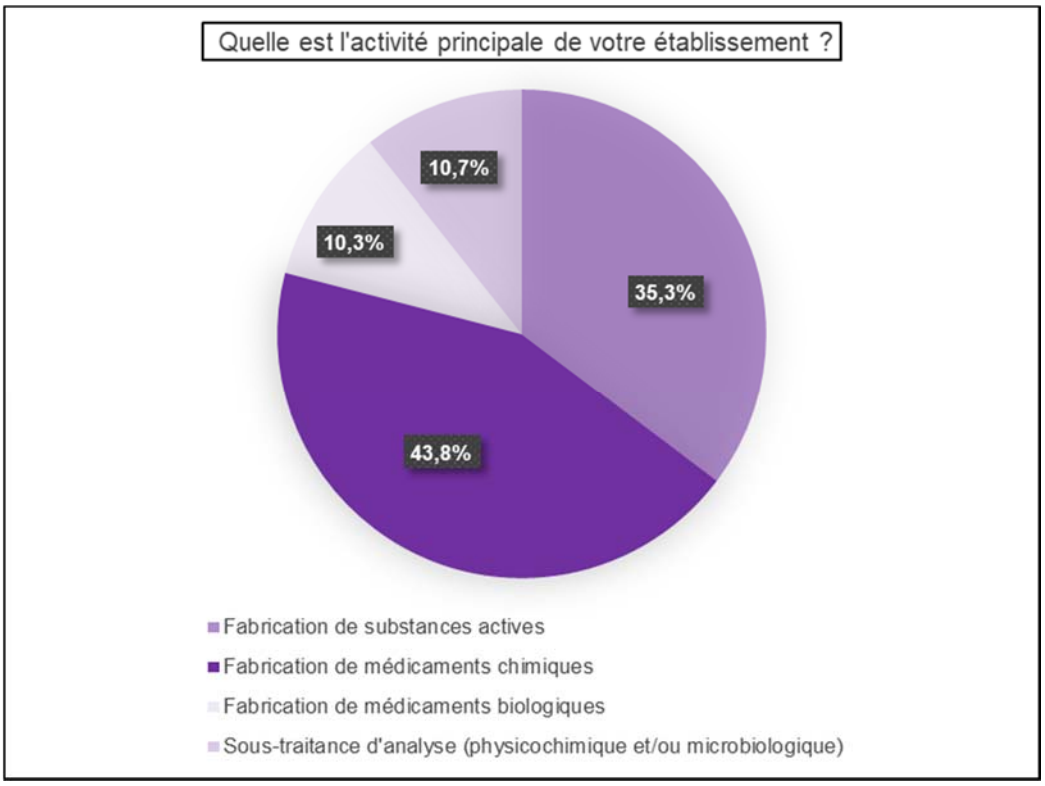
Pour obtenir une vision d'ensemble de l'intégrité des données électroniques générées dans les laboratoires de contrôle qualité, il a été décidé d'adopter une approche permettant de comparer les résultats obtenus lors de la campagne d'inspections avec les réponses des opérateurs à l'enquête réalisée par l'ANSM. L'objectif de cette approche étant d'avoir une vue d'ensemble consolidée incluant la totalité des informations et des non-conformités relevées. Les tendances majeures et les domaines de défaillance récurrents ont été ensuite analysés. Cette analyse a permis d'identifier les principaux points de vulnérabilité en matière d'intégrité des données et de proposer des recommandations.

2.1. Données recueillies lors de l'enquête conduite par l'ANSM

Les réponses des 239 établissements ayant participé à cette enquête ont été consolidées et évaluées et les risques associés à chaque domaine de vulnérabilité ont été identifiés et présentés dans le paragraphe 2.1.3 de ce document.

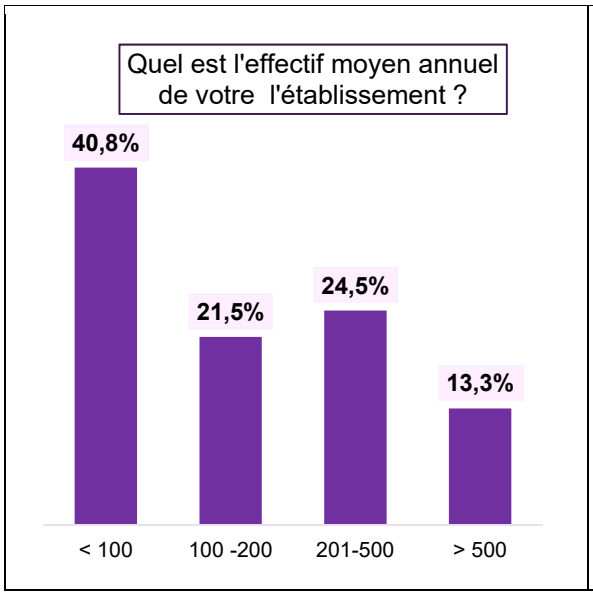
2.1.1. Renseignements sur les établissements ayant répondu à cette enquête

La répartition des 239 établissements ayant répondu à cette enquête par secteur d'activité est mentionnée dans le graphique 2.

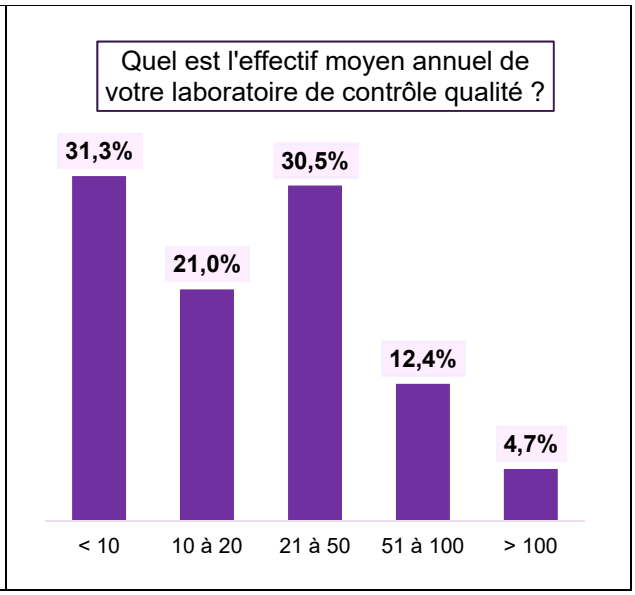


Graphique 1

La répartition de l'effectif moyen annuel de ces établissements ainsi que celle de leurs laboratoires de contrôle qualité sont présentées respectivement dans les graphiques 3 et 4.



Graphique 3



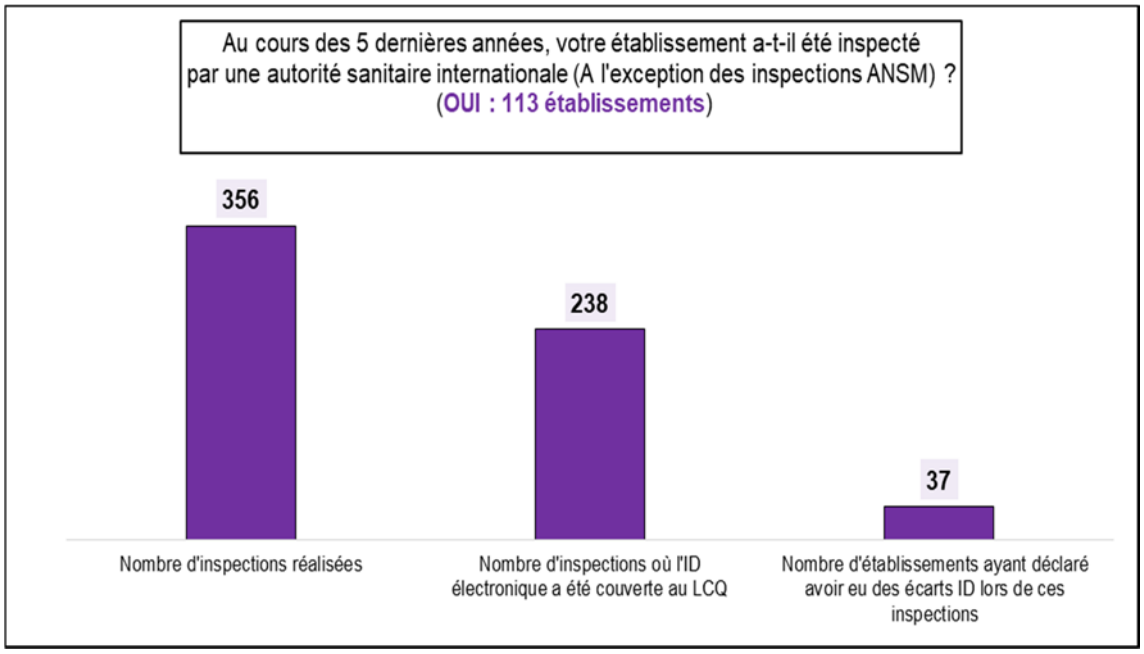
Graphique 4

Les établissements ayant répondu à cette enquête avaient des effectifs très différents, ce qui permet de démontrer une bonne représentativité dans les réponses fournies à cette enquête. De plus, l'évaluation des réponses reçues a montré une corrélation entre l'effectif moyen de l'établissement et celui du laboratoire de contrôle qualité. Par exemple, parmi les laboratoires de contrôle qualité ayant un effectif inférieur à 10 personnes, 80,2 % appartiennent à des établissements ayant un effectif inférieur à

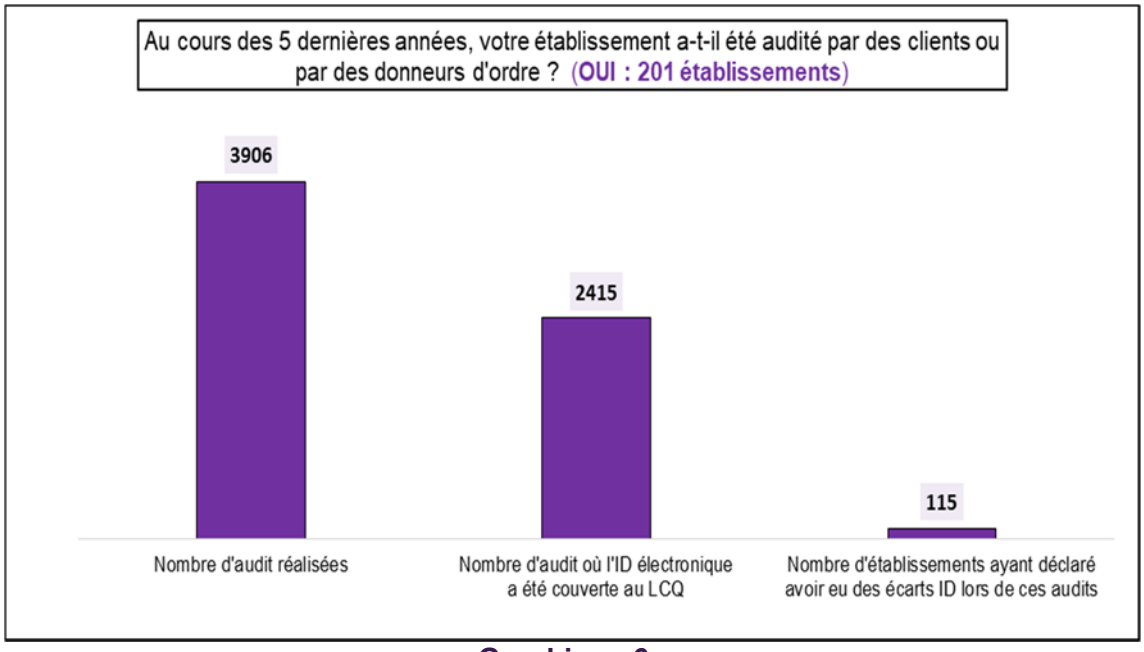
100. Les 19,8% restants appartiennent à des établissements ayant un effectif compris entre 100 et 200 personnes.

2.1.2. Résultats des inspections internationales, des audits clients ou donneurs d'ordre et des audits internes ayant couvert des aspects liés à l'intégrité des données électroniques générées au laboratoire de contrôle qualité

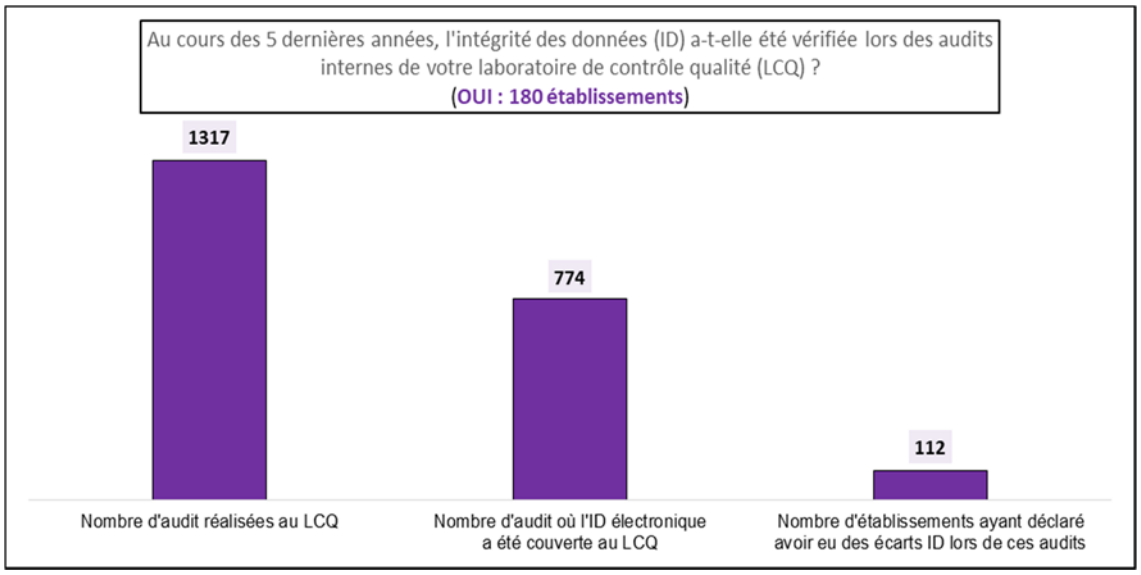
Le nombre et les résultats des inspections internationales, des audits clients ou donneurs d'ordre, ainsi que des audits internes couvrant l'intégrité des données (ID) électroniques générées par les laboratoires de contrôle qualité sont présentés dans les graphiques 5, 6 et 7.



Graphique 5



Graphique 6



Graphique 7

Ces réponses montrent que le pourcentage de vérification de l'intégrité des données électroniques au laboratoire de contrôle qualité est assez homogène entre les inspections effectuées par des autorités internationales (66,9% soit 238 fois sur les 356 inspections réalisées), les audits externes (61,8% soit 2415 fois sur les 3906 audits externes réalisés) et les audits internes (58,8% soit 774 fois sur les 1317 audits internes réalisés).

De plus, lors des inspections réalisées par des autorités internationales au laboratoire de contrôle qualité, 32,7% des établissements (soit 37 sur les 113 établissements inspectés) ont signalé avoir eu des écarts sur l'intégrité des données électroniques. Cependant, il a été observé que ce pourcentage a été plus élevé pour les audits externes et les audits internes soit respectivement à 57,2% (soit 115 sur les 201 établissements audités) et 62,2% (soit 112 sur les 180 établissements audités).

Enfin, ces établissements ont également communiqué avoir eu, en plus des écarts classés « Autres » :

- 30 écarts « Majeurs » ou « Critiques » lors des inspections menées par des autorités internationales ;
- 6 écarts « Critiques » et 291 écarts « Majeurs » lors des audits externes ;
- 9 écarts « Critiques » et 251 écarts « Majeurs » lors des audits internes.

Deux facteurs peuvent notamment expliquer ces différences de résultats observées en termes de nombre d'écarts formulés entre les inspections menées par des autorités internationales et les audits (externes et internes) réalisés :

- le nombre important d'audits externes réalisés au laboratoire de contrôle qualité (2414) ;
- pour les audits internes, la connaissance qu'ont les établissements de leurs points faibles concernant l'intégrité des données électroniques.

2.1.3. Etat des lieux, problème rencontrés et moyens mis en œuvre pour assurer la conformité aux exigences réglementaires des données électroniques générées dans les laboratoires de contrôle qualité

Les réponses des établissements aux questions posées sont présentées dans le tableau ci-dessous. Ces questions ont été regroupées comme suit :

A- Nombre de systèmes informatisés, y compris les systèmes autonomes ;
B- Difficultés de compréhension des exigences réglementaires ;
C- Activités sous-traitées ;
D- Remplacement et mise à jour des systèmes informatisés ;
E- Journal d'audit (dit « audit trail ») ;
F- Formation et augmentation des ressources ;
G- Système de gouvernance des données ;
H- Processus d'alerte.

<table>
<tr><th>Question</th><th>Réponses</th></tr>
<tr><td colspan="2">A- Nombre de systèmes informatisés, y compris les systèmes autonomes</td></tr>
<tr><td rowspan="3">1- Quel est le nombre de systèmes informatisés (pilotés par un logiciel spécifique) utilisés au laboratoire de contrôle qualité ?

• Existe-t-il des systèmes informatisés autonomes ?

Si oui, quel est le nombre des systèmes autonomes dont vous disposez ?</td><td>Nombre total pour l'ensemble des établissements = 3219
[Moyenne ~ 13,5 ; Ecart-type (Dispersion des réponses par rapport à leur moyenne) ~ 18,4]</td></tr>
<tr><td> 
</td></tr>
<tr><td>Nombre total pour l'ensemble des établissements : 1321
[Moyenne ~ 8,1 ; Ecart-type ~ 13,0%]</td></tr>
<tr><td colspan="2">Commentaire (Question 1) : La réponse à cette question indique que la majorité des établissements (68%) utilisent des systèmes informatisés autonomes dans leurs laboratoires de contrôle qualité.

Une analyse approfondie des réponses des opérateurs a montré que sur un total de 3219 systèmes informatisés utilisés dans les laboratoires des établissements ayant répondu à cette enquête, 1321 (41,0%) sont des systèmes autonomes. Cette évaluation n'a pas permis de démontrer une corrélation entre la taille du laboratoire de contrôle qualité et le nombre de systèmes informatisés autonomes utilisés.</td></tr>
</table>

Risque(s) associé(s) :

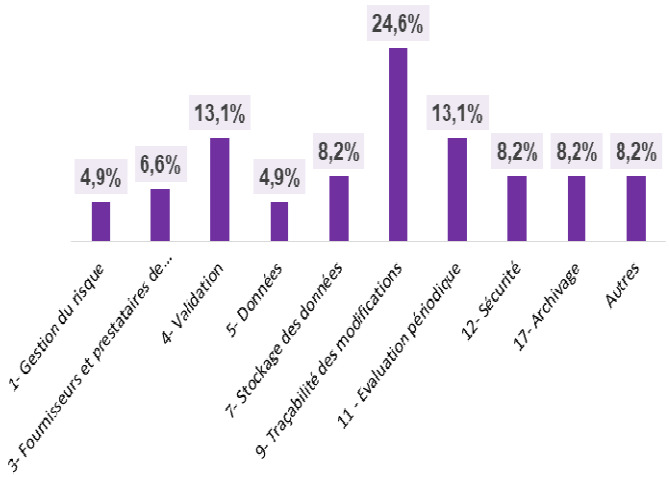
L'utilisation de systèmes informatisés autonomes peut présenter notamment des risques significatifs en termes de :

- perte de données ;
- carences dans les mesures de sécurité, car ils ne bénéficient pas des mêmes protections que les environnements connectés au réseau. Cela inclut notamment l'absence de politiques de gestion centralisée et de mises à jour continues. Ces lacunes peuvent entraîner une mauvaise gestion des identifiants et des mots de passe uniques, rendant ces systèmes vulnérables à des manipulations non autorisées.

B- Difficultés de compréhension des exigences réglementaires

2- Avez-vous rencontré des difficultés dans la compréhension de certaines exigences en matière d'intégrité des données électroniques ?

Si oui, préciser dans quelle(s) section(s) de l'annexe 11 des BPF ?



Graphique 8

Commentaire (Question 2) : La réponse à cette question a montré que 25,0% des établissements ont eu des difficultés à comprendre certaines parties de l'annexe 11 "Systèmes informatisés" des BPF. Les chapitres concernés dans cette annexe sont présentés sur le graphique 8.

Certains établissement ont rencontré des difficultés pour :

1. comprendre la conception et l'architecture de leurs systèmes informatisés ;
2. mettre en place une gestion du risque appliquée tout au long du cycle de vie du système informatisé ;

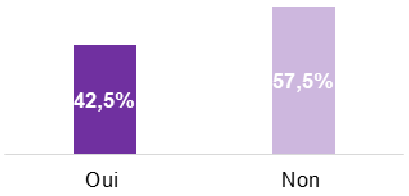
3. évaluer les fournisseurs de systèmes informatisés et établir des contrats avec eux ;
4. mettre en œuvre des « audits trails » (séquence d'analyse et système) et à fixer une fréquence de revue déterminée sur la base d'une évaluation des risques ;
5. identifier un administrateur indépendant du service utilisateur pour les systèmes informatisés du laboratoire de contrôle qualité, en particulier pour les petites structures ;
6. minimiser les risques liés à l'utilisation des systèmes autonomes ;
7. comprendre les attentes en termes de sauvegarde de données et de validation des systèmes informatisés ;
8. comprendre les attentes des autorités en termes de numérisation des "originaux" papiers.

Risque(s) associé(s) :

Les difficultés rencontrées dans la compréhension des différentes exigences de l'annexe 11 (voir graphique 8) peuvent avoir des conséquences majeures sur les pratiques de gestion des données électroniques générées dans les laboratoires de contrôle qualité. Ces pratiques sont nécessaires afin d'assurer la fiabilité et la traçabilité des données, et tout manquement majeur à ces exigences peut potentiellement affecter la sécurité des patients.

C- Activités sous-traitées

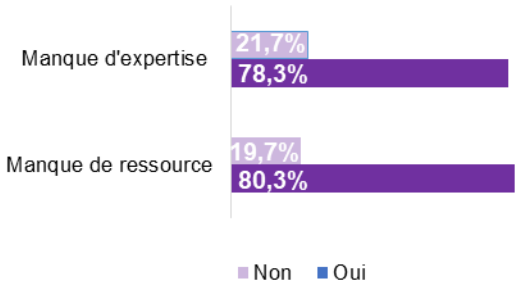
3- Avez-vous fait appel à des consultants pour l'élaboration et/ou l'exécution de vos plans de remédiation afin d'assurer la conformité des systèmes informatisés du laboratoire de contrôle qualité ?



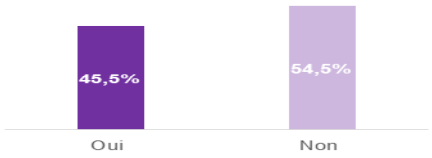
Si oui, expliquez la(es) raison(s) principale(s) pour lesquelles vous avez fait appel à des consultants (*Réponse à choix multiples*) :

a) Manque d'expertise sur la thématique d'intégrité des données électroniques et/ou sur la gestion des systèmes informatiques et réseaux ?

b) Manque de ressources ?



4- Avez-vous fait appel à un prestataire externe pour le support informatique ?

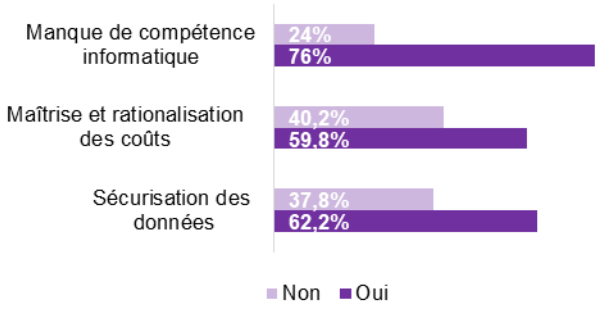


Si oui, expliquez la(es) raison(s) principale(s) pour laquelle(lesquelles) cette activité a été externalisée (*Réponse à choix multiples*) :

a) Manque de compétences informatique ?

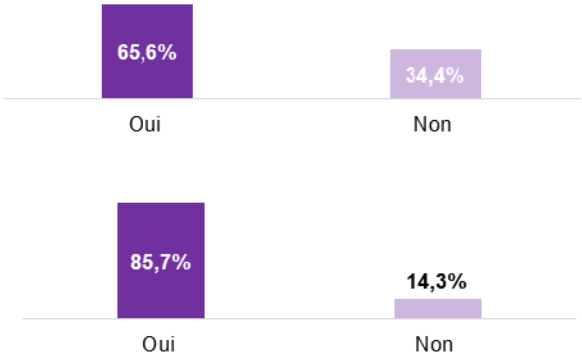
b) Maîtrise et rationalisation des coûts ?

c) Sécurisation des données ?



- Votre prestataire externe possède-t-il des droits administrateur à vos systèmes informatisés ?

- Cet administrateur système est-il formé à la bonne gestion des données électroniques ?



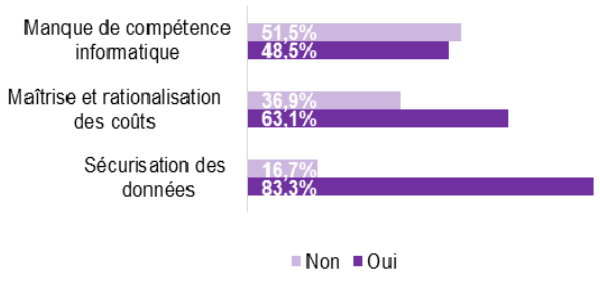
5. Avez-vous confié tout ou partie du processus de sauvegarde de vos données électroniques critiques à un prestataire extérieur ?

Si oui, expliquez la(es) raison(s) principale(s) pour lesquelles cette activité a été externalisée :

a) Manque de compétences informatiques sur le site ?

b) Maîtrise et rationalisation des coûts ?

c) Sécurisation des données ?

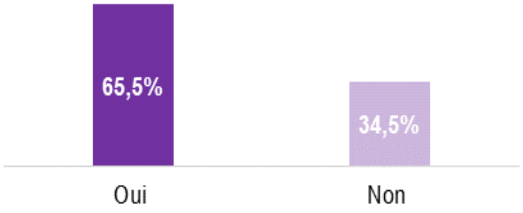


Commentaire (Questions 3, 4 et 5) : Ces réponses montrent que les opérateurs font appel à des prestataires externes pour le support informatique (45,5%) et à des consultants (42,5%) pour élaborer et/ou mettre en œuvre des plans de remédiation liés aux systèmes informatisés du laboratoire de contrôle qualité. Les raisons principales qui ont incité les opérateurs à choisir la sous-traitance sont le manque de compétences et d'expertise en gestion des systèmes informatisés, ainsi que le manque de ressources. De plus, 30,6% d'entre eux ont externalisé la sauvegarde des données électroniques critiques, principalement pour la sécurisation de leurs données (83,3%).

Risque(s) associé(s) :

L'externalisation peut avoir des avantages tels que l'accès à une expertise spécialisée et la réduction des coûts opérationnels. Cependant, elle comporte également des risques significatifs si des mesures particulières n'ont pas été mises en place. Ces risques incluent une dépendance accrue à des fournisseurs externes au support informatique ou des consultants pour gérer des problèmes liés à l'intégrité des données informatisées, particulièrement si des efforts de formation ne sont pas déployés au sein des établissements pour renforcer les compétences de l'organisation dans ce domaine. De plus, confier la sauvegarde des données critiques à un tiers peut représenter une menace de perte de données, si des mesures de sécurité appropriées ne sont pas en place et vérifiées régulièrement par le donneur d'ordre.

D- Remplacement et mise à jour des systèmes informatisés

6. Dans le cadre de la mise en conformité de vos systèmes informatisés avec l'annexe 11 des BPF, avez-vous remplacé des équipements / logiciels du laboratoire de contrôle qualité ?	
Si oui, quel est le nombre des équipements impactés ?	Nombre total des équipements pour l'ensemble des établissements : 1097 ; [*Moyenne ~ 7,0 ; Ecart-type ~ 12,8*]
• Avez-vous rencontré des problèmes particuliers dans l'identification de fournisseurs/systèmes informatisés conformes aux exigences de l'annexe 11 ?	
Préciser :	Voir le commentaire relatif aux questions n° 6, 7 et 8.

7. Dans le cadre de la mise en conformité de vos systèmes informatisés avec l'annexe 11 des BPF, avez-vous réalisé des montées de version des logiciels utilisés pour le pilotage des équipements du laboratoire de contrôle qualité ?	
• Quel est le nombre de logiciels ayant fait l'objet d'une montée de version ?	Nombre total des logiciels pour l'ensemble des établissements : 683 [*Moyenne ~ 4,2 ; Ecart-type ~ 9,4*]
• Quelle est la nature des équipements impactés ?	Les équipements les plus cités (par ordre décroissant) sont les suivants : spectrophotomètres (UV-Visible / Infrarouge), chromatographes (CLHP, CPG), Titrateurs potentiométriques, Titrateurs, Karl Fisher, spectrophotomètre d'absorption atomique, lecteurs de plaques (dosage des endotoxines bactériennes), Dissolutests et analyseurs COT (Carbone Organique Total).
8. Dans le cadre de la mise en conformité de vos systèmes informatisés avec l'annexe 11 des BPF, avez-vous augmenté la capacité de stockage serveur(s) ou changé de serveur(s) ?	

Commentaire (Questions 6, 7 et 8) : Dans le cadre du processus de mise en conformité des systèmes informatisés du laboratoire de contrôle qualité avec l'annexe 11 des BPF, environ 65% des établissements ont répondu avoir changé des équipements et/ou mis à jour les logiciels utilisés pour piloter ces équipements.

De plus, environ 35% ont signalé avoir rencontré des problèmes particuliers dans l'identification des fournisseurs de systèmes informatisés conformes aux exigences de l'annexe 11 des BPF pour les raisons principales suivantes :

1. Certains interlocuteurs commerciaux des fournisseurs peinent à comprendre les attentes concernant l'intégrité des données en raison d'une connaissance

insuffisante des exigences de l'annexe 11 des BPF. De plus, certains fournisseurs déclarent que leurs systèmes informatisés sont conformes à l'annexe 11, mais cette affirmation n'est pas toujours fondée ;

2. Il est parfois difficile, voire impossible, de trouver des systèmes informatisés qui répondent entièrement aux exigences de l'annexe 11 des BPF ;
3. Les fournisseurs d'équipements pour les analyses biologiques et microbiologiques ne prennent pas toujours en compte les exigences de l'annexe 11 des BPF, car la plupart de leurs clients, notamment les laboratoires d'analyses biologiques, ne sont pas tenus de respecter cette réglementation.

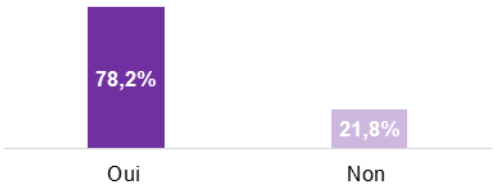
Enfin, 53,2% des établissements ont mentionné avoir augmenté la capacité de stockage de leurs serveurs ou effectué des remplacements de serveurs. Cette évolution est notamment due à l'installation de nouveaux systèmes informatisés ou à la montée en version des logiciels pilotant les équipements existants du laboratoire de contrôle qualité. Cela nécessite généralement une mise en réseau, ce qui requiert un besoin plus important d'espace de stockage.

Risque(s) associé(s) :

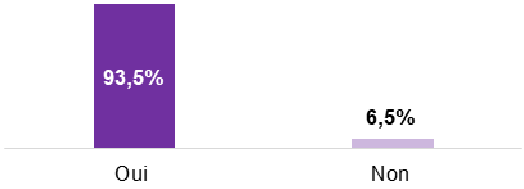
Un risque important sur la fiabilité des données persistera si le changement de ces équipements et de leurs logiciels de pilotage n'est pas maitrisé, notamment si les spécifications utilisateurs (« *Users Requirements Specifications* » - URS) n'ont pas été correctement définies dès le départ et que le niveau de validation n'est pas adapté à la criticité du système informatisé.

E- « Audit trails »

9. Les « audit trails » des systèmes informatisés du laboratoire de contrôle qualité sont-ils réalisés selon une fréquence prédéfinie ?



Si oui, avez-vous défini des fréquences pour les différents « audit trails » (système, séquence d'analyse, etc.) ?



- Quel est la fréquence de réalisation de ces « audit trails » ?

Voir le commentaire relatif à la question n°9.

Commentaire (Question 9) :

Les fréquences d' « audit trails » définies par les établissements sont :

- pour les « audit trails » séquence d'analyse : environ 56% des établissements indiquent que cet audit trail est réalisé à chaque analyse lors de la vérification des résultats avant certification/libération de(s) lot(s) concerné(s) ;
- pour les « audit trails » système : la majorité des établissements indique que cet audit trail est réalisé à une fréquence semestrielle ou annuelle.

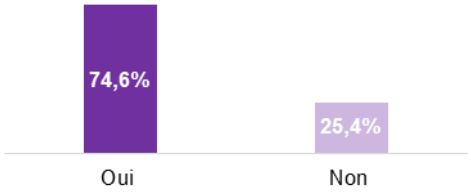
Les autres réponses à cette question varient considérablement d'un établissement à l'autre. Dans certains cas, ces fréquences sont déterminées sur la base d'une analyse de risque, tandis que dans d'autres cas, elles sont fixées de manière aléatoire.

<u>Risque(s) associé(s)</u> :

Une fréquence d' «audit trail » définie sans une évaluation de risques peut ne pas être adaptée pour détecter dans un temps opportun des problèmes critiques d'intégrité des données.

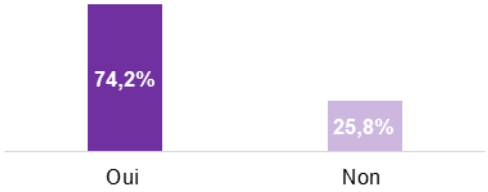
F- Formation et augmentation des ressources

10. Une formation sur les principes de gestion des données électroniques a-t-elle été dispensée au personnel du laboratoire de contrôle qualité ?



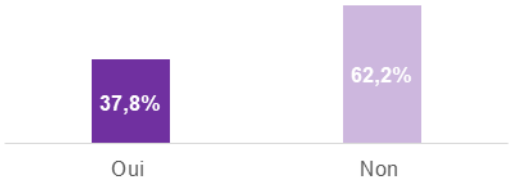
- Avez-vous fait appel pour ce type de formation à un prestataire externe ?

- Cette formation doit-t-elle être renouvelée sur une base régulière ?



- Quel est le nombre de formations réalisées sur cette thématique lors des 5 dernières années ?

Nombre total de formation : 866
[*Moyenne ~ 4,9 ; Ecart-type ~ 18,4*]

11. La gestion de l'intégrité des données a-t-elle nécessité une création de poste(s) au sein de votre organisation ?	
Si oui, Quel est le nombre de poste(s) créé(s) au niveau de votre établissement ? de votre groupe le cas échéant ?	Nombre total de postes : 108 [*Moyenne ~ 1,2 ; Ecart-type ~ 1,2*]

Commentaire (Questions 10 et 11) : 25,4% des établissements ont répondu ne pas avoir dispensé de formation sur les principes de gestion des données électroniques au personnel du laboratoire de contrôle qualité. De plus, 25,8% des établissements ont mentionné qu'ils n'ont pas prévu de renouveler ce type de formation de manière régulière.

Une analyse approfondie des réponses fournies a montré qu'environ 83% des établissements ayant eu recours à des prestataires externes pour ces formations prévoyaient de les renouveler régulièrement.

Enfin, 37,8% des établissements ont indiqué que la gestion de l'intégrité des données avait exigé la création de nouveaux postes au sein de leur organisation.

Risque(s) associé(s) :

Un personnel non formé ne maitrise pas bien les exigences relatives à l'intégrité des données électroniques. En conséquence, les employés peuvent commettre des erreurs involontaires ou manipuler des données intentionnellement, ce qui compromet l'intégrité des résultats. Des données incorrectes ou incomplètes peuvent entraîner de mauvaises décisions notamment lors de la certification/libération des produits, ce qui peut compromettre la sécurité des patients ;

Un prestataire de formation n'ayant pas d'expertise dans le domaine de l'intégrité des données peut proposer une formation insuffisante ou inexacte. De plus, les prestataires externes peuvent offrir des formations standard qui ne répondent pas précisément aux besoins spécifiques de l'établissement.

G- Système de gouvernance des données

12. Avez-vous mis en œuvre un « système de gouvernance des données » permettant de définir, prioriser et communiquer vos activités de gestion des risques liées à l'intégrité des données ?	

Commentaire (Question 12) : 40, 9% des établissements ont répondu ne pas avoir mis en œuvre un système de gouvernance des données (cf. définition dans le document : *PIC/S Guidance*, bibliographie réf. [4]).

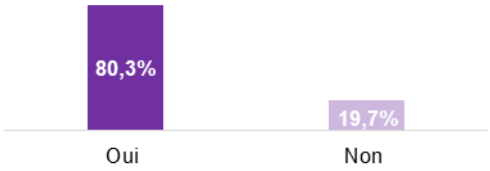
« *La mise en place de ce système devrait garantir que les données sont enregistrées, traitées et utilisées de manière à assurer leur intégrité tout au long de leur cycle de vie. Un système de gestion des données mature doit adopter une approche de gestion des risques qualité, avec une évaluation continue et des mesures proportionnées pour réduire les risques résiduels à travers l'organisation dans tous les domaines du système qualité, tout au long du cycle de vie du système informatisé* ».

Risque(s) associé(s) :

Ne pas mettre en place de système de gouvernance des données risque de limiter le processus de maîtrise globale de l'intégrité des données électroniques uniquement à la seule conformité des systèmes informatisés de laboratoire aux exigences de l'Annexe 11 des BPF.

H- Processus d'alerte

13. Votre organisation dispose-t-elle d'un système ou processus formalisé permettant de notifier au responsable du management tout dysfonctionnement lié à l'intégrité des données afin d'enquêter sur les problèmes de qualité, le cas échéant ?



Commentaire (Question 13) : 19,7% des établissements ont répondu ne pas disposer d'un système ou d'un processus formel pour signaler au responsable du management tout problème lié à l'intégrité des données.

Risque associé :

La direction pourrait sous-estimer les problèmes d'intégrité des données, ce qui peut entraîner un manque de réactivité face à des problèmes graves pouvant mettre en cause la conformité des produits et ainsi entrainer une allocation insuffisante des ressources nécessaires à leur résolution telle que la formation du personnel à la bonne utilisation des systèmes, la formation aux exigences réglementaires et le soutien en moyens financiers pour la mise en conformité des systèmes informatisés.

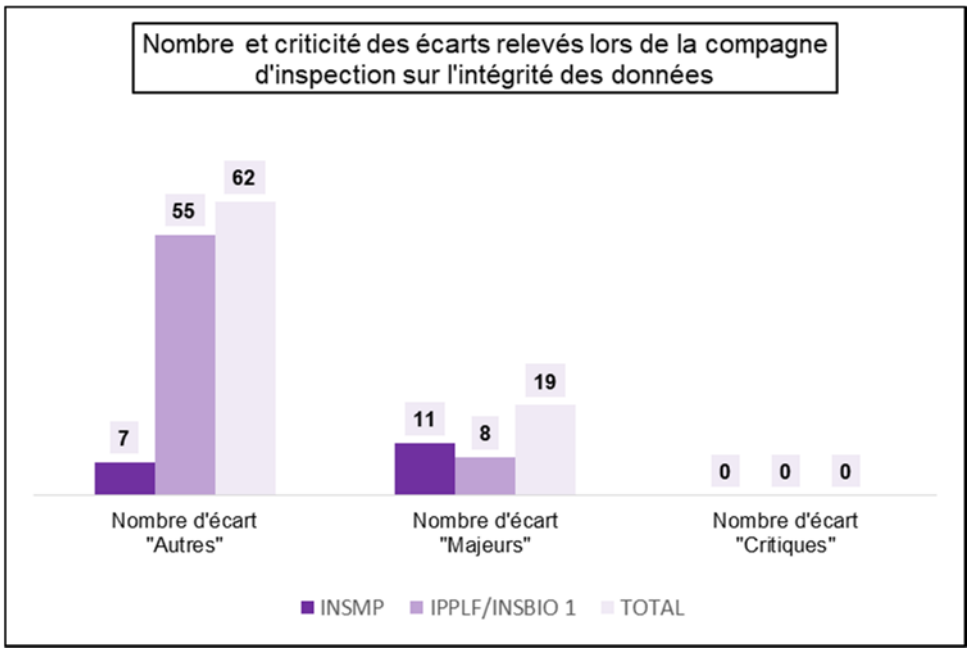
2.2. Données recueillies lors de la campagne d'inspections réalisées par l'ANSM

Les informations et données collectées lors de cette campagne d'inspections viennent compléter les résultats de l'enquête conduite par l'ANSM. Cette campagne d'inspections qui a été menée entre juillet 2019 et juillet 2022 auprès de 27 établissements de production et de contrôle de substances actives, de médicaments

à usage humain (médicaments chimiques et biologiques) a permis d'évaluer la conformité des établissements inspectés à la réglementation actuelle en matière d'intégrité des données électroniques au laboratoire de contrôle qualité. Elle a également permis de conduire des entretiens approfondis avec le personnel de ces établissements pour évaluer leur compréhension des exigences réglementaires et des attentes de l'ANSM à cet égard.

2.2.1. Présentation générale des résultats d'inspection, mettant en évidence le nombre et la criticité des écarts par domaine d'inspection

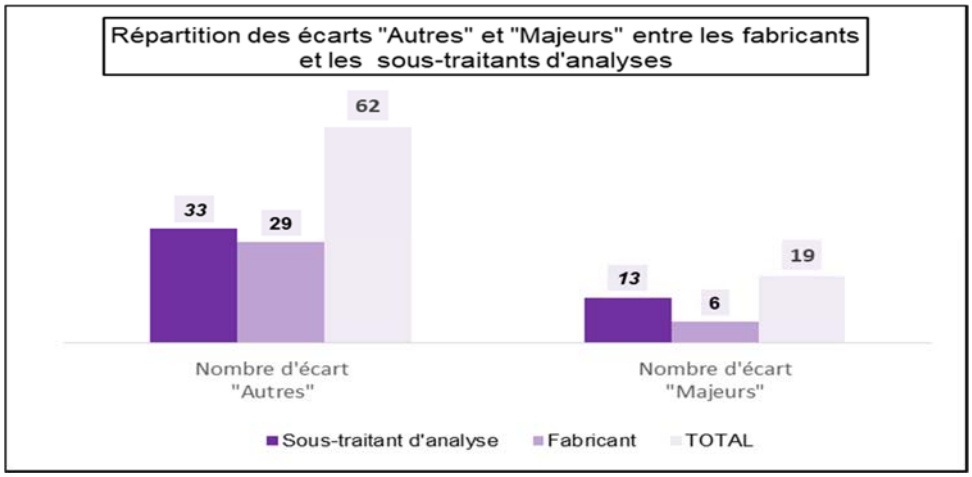
La synthèse des résultats obtenus lors de cette campagne d'inspections a mis en évidence les constats suivants : parmi les 62 écarts « Autres » formulés, 55 d'entre eux (88.7%) ont été observés lors des inspections des établissements pharmaceutiques réalisées par les pôles d'inspection des produits biologiques [INSBIO1] et d'inspection des produits pharmaceutiques et lutte contre les fraudes [IPPLF] (12 fabricants de médicaments et 6 sous-traitants d'analyses), tandis que les inspections réalisées par le pôle d'inspection des matières premières [INSMP] (5 fabricants de substances actives ; 4 sous-traitants d'analyses (dont 3 ayant un statut d'établissement pharmaceutique) ont relevés 7 écarts (11,3%).
Sur 18 écarts « Majeurs » relevés lors de ces inspections, 11 ont été observés lors des inspections réalisées par le pole INSMP (57,9%), et 8 (42,1%) lors des inspections réalisées par les pôles d'inspection INSBIO1 et IPPLF. Aucun écart critique n'a été identifié lors de cette campagne d'inspections (voir graphique 9).



Graphique 9

La comparaison des résultats d'inspection entre les établissements fabricants de substances actives et les établissements fabricants de médicaments à usage humain (médicaments chimiques et biologiques) n'a pas permis de démontrer de différence significative. Cependant lors de la comparaison des résultats obtenus entre les sous-traitants d'analyse et les fabricants de substances actives et médicaments, il a été constaté que bien que le nombre de fabricants inspectés soit nettement supérieur à celui des sous-traitants d'analyses (17 établissements versus 10), ces derniers ont

eu deux fois plus d'écarts « Majeurs » que les fabricants et un nombre d'écarts « Autres » légèrement plus élevé (voir graphique 10).

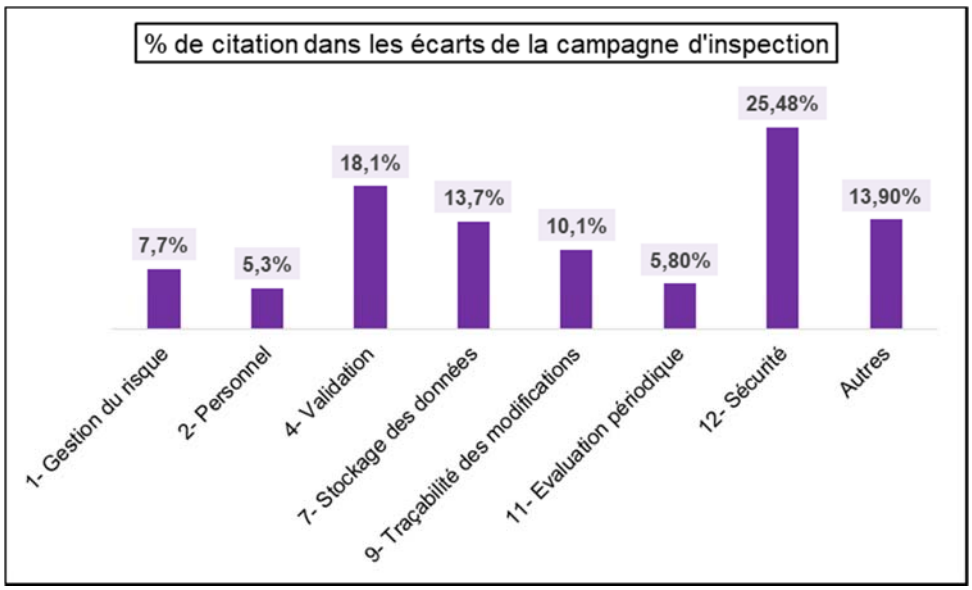


Graphique 10

Il est à noter que les 13 écarts « Majeurs » relevés chez les sous-traitants d'analyses étaient répartis sur 8 établissements distincts, représentant ainsi 80 % des établissements inspectés. De plus, les 33 écarts « Autres » ont été répartis entre les 10 établissements sous-traitants, chacun ayant entre un et six écarts « Autres ».

2.2.2. Identification des domaines de défaillance et analyse de tendance

La campagne d'inspections a révélé plusieurs manquements significatifs vis-à-vis des différents chapitres de l'Annexe 11 des BPF, avec des tendances claires se dégageant dans plusieurs domaines. Comme le montre le graphe ci-dessous (graphique 11), la majorité des écarts ont été relevés pour les chapitres n° 1, 2, 4, 7, 9, 11 et 12. Ces tendances sont très comparables à celles obtenues lors de l'enquête envoyée aux opérateurs. Les résultats mettent en évidence les domaines clés nécessitant une attention particulière de la part des opérateurs de l'industrie pharmaceutique pour garantir la conformité des systèmes informatisés à la réglementation en vigueur :



Graphique 11

2.2.3. Analyse des domaines problématiques

Les défaillances mentionnées dans le graphique 11 sont analysées dans ce paragraphe, avec des exemples d'écarts relevés, tout en soulignant les risques correspondants.

2.2.3.1. Gestion du risque

La réglementation en vigueur stipule que la gestion des risques utilisant les principes de l'ICH Q9 doit être appliquée tout au long du cycle de vie des systèmes informatisés, en prenant en compte la sécurité des patients, l'intégrité des données et la qualité du produit. Cependant, lors de cette campagne d'inspections, il a été constaté qu'environ un tiers des établissements inspectés ne maitrisaient pas pleinement le concept de cycle de vie des données et que parfois leur compréhension se limitait uniquement à énumérer quelques étapes de ce cycle de vie. De plus, pour ce type d'établissements, il a été observé l'absence de procédure définissant la méthode d'évaluation de la criticité de chaque système informatisé ainsi que l'absence d'inventaire pour ces systèmes.

A titre d'exemples, les observations les plus marquantes relevées sur cette thématique sont reprises ci-dessous :

- ***Exemple 1*** : « L'évaluation de chaque étape du cycle de vie des données électroniques du laboratoire de contrôle qualité n'a pas été effectuée. Par conséquent, les risques potentiels associés à chaque étape de ce cycle de vie n'ont pas été identifiés (avec pour objectif de les minimiser). A titre d'exemple, le transfert manuel des données brutes générées lors des analyses par CLHP, CPG et UV vers des fichiers Excel® pour réaliser les calculs de teneur selon les monographies en vigueur n'a pas été évalué » ;
- ***Exemple 2*** : « L'établissement n'a pas effectué un état des lieux détaillé pour évaluer la conformité des systèmes informatisés utilisés au laboratoire de contrôle qualité avec les exigences réglementaires en vigueur. Par conséquent, tous les risques associés à chaque système informatisé ainsi que les actions correctives et préventives nécessaires à les réduire n'ont pas été identifiés ni formalisés » ;
- ***Exemple 3*** : « Une analyse de risque a été réalisée pour chacun de ces équipements afin de déterminer leur conformité aux exigences de l'annexe 11 des bonnes pratiques de fabrication […]. Les manquements identifiés lors de ces analyses de risque ont permis de conclure que ces équipements n'étaient pas conformes à la réglementation en vigueur et leur criticité a été qualifiée de « haute ». Cependant, à ce jour, l'établissement n'a pas mis en place d'actions compensatoires dans l'attente de l'identification et de la mise en place d'actions correctives adéquates ».

2.2.3.2. Personnel

La qualification du personnel à travers des formations appropriées sur les systèmes informatisés est nécessaire afin de garantir la fiabilité des résultats générés et la sécurité des opérations réalisées. Chaque niveau de formation doit être ajusté en fonction des responsabilités attribuées à chaque employé. Ce type de formations est étroitement lié aux formations concernant le cycle de vie des données et au maintien de l'intégrité des données.

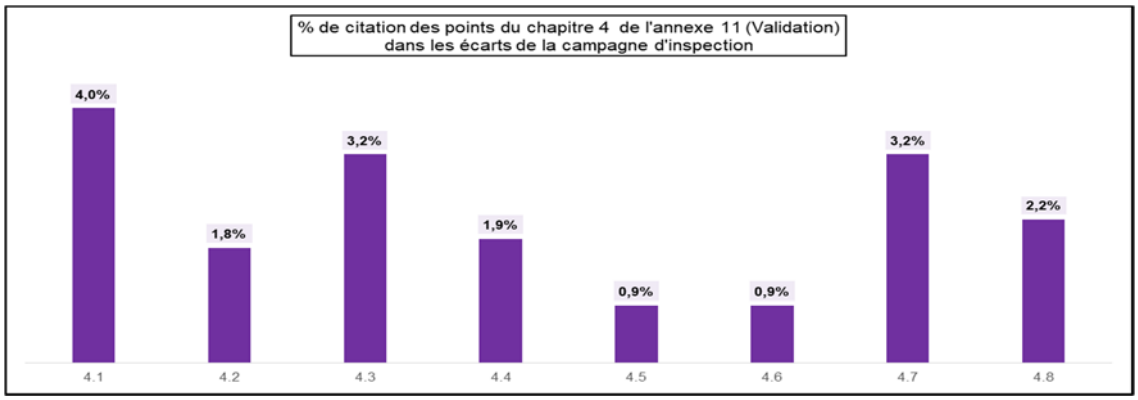
Lors de cette campagne d'inspections, il a été observé que presque tous les établissements (sauf deux) ont déployé au moins une formation sur l'intégrité des données à l'ensemble de leurs employés.

A titre d'exemples, les observations les plus marquantes relevées sur cette thématique sont reprises ci-dessous :

- ***Exemple 1*** : « La formation sur l'intégrité des données n'a pas été dispensée à toutes les personnes concernées. Par exemple, un administrateur des systèmes informatisés n'a pas été identifié comme étant une personne devant suivre cette formation. De plus, aucune évaluation n'a été réalisée pour mesurer l'efficacité de cette formation » ;
- ***Exemple 2*** : « La formation sur l'intégrité des données se limitait à expliquer la signification de l'acronyme ALCOA » ;
- ***Exemple 3*** : « La formation sur l'intégrité des données s'est principalement limitée aux données produites sur support papier ».

2.2.3.3. Validation

Les références du chapitre "4-Validation" de l'annexe 11 des BPF ont été mentionnées dans 18,1% des écarts identifiés lors de l'inspection. Le graphique 12 illustre la répartition des sous-chapitres de cette section « Validation » dans les écarts formulés lors de cette campagne d'inspections :



Graphique 12

Il a été observé que le niveau de validation des systèmes informatiques variait considérablement d'un établissement à l'autre. Cette différence résulte principalement de disparités en termes de compétences techniques, de ressources disponibles, de complexité des systèmes, de culture organisationnelle et d'exigences réglementaires relatives à l'industrie pharmaceutique.

A titre d'exemples, les observations les plus marquantes relevées sur cette thématique sont reprises ci-dessous :

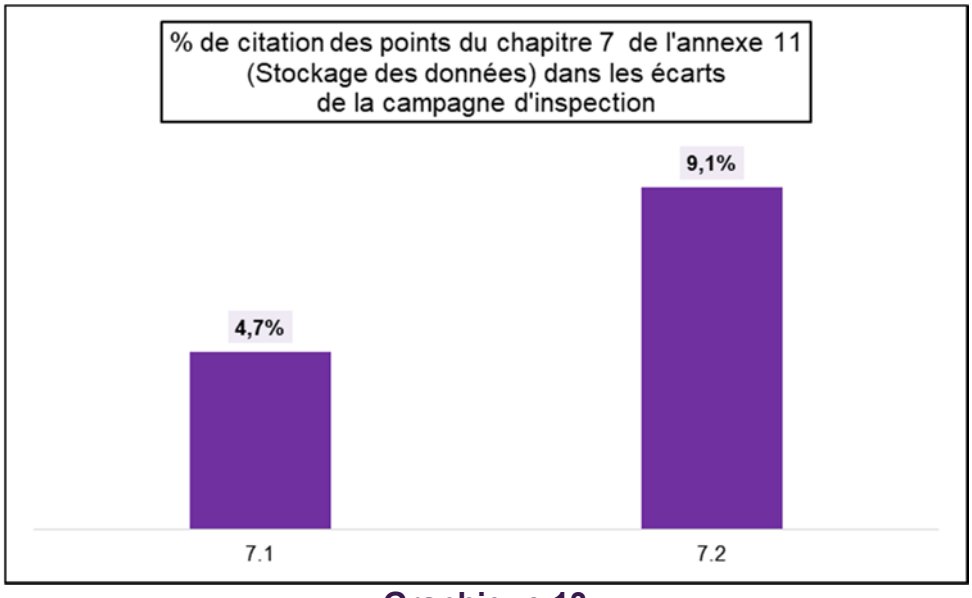
- ***Exemple 1*** : « L'établissement ne dispose pas de document maître de validation pour les systèmes informatisés qui mentionne à la fois le statut de validation de chaque système informatisé (QI, QO et QP) et les validations manquantes avec leurs dates prévisionnelles de réalisation » ;
- ***Exemple 2*** : « La validation des systèmes informatisés n'était pas basée sur une évaluation détaillée des risques à chaque phase critique du cycle de vie des données pour démontrer que les systèmes respectent les normes de sécurité et de fiabilité nécessaires. De plus, l'unité qualité n'est pas impliquée dans

l'approbation des protocoles et des rapports de validation des systèmes informatisés » ;

- ***Exemple 3*** : « L'établissement ne dispose pas d'une liste exhaustive d'inventaire des systèmes informatisés utilisés pour l'analyse et la gestion des données au sein du laboratoire de contrôle. De plus, il n'existe pas de documents décrivant les flux de données et les interfaces entre les différents systèmes informatisés utilisés au laboratoire de contrôle qualité » ;
- ***Exemple 4*** : « L'établissement n'a pas mis en place de procédure définissant comment déterminer la criticité de chaque système informatisé ni de schéma détaillé de mise en réseau afin de déterminer le niveau de validation requis pour chaque système » ;
- ***Exemple 5*** : « Plusieurs fonctionnalités tels que les profils d'utilisateurs, les « audit trails », la déconnexion automatique des utilisateurs après une période d'inactivité, les sauvegardes et les extractions de données n'ont pas été évaluées lors de la validation des systèmes informatisés » ;
- ***Exemple 6*** : « L'interface […] utilisée pour dupliquer les données analytiques vers un serveur de sauvegarde n'a pas été validée » ;
- ***Exemple 7*** : « Tous les systèmes informatisés ne sont pas régulièrement évalués pour confirmer qu'ils restent dans un état valide et qu'ils sont conformes aux BPF » ;
- ***Exemple 8*** : « Il n'y a pas de matrice de traçabilité disponible pour garantir que toutes les exigences identifiées dans les spécifications des besoins utilisateurs (URS) sont testées pour vérifier leur conformité » ;
- ***Exemple 9*** : « Les feuilles de calcul Excel® utilisées pour la détermination de la teneur […] au laboratoire de contrôle qualité n'ont pas été validées ».

2.2.3.4. Stockage des données

Les références du chapitre "7-Stockage des données" de l'annexe 11 des BPF ont été mentionnées dans 13,7% des écarts identifiés lors de l'inspection. Le graphique 13 décrit la répartition des sous-chapitres de cette section « Stockage des données » dans les écarts formulés lors de cette campagne d'inspections :



Graphique 13

Il a été observé lors de cette campagne d'inspections que les fréquences de sauvegarde des données des systèmes autonomes variaient considérablement d'un établissement à l'autre. Ces fréquences n'ont pas toujours été justifiées par une analyse de risque approfondie tenant compte des conséquences potentielles d'une perte de données et de métadonnées.

A titre d'exemple, les observations les plus marquantes relevées sur cette thématique sont reprises ci-dessous :

- ***Exemple 1*** : « L'exactitude des données sauvegardées, ainsi que la capacité à restaurer les données, n'ont pas été vérifiées pendant la validation des systèmes informatisés » ;
- ***Exemple 2*** : « La fréquence à laquelle les données générées par les systèmes autonomes sont sauvegardées n'a pas été établie sur la base d'une analyse de risque. De plus, les données électroniques produites par ces systèmes autonomes ne font pas l'objet d'une sauvegarde régulière » ;
- ***Exemple 3*** : « Les données issues de l'autoclave sont enregistrées sur une clé USB disponible pour l'ensemble du personnel. Cette pratique est inacceptable dans la mesure où ces données sont accessibles à l'ensemble du personnel et ne sont pas protégées contre d'éventuelles modifications » ;
- ***Exemple 4*** : « Le prestataire responsable de la sauvegarde des données électroniques du site n'est pas audité par […]. De plus, il n'existe aucun cahier des charges qualité signé avec ce prestataire » ;
- ***Exemple 5*** : « La prise de connaissance, par la société de prestation informatique […], de la procédure de gestion informatique, de sauvegarde et de la sécurité des données […] n'a pas pu être démontrée ».

2.2.3.5. Traçabilité des modifications

Lors de cette campagne d'inspections, il a été constaté que pour 5 établissements, les « audit trails » n'étaient pas effectués pour les systèmes informatisés des laboratoires de contrôle qualité. De plus, il a été observé que pour 6 autres établissements, les « audit trails » ont été mis en œuvre partiellement ; parmi ces établissements, 4 ne réalisent des « audits trails » que pour les systèmes chromatographiques.

A titre d'exemple, les observations les plus marquantes relevées sur cette thématique sont reprises ci-dessous :

- ***Exemple 1*** : « Il n'existe pas de procédure qui définit précisément, par qui, quand et comment les revues des « audit trails » projet et système doivent être réalisées pour les équipements, pilotés par des systèmes informatisés, autres que les chaines chromatographiques (par exemple, spectrophotomètre UV-Visible, spectrophotomètre Infrarouge etc…). De plus, aucun système n'a été mis en place (par exemple « checklist ») pour enregistrer ces revues » ;
- ***Exemple 2*** : « Pour l'ensemble des équipements, la réalisation des « audit trails » système n'est pas exigée par une procédure interne et ne fait pas l'objet d'une revue régulière » ;
- ***Exemple 3*** : « Les « audit trails » projet et système n'ont pas été vérifiés lors de la validation du système informatisé » ;
- ***Exemple 4*** : « A l'exception des logiciels validés utilisés pour le pilotage des chaines CLHP et CPG, la revue régulière de l'« audit trail » n'a pas été mise en place » ;
- ***Exemple 5*** : « L' « audit trail » n'est vérifié que sur la séquence d'injection

validé. Cependant, cette revue des « audit trails » ne tient pas compte du risque potentiel associé à la ré-analyse non autorisée de l'échantillon par l'analyste » ;

- ***Exemple 6*** : « Les systèmes informatisés n'intègrent pas des moyens de contrôle suffisants afin de prévenir tout accès ou toute modification de données sans autorisation (par exemple, l'utilisation d'un « audit trail ») » :
  a) Pour le spectrophotomètre IR n° […], l'« audit trail » est limité aux opérations : « Login », « Open application », « Initializing », «Scan n° analysis » et « Logout » ;
  b) Pour le spectrophotomètre UV n° […] : l'« audit trail » est limité aux opérations : « log on », « log off » et création de compte ;
  c) Pour les deux chaines CLHP […] n° […], les enregistrements d'« audit trail » sont supprimés tous les 5 jours. De plus, lors de cette inspection l'établissement n'était pas en mesure de démontrer que l'« audit trail » était activé sur ces systèmes chromatographiques » ;
- ***Exemple 7*** : « Dans le logiciel d'acquisition […] des données des chaines de CLHP, la fonctionnalité dite « audit trail » ne permet pas de tracer de manière suffisante toute modification ou suppression survenue lors des analyses. En effet :
  a) l'unique modification tracée est le renommage de pic de chromatogramme ;
  b) lors de l'impression de l' « audit trail » après une analyse, seuls les « audit trails » des analyses précédentes sont reportés. Il n'est pas possible de lire l'« audit trail » de l'analyse en cours ;
  c) enfin, il a été déclaré que l'ancienneté du logiciel ne permet pas d'améliorer l'état actuel de l'« audit trail » afin qu'il réponde aux exigences pharmaceutiques en vigueur » ;
- ***Exemple 8*** : « La revue des « audit trails » des chaines HPLC est réalisée uniquement à une fréquence annuelle et le risque associé à cette pratique n'a pas été évalué » ;
- ***Exemple 9*** : « L'« audit trail » du logiciel […] n'est pas disponible sous une forme intelligible » ;
- ***Exemple 10*** : « La revue de l'« audit trail » projet n'était pas formalisée » ;
- ***Exemple 11*** : « La revue de l'«audit trail » ne permet pas de détecter des intégrations manuelles de chromatogrammes. De plus, ces intégrations manuelles n'étaient pas non plus reportées sur le rapport d'analyse ».

2.2.3.6. Evaluation périodique

Lors de cette campagne d'inspections il a été observé que les systèmes informatisés n'étaient pas toujours périodiquement évalués. Cette évaluation n'était pas réalisée dans 9 établissements, tandis que dans 2 établissements, seule une partie de ces systèmes faisait l'objet d'une évaluation régulière.

A titre d'exemple, les observations les plus marquantes relevées sur cette thématique sont reprises ci-dessous :

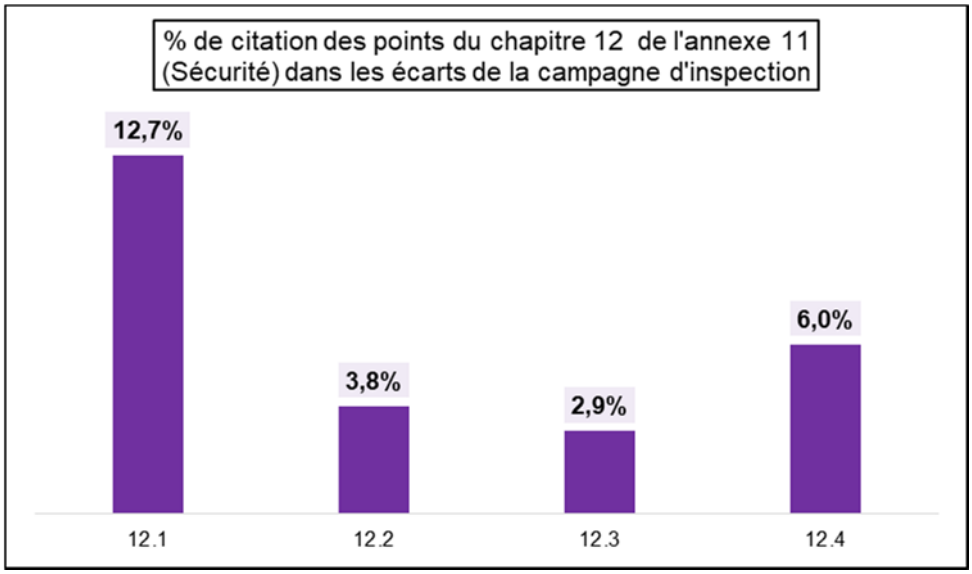
- ***Exemple 1*** : « De nombreux systèmes informatisés associés aux équipements du laboratoire de contrôle ne font pas l'objet d'une revue périodique afin de s'assurer du maintien de leur état validé » ;
- ***Exemple 2*** : « Afin de maintenir l'état validé de l'ensemble des systèmes informatisés utilisés sur le site et ayant un impact sur la qualité des produits, l'établissement a défini une fréquence de revue à 1 an. Cependant il a été

constaté que cette fréquence n'est pas toujours respectée et ceci sans justification ».

2.2.3.7. Sécurité

Lors de cette campagne d'inspections, il a été constaté que pour 6 établissements, les profils d'accès aux systèmes informatisés n'étaient pas correctement définis.

Les références du chapitre "12-Sécurité" de l'annexe 11 des BPF ont été mentionnées dans environ 25,5% des écarts formulés lors des inspections. Le graphique 14 illustre la répartition des sous-chapitres de cette section « Sécurité » dans les écarts formulés lors de cette campagne d'inspections :



Graphique 14

A titre d'exemple, les observations les plus marquantes relevées sur cette thématique sont reprises ci-dessous :

- ***Exemple 1*** : « La gestion des profils d'utilisateurs et de droit d'accès aux différentes fonctionnalités des systèmes informatisés n'est pas formalisée en termes de création, modification et suppression de compte. De plus, des vérifications périodiques n'ont pas été mises en place pour garantir un accès approprié aux utilisateurs » ;
- ***Exemple 2*** : « Il n'a pas été défini de niveaux d'accès personnalisés pour les administrateurs du logiciel […]. Ainsi, seul un compte générique est disponible pour tous les administrateurs ce qui ne permet pas d'identifier la personne concernée » ;
- ***Exemple 3*** : « Il a été constaté que le technicien […] qui n'a pas été habilité aux analyses CLHP, détient les droits d'accès correspondants au niveau du système de pilotage des chaines chromatographiques […] » ;
- ***Exemple 4*** : « Les techniciens du laboratoire de contrôle qualité utilisent le compte « Administrateur » pour accéder aux chaînes de chromatographie liquide haute performance » ;
- ***Exemple 5*** : « Tous les techniciens du laboratoire utilisent un identifiant et un mot de passe uniques pour accéder, via le profil « Analyst », aux deux chaînes CLHP […]. De plus, il a été noté que ce profil permet aux techniciens de supprimer diverses données telles que des méthodes et des données, par exemple « *Delete*

instrumental method », « *Delete processing method* », « *Delete reporting method* », « *Delete sample set method* », « *Delete method set* », « *Delete calibration curves* », « *Delete results* », etc. ».

- ***Exemple 6*** : « L'accès au logiciel […] n'était pas muni d'un système de déconnexion automatique ».

3. RECOMMANDATIONS

Ce paragraphe n'a pas pour objectif d'exposer l'ensemble des exigences réglementaires, mais il fournit des recommandations et expose certains points de vigilance en lien avec des manquements identifiés lors de la campagne d'inspections et lors de l'exploitation des résultats de l'enquête :

- L'emploi des systèmes informatisés autonomes utilisés pour le pilotage des équipements du laboratoire de contrôle qualité est encore assez répandu dans les laboratoires de contrôle qualité. Afin de minimiser les risques liés à leur utilisation, il est conseillé de tenir compte des recommandations suivantes :
  - Bien que ces systèmes puissent se connecter à un serveur, il est souvent constaté qu'ils fonctionnent de manière indépendante, avec des intervalles de sauvegarde de données très variables selon les établissements. Il est donc nécessaire de mettre en place des sauvegardes régulières pour minimiser les risques de perte de données liés à leur utilisation. Les fréquences de ces sauvegardes doivent être déterminées à partir d'une analyse de risque formalisée tenant compte de l'impact potentiel de perte de données.
    Il est évident que si ces sauvegardes sont moins fréquentes, le risque de perte d'un grand volume de données, en cas de défaillance irréversible du matériel (Hardware), est important.
    Cette perte éventuelle de données informatisées peut compromettre sérieusement la capacité des établissements à mener des investigations approfondies pour identifier les causes racines notamment en cas de problèmes particulièrement graves de santé publique. Dans ce cas l'établissement peut ne pas être en mesure de fournir les preuves nécessaires aux autorités pour attester que les analyses ont été effectuées ;
  - De plus, certains de ces systèmes autonomes pouvant ne pas avoir de mesures de sécurité telles que l'authentification par identifiant et mot de passe et/ou d'« audit trail », il est nécessaire de mettre en place un système permettant d'assurer la traçabilité des opérations effectuées sur ces systèmes afin de détecter toute activité non autorisée (par exemple, des registres papier ou électroniques pour enregistrer les opérations réalisées sur chaque système informatisé, des doubles vérifications pour les opérations critiques, etc.) ;

- L'externalisation des activités telles que le support informatique, la sauvegarde des données ou l'emploi de consultants pour l'élaboration des plans de remédiation est assez répandue dans le secteur pharmaceutique et l'appel à ce type de prestations n'est pas interdit par les BPF. Cependant, ces opérations de sous-traitance doivent être maitrisées et les établissements donneurs d'ordre doivent contrôler leurs prestataires afin de garantir l'intégrité

des données. Afin de minimiser les risques liés à leur utilisation, il est nécessaire de prendre, *a minima*, les précautions suivantes :

- Le processus de qualification des prestataires de services pour le support informatique et la sauvegarde des données devrait intégrer une évaluation de leur conformité aux exigences réglementaires en matière d'intégrité des données informatisées ;
- La sélection des consultants doit non seulement prendre en compte la vérification de leur maîtrise des BPF, mais aussi l'évaluation de leur expertise en systèmes informatisés ;
- L'externalisation de ces activités ne devrait pas dispenser les établissements de former leur personnel dans ces domaines. Ces formations sont nécessaires pour contrôler les services fournis par les prestataires lors des audits sur site par exemple ;

- La validation des systèmes informatisés doit au minimum inclure les fonctionnalités critiques de ces systèmes pour assurer l'intégrité des données, telles que la vérification des profils d'accès, l' « audit trail », ainsi que la sauvegarde et la restauration des données. Ces vérifications doivent être formalisées, par exemple au travers de fiches de test ;

- Lorsque les administrateurs des systèmes informatisés sont indépendants de l'unité qualité, leurs activités devraient être enregistrées et faire l'objet d'une vérification régulière par l'unité qualité. De plus, ces administrateurs devraient recevoir une formation à la bonne gestion des données ;

- Plusieurs établissements ont rencontré des difficultés pour interpréter certaines exigences réglementaires stipulées dans diverses sections de l'annexe 11 des BPF. Pour améliorer leur compréhension des exigences de cette annexe, il est fortement conseillé de se référer notamment aux guides et aux questions-réponses élaborés par les autorités de santé. Les références de ces documents (liste non exhaustive) sont mentionnées dans la section « Bibliographie » ;

- Le changement des équipements ou la montée en version des logiciels afin de répondre aux exigences de la réglementation en vigueur ne suffiront pas à garantir l'intégrité des données. Un système de gouvernance des données correctement mis en place, applicable tout au long du cycle de vie des données informatisées, est nécessaire pour assurer une utilisation efficace et efficiente de ces données. A titre d'exemple, un résultat erroné (non fiable) peut-être généré par un système informatisé conforme aux exigence réglementaires si la donnée d'entrée est incorrecte ou si l'analyste ayant réalisé l'analyse n'a pas été formé à l'utilisation de l'équipement et/ou du logiciel ;

- L' « audit trail » permet de tracer dans un ordre chronologique les opérations réalisées sur les systèmes informatisés et ainsi identifier toutes activités non autorisées, le cas échéant :
  - Généralement, l'« audit trail » devrait être réalisé pour tous les systèmes informatisés du laboratoire de contrôle qualité utilisés pour générer des données critiques utilisées pour la certification/libération des lots de substances actives ou de médicaments. De plus, il est recommandé de réaliser l'« audit trail » de la séquence d'analyse pendant la période de

revue des résultats d'analyse avant certification/libération. Enfin, cette revue doit être complète et elle doit être formalisée ;
    - La vérification de l'« audit trail » ne doit pas se limiter à la séquence d'analyse validée par l'analyste. Il est à noter que l'un des objectifs de l'« audit trail » est de repérer les réanalyses non autorisées. Afin de minimiser les risques liés à ces réanalyses non autorisées, il est nécessaire de vérifier l'« audit trail » pendant la période où les échantillons du lot sont présents dans le laboratoire. Cela correspond à la période entre la réception des échantillons au laboratoire et la validation des résultats du lot analysé ;
    - Afin de faciliter la vérification des « audit trails », il est recommandé de mettre en place au niveau du laboratoire de contrôle qualité un système formalisé de numérotation des échantillons à analyser ;

- Pour les entreprise ayant plusieurs sites de production situés sur le territoire national ou à l'international, il est recommandé d'avoir un système en place permettant de partager les écarts observés sur chacun des sites lors des inspections réglementaires, audits clients et audits internes afin d'étendre systématiquement les actions correctives et préventives au niveau de l'organisation qualité « Groupe ».

4. CONCLUSION

Globalement, la conformité des établissements inspectés est jugée satisfaisante, avec un respect des normes et des procédures dans la majorité des cas. Aucun cas de falsification ou de manipulation involontaire des données n'a été relevé, ce qui démontre une gestion fiable et transparente de l'information. Cependant, des écarts de conformité ont été observés d'un établissement à l'autre, ce qui indique qu'il existe des variations dans l'application des pratiques, soulignant ainsi la nécessité d'une harmonisation, ainsi qu'une meilleure sensibilisation et compréhension de la réglementation en vigueur pour assurer une conformité comparable entre les différents établissements

Il est de la responsabilité des opérateurs 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 problèmes liés à l'intégrité des données informatisées. Afin d'atteindre cet objectif, il est primordial de :

- Former et sensibiliser le personnel à la réglementation, aux concepts assurant l'intégrité des données, aux systèmes informatisés et à la détection des problèmes liés aux données générées par ces systèmes ;
- Intégrer la vérification de l'intégrité des données dans le cadre des programmes d'audits internes et des processus de qualification des prestataires externes ;
- Mettre en place un mécanisme interne permettant de signaler à la direction du site des problèmes graves liés à l'intégrité des données afin de prendre les mesures nécessaires pour les corriger (moyens organisationnels, financiers et de contrôles internes).

5. BIBLIOGRAPHIE

[1] - Annexe 11 des BPF « Systèmes informatisés ». https://ansm.sante.fr/documents/reference/bonnes-pratiques-de-fabrication-de-medicaments-a-usage-humain

[2] - EMA Q&A on « Annex 11: Computerised system » and « Data Integrity ». https://www.ema.europa.eu/en/human-regulatory/research-development/compliance/good-manufacturing-practice/guidance-good-manufacturing-practice-good-distribution-practice-questions-answers

[3] - MHRA: « GXP » Data Integrity Guidance and Definitions. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/687246/MHRA_GxP_data_integrity_guide_March_edited_Final.pdf

[4] - PIC/S Guidance « Good practices for data management and integrity in regulated GMP/GDP environments ». https://picscheme.org/docview/4234

[5] - WHO Guideline « TRS 1033 - Annex 4: WHO Guideline on data integrity ». https://www.who.int/publications/m/item/Annex-4-trs-1033

[6] - FDA: « Data Integrity and compliance with current manufacturing practice ». https://www.fda.gov/regulatory-information/search-fda-guidance-documents/data-integrity-and-compliance-drug-cgmp-questions-and-answers

[7] - FDA Guidance for Industry: « Data Integrity and compliance with current manufacturing practice - Questions And Answers ». https://www.fda.gov/regulatory-information/search-fda-guidance-documents/data-integrity-and-compliance-drug-cgmp-questions-and-answers-guidance-industry

143/147, boulevard Anatole France
F-93285 Saint-Denis Cedex
Tél. : +33 (0) 1 55 87 30 00

ansm.sante.fr • **@ansm**