# Commission nationale de l'informatique et des libertés

## Délibération n° 2026-052 du 19 mars 2026 portant homologation de l'annexe « contrôle qualité » pour les méthodologies de référence relatives aux traitements de données à caractère personnel mis en œuvre dans le cadre des recherches dans le domaine de la santé

NOR : *CNIS2613682X*

La Commission nationale de l'informatique et des libertés,

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) ;

Vu le code de la santé publique ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés (loi « informatique et libertés ») ;

Vu la délibération n° 2026-049 du 19 mars 2026 portant homologation de l'annexe « sécurité » pour les méthodologies de référence relatives aux traitements de données à caractère personnel mis en œuvre dans le cadre des recherches dans le domaine de la santé (annexe sécurité) ;

Après avoir entendu le rapport de Mme Marie Zins, commissaire, et les observations de M. Damien Milic, commissaire du Gouvernement ;

Formule les observations suivantes :

La mission de contrôle qualité consiste à vérifier l'exhaustivité et l'exactitude des données collectées dans le cadre d'une recherche, une étude ou évaluation dans le domaine de la santé (ci-après, « recherche en santé »). Elle est réalisée par comparaison entre les données à caractère personnel collectées dans le cadre d'une recherche en santé et celles issues de documents dits sources (par exemple le dossier médical de la personne se prêtant à la recherche).

La réalisation « sur site » de cette mission, c'est-à-dire au sein du lieu où se déroule la recherche, peut d'ores et déjà intervenir dans le cadre d'une déclaration de conformité aux méthodologies de référence (MR) 001, 002, 003 et 004.

La crise sanitaire liée à la covid-19 a fortement développé le recours au contrôle qualité « à distance », conduisant la CNIL à adopter des recommandations provisoires, applicables jusqu'au 31 décembre 2021. Ces recommandations ont été mises à jour et mises en consultation publique entre mai et juillet 2024.

Au regard de la sensibilité des données à caractère personnel traitées dans le cadre d'une mission de contrôle qualité, il est nécessaire de préciser les mesures juridiques, techniques et organisationnelles à mettre en œuvre pour garantir la protection des droits et libertés des personnes concernées. Ces mesures étant communes à l'ensemble des recherches en santé, il est apparu utile de les rassembler au sein d'un document unique auquel les MR pourront faire référence.

Un responsable de traitement d'une recherche en santé pourra mettre en œuvre une mission de contrôle qualité dans le cadre d'une déclaration de conformité à une MR dès lors que :

– la MR concernée prévoit la réalisation de cette mission ;
– cette mission est réalisée dans des conditions conformes à la présente annexe ;
– les autres conditions de mise en œuvre de la recherche en santé sont conformes à la MR applicable.

**Dans ces conditions, la CNIL homologue l'annexe « contrôle qualité » des méthodologies de référence relatives aux traitements de données à caractère personnel mis en œuvre dans le cadre des recherches dans le domaine de la santé.**

La présente délibération sera publiée au *Journal officiel* de la République française.

*La présidente,*
M.-L. Denis

ANNEXE

CONTRÔLE QUALITÉ

POUR LES MÉTHODOLOGIES DE RÉFÉRENCE (MR)

*Version avril 2026*

## 1. **Table des matières**



## 2. **Définitions**

Aux fins de la présente annexe, les termes suivants sont ainsi définis :

**Données à caractère personnel :** telles que définies au 1° de l'article 4 du RGPD ;

**Information RGPD :** les informations à fournir, en application des articles 12 à 14 du RGPD ainsi que des articles 69 à 71 de la loi « informatique et libertés », aux personnes concernées par un traitement de leurs données à caractère personnel dans le cadre d'une recherche, ou à leurs représentants légalement désignés ;

**Lieu de recherche :** lieu dans lequel la recherche est réalisée conformément aux règlementations sectorielles, comme par exemple le service d'un établissement de santé, à l'exclusion du domicile du patient ;

**Mission de contrôle qualité :** l'activité consistant à vérifier :

– le respect des réglementations applicables et du protocole d'une recherche ;
– l'exhaustivité et l'authenticité des données collectées dans le cadre de la recherche et transmises par le professionnel intervenant dans la recherche au responsable de traitement ou à ses sous-traitants ;

**Personne se prêtant à la recherche** la personne participant à une recherche conformément aux règlementations sectorielles applicables et dont les données à caractère personnel sont traitées ;

**Professionnel intervenant dans la recherche** la personne physique qui collecte les données, dirige ou surveille la réalisation de la recherche. Il s'agit notamment :

– de l'investigateur et ses collaborateurs agissant sous sa responsabilité et son autorité ;
– du professionnel de santé et ses collaborateurs agissant sous sa responsabilité et son autorité ;
– du personnel médical ;
– des personnes qualifiées, au sens des règlementations sectorielles ;

**Recherche :** notion générique qui couvre les recherches incluses dans le périmètre d'une méthodologie de référence, notamment :

– les recherches impliquant la personne humaine visées aux articles L. 1121-1 et suivants du code de la santé publique ;
– les essais cliniques sur des médicaments à usage humains visés par le règlement (UE) n° 536/2014 ;
– les investigations cliniques concernant des dispositifs médicaux visées par le règlement (UE) n° 2017/745 ;
– les études de performances concernant les dispositifs médicaux de diagnostic *in vitro* visées par le règlement (UE) n° 2017/746 ;
– les recherches n'impliquant pas la personne humaine ;

**Règlementation sectorielle :** la règlementation applicable aux recherches couvertes par une méthodologie de référence ou applicable à certains actes. Il s'agit notamment :

– du règlement (UE) n° 536/2014 relatif aux essais cliniques de médicaments à usage humain et de l'article L. 1124-1 du code de la santé publique ;
– du règlement (UE) n° 2017/745 relatif aux dispositifs médicaux et des articles L. 1125-1 à L. 1125-31 du code de la santé publique ;
– du règlement (UE) n° 2017/746 relatif aux dispositifs médicaux de diagnostic *in vitro* et des articles L. 1126-1 à L. 1126-29 du code de la santé publique ;
– des articles L. 1121-1 et suivants du code de la santé publique, s'agissant des recherches impliquant la personne humaine ;
– des règlementations sectorielles applicables dans un territoire ou pays tiers, lorsque le responsable de traitement est établi en France ;

**Responsable de traitement :** tel que défini au 7° de l'article 4 du RGPD. Il s'agit notamment du promoteur de la recherche conformément aux règlementations sectorielles. Il est responsable des différentes opérations de traitement dans le cadre d'une recherche, dont la mission de contrôle qualité ;

**Sous-traitant :** tel que défini au 8° de l'article 4 du RGPD. Il s'agit d'une entité juridique distincte du responsable de traitement, qui doit disposer de la personnalité juridique. Ainsi les différents services, directions, départements, etc. d'une même personne morale ne peuvent pas être considérés comme des sous-traitants distincts les uns des autres ;

**Traitement :** tel que défini au 2° de l'article 4 du RGPD.

## 3. **Introduction**

1. Le contrôle qualité, aussi appelé « *monitoring* », constitue une étape indispensable dans le cadre de recherche dans le domaine de la santé. Il permet notamment de vérifier l'exhaustivité et l'exactitude des données cliniques collectées.

2. Traditionnellement, le contrôle qualité est réalisé sur site, c'est-à-dire lors d'une visite au sein d'un lieu de recherche. Avec le développement de solutions numériques dans le domaine des recherches en santé, celui-ci est de plus en plus réalisé à distance par voie dématérialisée.

## 4. **Périmètre de l'annexe**

3. Cette annexe s'adresse à toutes les personnes physiques ou morales qui sont amenées à organiser ou mettre en œuvre une mission de contrôle qualité dans le cadre d'une recherche. Plus particulièrement, elle est destinée au(x) responsable(s) de traitements qui mettent en œuvre une recherche ainsi qu'aux sous-traitants intervenant pour la mise en œuvre d'une mission contrôle qualité (centre investigateur, personne chargée de réaliser le contrôle qualité, éditeur de logiciel, etc.).

4. Les exigences décrites dans cette annexe, indiquées comme [CQ-XXX-XX-00], sont applicables aux traitements mis en œuvre dans le cadre des méthodologies de référence homologuées par la CNIL en application de l'article 73 de la loi « informatique et libertés » qui renvoient expressément à ce document. En l'absence de conformité aux exigences de la présente annexe, une demande d'autorisation devra être sollicitée préalablement à la mise en œuvre de la recherche.

### A. – *Qu'est-ce que le contrôle qualité lors d'une recherche en santé ?*

5. La mission de contrôle qualité contribue à garantir la fiabilité et la robustesse des résultats de la recherche menée. Elle peut notamment consister en la vérification, par un attaché de recherche clinique (ARC) pour le compte du responsable de traitement, des documents sources (dossiers médicaux, comptes rendus d'analyses de laboratoires, etc.) en comparaison des données collectées par l'investigateur dans le cahier d'observation papier (CRF) ou électronique (eCRF).

### B. – *Champ d'application de l'annexe*

6. L'annexe couvre :

– **le contrôle qualité sur site** réalisé lors d'une visite au sein d'un lieu de recherche ;
– **le contrôle qualité à distance réalisé soit :**
  – **via un outil de vidéoconférence ;**
  – **via une plateforme sécurisée** permettant la mise à disposition des données strictement nécessaires.

7. Cette annexe ne couvre pas la mission de contrôle qualité réalisée à distance :

– par un accès direct au dossier médical ou dossier patient informatisé (DPI) ;
– par accès direct aux services ou outils numériques dans lesquels sont traitées des données permettant l'identification directe des personnes concernées (données administratives notamment) ou qui sont qualifiés de service numérique en santé au sens de l'article L. 1470-1 du code de la santé publique (par exemple : application mobile de télésuivi) ;

– portant sur les formulaires de consentement recueillis ou signés par voie électronique par les personnes en vue de leur participation à la recherche.

### 5. **Les conditions communes applicables au contrôle qualité (sur site ou à distance)**

8. Les exigences décrites ci-dessous sont applicables à la mission de contrôle qualité, quelle que soit sa forme.

#### A. – *Choisir un type de contrôle qualité et consulter les parties intéressées*

9. Le choix des modalités de réalisation du contrôle qualité relève du responsable de traitement, après consultation de son délégué à la protection des données (DPD) et de son responsable de la sécurité des systèmes d'information (RSSI), le cas échéant.

10. Le responsable de traitement est tenu de s'assurer que son sous-traitant est en capacité de mettre en œuvre les mesures techniques et organisationnelles nécessaires pour garantir la protection des données, notamment celles détaillées dans cette annexe [CQ-COM-JUR-1]. Cette vérification suppose que :

– le responsable de traitement communique sur le type de contrôle qualité souhaité, ses caractéristiques essentielles et les conséquences notamment opérationnelles pour ses sous-traitants ;
– le sous-traitant transmette au responsable de traitement toute information pertinente sur la manière dont cette activité sera réalisée.

11. Pour les recherches en cours, la modification du type du contrôle qualité réalisé (sur site ou à distance) constitue une modification substantielle du traitement de données lié. La mise en œuvre de cette modification nécessite la consultation préalable de chaque organisme qualifié de lieu de recherche concerné afin de garantir qu'il est en capacité de mettre en œuvre les mesures appropriées pour la protection des données. Cette consultation suppose l'intervention des profils métiers adéquats et notamment le DPD et, le cas échéant, le RSSI.

#### B. – *Encadrer le périmètre du contrôle qualité et ses caractéristiques essentielles*

12. Lorsque la mission de contrôle qualité implique l'intervention d'un ou plusieurs sous-traitants, un contrat conforme l'article 28 du RGPD est conclu avec chaque sous-traitant y participant (par exemple le centre investigateur, la société de recherche sous contrat – CRO – et, le cas échéant, le prestataire proposant la solution numérique utilisée) [CQ-COM-JUR-2].

13. Au regard des risques spécifiques associés à la mission de contrôle qualité, il est recommandé que le contrat de sous-traitance prévoie spécifiquement les éléments suivants :

– le type de contrôle qualité retenu (sur site et/ou à distance) ;
– la recherche pour laquelle le contrôle est réalisé et ses principales caractéristiques permettant de déterminer les catégories de personnes concernées et les données strictement nécessaires à sa réalisation ;
– une clause de confidentialité spécifique, tenant compte des risques liés aux modalités de réalisation du contrôle qualité. Cette clause précise notamment que les personnes chargées du contrôle qualité s'engagent à ne pas effectuer d'impression écran ou de photos, à consulter les données dans un endroit clos sans passage de tiers, à utiliser uniquement du matériel informatique maîtrisé à usage strictement professionnel ;
– les instructions détaillées sur la réalisation de la mission ou à défaut, les modalités selon lesquelles ces instructions seront précisées aux acteurs qui y participent.

#### C. – *Minimiser les données traitées par rapport à l'objectif poursuivi*

14. Les données à caractère personnel consultées dans le cadre d'une mission de contrôle qualité servent exclusivement à :

– vérifier le respect des réglementations sectorielles applicables et du protocole (par exemple le respect des critères d'inclusion) ;
– le cas échéant, vérifier l'authenticité et la cohérence des formulaires de consentement recueillis au format papier ;
– vérifier l'authenticité et la cohérence des informations recueillies dans le cadre de la recherche conformément au protocole notamment par rapport au contenu des documents sources.

15. Seules les données strictement nécessaires pour atteindre les objectifs précités peuvent être traitées [CQ-COM-JUR-3]. Le contrôle qualité ne justifie pas un accès à l'ensemble du dossier médical de la personne concernée. Ainsi, les personnes chargées de ce contrôle ont accès uniquement aux données à caractère personnel :

– relatives à la personne concernée par la recherche ;
– et qui ont un lien direct avec la recherche concernée.

16. Conformément aux bonnes pratiques cliniques, le contrôle qualité peut être réalisé sur des données permettant l'identification directe de la personne concernée (données administratives notamment).

D. *Déterminer les personnes habilitées à réaliser le contrôle qualité*

17. Les personnes chargées du contrôle qualité peuvent être toute personne agissant sous l'autorité du responsable de traitement. Il peut s'agir de son personnel habilité ou d'un sous-traitant.

18. Les personnes chargées du contrôle qualité :

– doivent disposer des qualifications et de l'expérience nécessaires à la réalisation de cette activité [CQ-COM-JUR-4] ;
– sont soumises au secret professionnel en application des règlementations sectorielles (1) et de l'article 68 de la loi « informatique et libertés » ;
– doivent être mandatées et habilitées [CQ-COM-JUR-5].

E. *Informer les personnes et respecter leurs droits*

19. Les personnes concernées doivent être informées lors de leur inclusion dans la recherche [CQ-COM-JUR-6] de ce que :

– un contrôle qualité pourra être réalisé et les modalités de ce contrôle (sur site et/ou à distance) ;
– ce contrôle qualité peut conduire des tiers à avoir accès aux données permettant leur identification directe (données administratives notamment) ;
– elles disposent d'un droit d'opposition à sa réalisation.

20. Cette information est insérée dans l'information RGPD et/ou dans la note d'information relative à la recherche prévue par la règlementation sectorielle applicable (2).

21. Aucun contrôle qualité ne peut être effectué sur les données à caractère personnel d'une personne qui s'y est opposée [CQ-COM-JUR-7].

22. Pour les recherches en cours, la modification des modalités de réalisation du contrôle qualité constitue une modification substantielle dont les personnes concernées doivent être informées.

23. Les autres droits des personnes concernées par une mission de contrôle qualité s'exercent conformément aux dispositions de la méthodologie de référence applicable.

F. *Mettre en place des mesures de sécurité adaptées*

24. La mission de contrôle qualité nécessite de respecter les exigences de l'annexe de sécurité complétées par les exigences de cette annexe [CQ-COM-SEC-1].

25. La mission de contrôle qualité est réalisée sous la direction et la surveillance d'un professionnel intervenant dans la recherche qui exerce dans le lieu de recherche concerné [CQ-COM-SEC-2].

26. Quelle que soit la modalité de contrôle qualité envisagée, les mesures techniques et organisationnelles suivantes sont mises en œuvre :

– l'exigence MR-SEC-10 s'applique en particulier avec la mise en place de comptes nominatifs [CQ-COM-SEC-3] ;
– l'exigence MR-SEC-13 s'applique en particulier avec la mise en place [CQ-COM-SEC-4] :
  – de profils spécifiques pour les personnes chargées du contrôle qualité ;
  – d'un accès en lecture seule aux données strictement nécessaires au contrôle qualité ;
  – d'une restriction de la durée des habilitations d'accès (ex. : désactivation des droits d'accès à la fin d'une phase de consultation des données, désactivation du compte à la fin de l'étude) ;
– les exigences MR-SEC-16 à MR-SEC-21 s'appliquent en particulier avec la sécurisation du poste de travail des personnes chargées du contrôle qualité [CQ-COM-SEC-5]. Il est notamment recommandé que la consultation ait lieu dans un endroit clos sans passage de tiers, qu'il soit opéré sur le poste de travail un blocage des possibilités de capture d'écran ainsi que la désactivation des assistants IA ;
– l'exigence MR-SEC-27 s'applique en particulier avec la mise en place de procédures spécifiques de gestion et de traitement des incidents de sécurité et des violations de données personnelles [CQ-COM-SEC-6] ;
– il est prévu un blocage applicatif des possibilités d'impression, de copie d'écran, d'export ou de téléchargement des données consultées pendant le contrôle qualité [CQ-COM-SEC-7].

## 6. **Les conditions complémentaires applicables au contrôle qualité à distance**

27. En complément des exigences décrites dans la partie 4, les exigences ci-dessous sont applicables pour le contrôle qualité réalisé à distance.

A. – *Choisir un type de contrôle qualité à distance, consulter les parties intéressées et les former*

28. Lorsque le responsable de traitement décide de recourir à un contrôle qualité à distance, celui-ci sera tenu de vérifier, par le biais notamment d'audits, que la solution technique retenue offre un niveau de protection approprié et conforme aux exigences de cette annexe [CQ-DIST-JUR-1]. Il est recommandé de réaliser un audit lors de la sélection d'un nouvel outil, puis au moins tous les trois ans si celui-ci est conservé.

29. Le responsable de traitement s'assure que les professionnels intervenant dans la recherche sont formés à l'utilisation de la solution technique retenue pour la réalisation du contrôle qualité à distance [CQ-DIST-JUR-2].

30. Au regard des enjeux liés à la protection des données, il est recommandé que le choix de recourir à un contrôle qualité à distance fasse l'objet d'échanges entre le responsable de traitement et ses sous-traitants, plus particulièrement les lieux de recherche concernés (dont leur DPD et RSSI).

31. Il est précisé que la mission de contrôle qualité réalisée via un outil de vidéoconférence a l'avantage de correspondre davantage à un contrôle qualité sur site.

B. – *Encadrer le contrôle qualité à distance et ses caractéristiques essentielles*

32. Outre les éléments mentionnés au paragraphe 16, il est recommandé que le contrat de sous-traitance précise :

- les spécifications détaillées de la solution technique retenue ainsi que, le cas échéant, le dossier de validation des systèmes informatisés mis à disposition des sous-traitants ;
- la procédure à suivre en cas de doute sur la véracité ou la complétude des données sources mises à disposition par le professionnel intervenant dans la recherche qui exerce dans le lieu de recherche concerné par le contrôle qualité ;
- les modalités de vérification liées. Les pratiques suivantes devraient a minima être mises en place :
  - les personnes chargées du contrôle qualité manifestent l'existence d'un doute, pendant la réalisation du contrôle qualité ;
  - cette information est transmise au responsable de traitement qui détermine les suites à donner.

33. En cas de doute, si le responsable de traitement souhaite vérifier la véracité ou la complétude des données mises à disposition, cette vérification devra prendre la forme d'un contrôle qualité sur site [CQ-DIST-JUR-3].

34. La solution de contrôle qualité à distance est hébergée au sein de l'Union européenne (UE), de l'Espace économique européen ou dans un pays disposant d'un niveau de protection adéquat au sens de l'article 45 du RGPD [CQ-DIST-JUR-4]. Par exception, cette exigence n'est pas applicable à la mission de contrôle qualité réalisée sur les données conservées par un organisme qualifié de lieu de recherche établi hors UE.

35. Le cas échéant, les modalités de transfert hors UE devront être conformes aux dispositions du référentiel ou de la MR applicable à la recherche concernée ou faire l'objet d'une demande d'autorisation. Il est rappelé que tout accès distant aux données (y compris une visualisation) depuis l'extérieur du territoire de l'UE constitue un transfert hors UE.

C. – *Mettre en place des mesures de sécurité adaptées*

7. **Mesures complémentaires pour un outil de vidéoconférence**

36. Le responsable de traitement recourt à des solutions de vidéoconférence sécurisées et dont il maîtrise les risques. Il est recommandé de privilégier des solutions ayant déjà fait l'objet d'une certification appropriée (3) ou, à défaut, qui sont couvertes par des référentiels existants (4).

37. Les mesures suivantes sont également mises en œuvre :

- l'exigence MR-SEC-12 s'applique avec une authentification multifacteur au sens de la recommandation de la CNIL (délibération n° 2025-019 ou sa version la plus récente) [CQ-VISIO-SEC-1] ou, par dérogation :
  - une authentification est prévue pour chacune des personnes participant à une vidéoconférence ou à défaut, la définition d'un code secret spécifique pour chaque session de vidéoconférence et utilisation d'une zone d'attente permettant à l'hôte de valider l'entrée de chaque participant ;
  - le mot de passe ou le code secret nécessaire pour se connecter à la plateforme de vidéoconférence est conforme à la recommandation relative aux mots de passe et autres secrets partagés de la CNIL (délibération n° 2022-100 ou sa version la plus récente) [EX-VISIO-SEC-2] ;
- l'exigence MR-SEC-14 s'applique en particulier par la conservation des données de journalisation de la solution de vidéoconférence, si celle-ci le permet, ou par la tenue d'une main courante par l'organisme qualifié de lieu de recherche détaillant les horaires et les personnes ayant participé aux vidéoconférences [CQ-VISIO-SEC-3] ;
- l'exigence CQ-COM-SEC-2 s'applique en particulier avec la présence d'un professionnel intervenant dans la recherche pendant toute la durée de la vidéoconférence [CQ-VISIO-SEC-4] ;
- il est prévu le recours à la fonctionnalité de partage d'écrans permettant d'afficher uniquement les documents sources dont les personnes chargées du contrôle ont besoin [CQ-VISIO-SEC-5] ;
- il est prévu le blocage des fonctionnalités de type « prise en main à distance » et « partage de documents » [CQ-VISIO-SEC-6] ;
- il est prévu le blocage des possibilités d'enregistrement ou de retranscription automatique de la session de vidéoconférence [CQ-VISIO-SEC-7].

8. **Mesures complémentaires pour une plateforme sécurisée**

38. La sensibilité des données susceptibles d'être traitées dans le cadre d'une mission de contrôle qualité impose la mise en place d'une solution technique particulièrement robuste.

39. Ainsi, les données mises à disposition de la personne chargée de réaliser le contrôle qualité par les professionnels intervenant dans un lieu de recherche concerné ne doivent pas lui être envoyées directement mais doivent être déposées sur une plateforme intermédiaire de visualisation de données.

40. Cette plateforme sécurisée ne doit contenir que les données strictement nécessaires au contrôle qualité et doit permettre une traçabilité exhaustive des actions de la personne chargée de le réaliser.

41. Les mesures suivantes sont mises en œuvre sur la plateforme de visualisation :

– l'exigence MR-SEC-09 s'applique en particulier avec le chiffrement au repos des données déposées sur la plateforme, et des sauvegardes, par des algorithmes cryptographiques à l'état de l'art [CQ-PF-SEC-1] ;
– l'exigence MR-SEC-12 s'applique, avec une authentification multifacteur au sens de la recommandation de la CNIL (délibération n° 2025-019 ou sa version la plus récente) [CQ-PF-SEC-2] ;
– l'exigence MR-SEC-19 s'applique en particulier avec la mise en place d'un cloisonnement des données entre différentes recherches pour lesquelles la même plateforme est utilisée lors du contrôle qualité [CQ-PF-SEC-3] ;
– l'exigence MR-SEC-14 s'applique en particulier avec la journalisation et la surveillance, par l'organisme qualifié de lieu de recherche concerné, des actions de la personne chargée de réaliser le contrôle qualité [CQ-PF-SEC-4] : conservation des données de journalisation permettant un audit complet des accès et des actions de la personne chargée de réaliser le contrôle qualité (enregistrement comprenant l'auteur individuellement identifié, l'horodatage, la nature de l'opération réalisée ainsi que la référence des documents auxquels la personne chargée de réaliser le contrôle qualité a eu accès) ;
– par dérogation à l'exigence CQ-COM-SEC-2, la surveillance des opérations de contrôle qualité est réalisée par une analyse détaillée de la journalisation requise par CQ-PF-SEC-4 [CQ-PF-SEC-5] ;
– il est prévu l'effacement des données déposées sur la plateforme, et de leurs éventuelles sauvegardes, dès la fin du contrôle qualité [CQ-PF-SEC-6] ;
– il est prévu qu'aucun fichier, même temporaire, contenant des données à caractère personnel mises à disposition par l'organisme qualifié de lieu de recherche pour le contrôle qualité ne puisse être conservé sur le terminal de la personne chargée de réaliser le contrôle qualité après une session de contrôle qualité à distance [CS-PF-SEC-7].

42. Le recours à un hébergeur de données de santé (HDS) (5) est nécessaire dès lors que les données transmises concernent des personnes résidant en France ou ayant été prises en charge par un établissement, un professionnel ou centre de santé établi en France et qu'au moins l'une des conditions suivantes est remplie :

– les données transmises sur la plateforme permettent l'identification directe de la personne concernée ;
– les données transmises sont celles initialement collectées pour une activité de prévention, de diagnostic, de soin, et de suivi social ou médico-social (par exemple pour la tenue du dossier médical ou le fonctionnement d'un service numérique en santé au sens de l'article L. 1470-1 du code de la santé publique).

Dans l'hypothèse où le recours à un HDS ne serait pas nécessaire (aucune de ces conditions n'est remplie), le responsable de traitement fait appel à un organisme certifié ISO/IEC 27001 : 2022 ou qui présente des garanties de sécurité équivalentes [CQ-PF-SEC-8].

---

(1) Il s'agit notamment de l'article L. 1121-3 du code de la santé publique (CSP) s'agissant des recherches impliquant la personne humaine, de l'article L. 1125-6 du CSP pour les investigations cliniques et l'article L. 1126-5 du CSP pour les études de performances.

(2) Ces règlementations sectorielles applicables correspondent notamment à :
– s'agissant des recherches impliquant la personne humaine, l'article L. 1122-1 du CSP ;
– s'agissant des essais cliniques, l'article 29 du règlement n° 536/2014 ;
– s'agissant des investigations cliniques, l'article 63 du règlement UE n° 2017/745 ;
– s'agissant de études de performances, l'article 59 du règlement (UE) n° 2017/746.

(3) Par exemple par l'ANSSI (Agence nationale de sécurité des systèmes d'information).

(4) Par exemple le socle interministériel des logiciels libres.

(5) Liste des hébergeurs certifiés disponible sur le site web de l'Agence du numérique en santé (https://esante.gouv.fr/offres-services/hds/liste-des-hebergeurs-certifies).

## 9. **Annexe – Liste des exigences applicables**

| Site | Visio | PF | Référence | Exigence |
|---|---|---|---|---|
| **X** | **X** | **X** | [CQ-COM-JUR-1] | S'assurer que les sous-traitants sont en capacité de mettre en œuvre les mesures techniques et organisationnelles nécessaires pour garantir la protection des données à caractère personnel, notamment celles détaillées dans l'annexe. |
| X | X | X | [CQ-COM-JUR-2] | Conclure un contrat de sous-traitance conforme à l'article 28 du RGPD avec l'ensemble des organismes participant à une mission de contrôle qualité. |
| **X** | **X** | **X** | [CQ-COM-JUR-3] | Minimiser les données : seules celles strictement nécessaires pour atteindre les objectifs du contrôle qualité peuvent être traitées dans ce cadre. |

| Site | Visio | PF | Référence | Exigence |
|---|---|---|---|---|
| X | X | X | [CQ-COM-JUR-4] | S'assurer que les personnes chargées du contrôle qualité disposent des qualifications et de l'expérience nécessaire à la réalisation de cette activité. |
| **X** | **X** | **X** | [CQ-COM-JUR-5] | Mandater et habiliter formellement les personnes chargées du contrôle qualité. |
| X | X | X | [CQ-COM-JUR-6] | Informer les personnes concernées lors de leur inclusion de la réalisation d'un contrôle qualité et de leur droit d'opposition. |
| **X** | **X** | **X** | [CQ-COM-JUR-7] | Exclure les données des personnes concernées qui se sont opposées au contrôle qualité sur leurs données. |
| X | X | X | [CQ-COM-SEC-1] | Mettre en œuvre les mesures MR-SEC-XX de l'annexe de sécurité en les complétant avec les exigences de cette annexe. |
| **X** | **X** | | [CQ-COM-SEC-2] | Réaliser le contrôle qualité sous la direction et la surveillance d'un professionnel intervenant dans la recherche qui exerce dans le lieu de recherche concerné. |
| X | X | X | [CQ-COM-SEC-3] | En complément de la MR-SEC-10, prévoir des comptes nominatifs. |
| **X** | **X** | **X** | [CQ-COM-SEC-4] | En complément de la MR-SEC-13, prévoir des profils spécifiques, un accès en lecture seule et des restrictions de la durée des habilitations d'accès. |
| X | X | X | [CQ-COM-SEC-5] | En complément des MR-SEC-16 à MR-SEC-21, sécuriser le poste de travail des personnes chargées du contrôle qualité. |
| **X** | **X** | **X** | [CQ-COM-SEC-6] | En complément de la MR-SEC-27, mettre en place des procédures spécifiques de gestion et de traitement des incidents de sécurité et des violations des données personnelles. |
| X | X | X | [CQ-COM-SEC-7] | Bloquer les possibilités d'impression, de copie d'écran, d'export ou de téléchargement des données consultées. |
| | **X** | **X** | [CQ-DIST-JUR-1] | Vérifier, par le biais notamment d'audits, que la solution de contrôle qualité à distance offre un niveau de protection appropriée et conforme aux exigences de cette annexe. |
| | X | X | [CQ-DIST-JUR-2] | Former les professionnels intervenant dans la recherche, ou les personnes placées sous leur autorité, à l'utilisation de la solution technique de contrôle qualité à distance. |
| | **X** | **X** | [CQ-DIST-JUR-3] | Si le responsable de traitement souhaite vérifier la véracité ou la complétude des données mises à disposition, cette vérification prend la forme d'un contrôle qualité sur site. |
| | X | X | [CQ-DIST-JUR-4] | Assurer l'hébergement de la solution de contrôle qualité à distance dans l'Union européenne (UE), dans l'espace économique européen ou dans un pays disposant d'un niveau de protection adéquat. Cette exigence n'est pas applicable pour les données conservées par un organisme qualifié de lieu de recherche établi hors UE. |
| | **X** | | [CQ-VISIO-SEC-1] | En complément de l'exigence MR-SEC-12, mettre en place une authentification conforme à la recommandation de la CNIL. |
| | X | | [CQ-VISIO-SEC-2] | Par dérogation à CQ-VISIO-SEC-1, prévoir soit :<br>- une authentification de chaque personne participant à une vidéoconférence ou à défaut, définir un code secret spécifique pour chaque session de vidéoconférence et utiliser une zone d'attente permettant à l'hôte de valider l'entrée de chaque participant ;<br>- un mot de passe ou un code secret conforme à la recommandation de la CNIL pour se connecter à la plateforme de vidéoconférence. |
| | **X** | | [CQ-VISIO-SEC-3] | En complément de la MR-SEC-14, conserver les données de journalisation des accès, si la solution de vidéoconférence le permet, ou tenir une main courante par l'organisme qualifié de lieu de recherche détaillant les horaires et personnes ayant participé aux vidéoconférences. |
| | X | | [CQ-VISIO-SEC-4] | En complément de CQ-COM-SEC-2, assurer la présence d'un professionnel intervenant dans la recherche pendant toute la durée de la vidéoconférence. |
| | **X** | | [CQ-VISIO-SEC-5] | Prévoir le recours à la fonctionnalité partage d'écrans permettant de respecter l'exigence [CQ-COM-JUR-3]. |
| | X | | [CQ-VISIO-SEC-6] | Bloquer les fonctionnalités de type « prise en main à distance » et « partage de documents ». |
| | **X** | | [CQ-VISIO-SEC-7] | Ne pas permettre l'enregistrement de la session de vidéoconférence ou de retranscription automatique de la session de vidéoconférence. |
| | | X | [CQ-PF-SEC-1] | En complément de MR-SEC-09, mettre en œuvre le chiffrement au repos des données déposées sur la plateforme, et des sauvegardes, par des algorithmes cryptographiques à l'état de l'art. |

| Site | Visio | PF | Référence | Exigence |
|---|---|---|---|---|
| | | **X** | [CQ-PF-SEC-2] | En complément de MR-SEC-12, mettre en place une authentification multifacteur conforme à la recommandation de la CNIL pour se connecter à la plateforme. |
| | | X | [CQ-PF-SEC-3] | En complément de MR-SEC-19, mettre en place un cloisonnement des données entre différentes recherches. |
| | | **X** | [CQ-PF-SEC-4] | En complément de MR-SEC-14, mettre en place la journalisation et la surveillance des actions de la personne chargée de réaliser le contrôle qualité par l'organisme qualifié de lieu de recherche. |
| | | X | [CQ-PF-SEC-5] | Par dérogation à l'exigence CQ-COM-SEC-2, la surveillance des opérations de contrôle qualité est réalisée par une analyse détaillée de la journalisation requise par CQ-PF-SEC-4. |
| | | **X** | [CQ-PF-SEC-6] | Limiter la durée de conservation des données déposées sur la plateforme à la stricte durée du contrôle qualité. |
| | | X | [CQ-PF-SEC-7] | S'assurer qu'aucun fichier, même temporaire, contenant des données personnelles relatives à la personne se prêtant à la recherche ne soit conservé sur le terminal de la personne chargée de réaliser le contrôle qualité après une session de contrôle qualité à distance. |
| | | **X** | [CQ-PF-SEC-8] | Recourir à un hébergeur de données de santé (HDS) si les données déposées sur la plateforme sont nominatives et/ou issues de la prise en charge du patient, et sinon recourir à un prestataire certifié ISO/IEC 27001 : 2022 ou qui présente des garanties de sécurité équivalentes. |