

Bonnes pratiques

CONTRÔLE QUALITÉ À DISTANCE DES ESSAIS CLINIQUES

16 mai 2024

Qu'est-ce que le contrôle qualité lors d'un essai clinique et comment se déroule-t-il habituellement ?

Le contrôle qualité, ou *monitoring*, consiste à vérifier l'exhaustivité et l'exactitude des données transmises par les centres d'investigation au promoteur afin d'assurer la fiabilité des résultats de l'étude.

Ce contrôle qualité peut notamment consister en la vérification, par un « attaché de recherche clinique » (ARC) pour le compte du promoteur, des documents sources (dossiers médicaux, comptes rendus d'analyses de laboratoires, etc.) en comparaison des données collectées dans le cahier d'observation par l'investigateur.

Conformément au principe du secret médical et aux dispositions encadrant la recherche impliquant la personne humaine (articles [L. 1110-4](#) et [L. 1121-3](#) du code de la santé publique), aux bonnes pratiques cliniques ([Décision du 24 novembre 2006](#) fixant les règles de bonnes pratiques cliniques pour les recherches biomédicales portant sur des médicaments à usage humain), aux dispositions du règlement relatif aux essais cliniques ([Règlement UE 536/2014 du 16 avril 2014](#)) et aux dispositions des méthodologies de référence ([MR-001](#), [MR 003](#), §2.3.2), cette consultation est habituellement réalisée « **au sein des centres investigateurs** », « **sous la direction et la surveillance d'un professionnel intervenant dans la recherche** », et dans des conditions apportant des garanties substantielles vis-à-vis des risques d'atteinte à la confidentialité des données.

Cette modalité de consultation permet de s'assurer que la documentation source concernant le patient reste dans le centre investigateur dans lequel il est pris en charge, et qu'elle est réalisée sous la surveillance de l'équipe investigatrice. En outre, « **la personne chargée du contrôle qualité ne peut avoir accès qu'aux données individuelles nécessaires à ce contrôle** ».

Toutefois, le développement de solutions numériques permettant la surveillance à distance des essais cliniques, en particulier pour faciliter la surveillance de ceux menés à partir de plusieurs sites, conduit la CNIL à proposer les bonnes pratiques suivantes.

Quelles formalités auprès de la CNIL ?

Le contrôle qualité à distance ne répond pas strictement aux dispositions des méthodologies de référence actuelles. Il constitue toutefois une modalité de dématérialisation des essais cliniques sollicitée par les acteurs de la recherche. La surveillance à distance d'une étude peut donc être mise en place, après avoir été autorisée par la CNIL.

Dans cette hypothèse, il est nécessaire de documenter spécifiquement la mise en place du contrôle qualité à distance comme point de non-conformité aux méthodologies de référence dans le dossier de demande. Il faudra également démontrer les modalités d'implémentation de ces bonnes pratiques.

L'autorisation de la CNIL, prenant acte notamment du respect des bonnes pratiques, intervient après l'obtention de l'avis du comité de protection des personnes (CPP) et, si nécessaire, de l'autorisation de l'ANSM. Ces organismes se prononcent donc également sur le recours à une solution de contrôle qualité à distance.

Par ailleurs, la mise en œuvre d'une modalité de contrôle qualité à distance pour une recherche en cours constitue une modification substantielle. Cette dernière doit être adressée pour avis au comité de protection des personnes, ainsi que, si nécessaire, à l'ANSM avant de faire l'objet d'une formalité auprès de la CNIL (dépôt d'une [demande d'autorisation](#), lorsque le traitement a été initialement mis en œuvre dans le cadre d'une déclaration de conformité à une méthodologie de référence, ou dépôt une [demande de modification substantielle](#) lorsque le traitement a déjà fait l'objet d'une autorisation de la CNIL).

Comment informer les personnes concernées ?

Les modalités de contrôle qualité à distance doivent être précisées dans le document d'information prévu à l'article L. 1122-1 du CSP.

Les personnes concernées doivent être informées et pouvoir exercer leurs droits conformément à l'article L.1121-3 du CSP.

Dans le cadre d'une modification substantielle, la note d'information délivrée doit être mise à jour sur ce point et remise aux personnes concernées. Les modalités à privilégier sont une remise en main propre directement aux personnes concernées ou un courrier postal. Dans certains cas, un appel téléphonique par le centre investigateur avec envoi d'un document écrit à la demande de la personne peut être envisagé, avec une documentation de la non-opposition du patient dans son dossier médical.

Le contrôle qualité à distance ne peut être effectué à partir du dossier médical d'une personne qui s'y est opposée.

Quelles sont les conditions générales à respecter ?

De manière générale, le promoteur doit mesurer l'impact du contrôle qualité à distance en **termes de charge de travail** pour le centre d'investigation, et s'adapter aux contraintes de chaque lieu de recherche.

Consultation du délégué à la protection des données et documentation

Le promoteur et le centre d'investigation **doivent consulter leur délégué à la protection des données (DPD)**, notamment afin de déterminer si le contrôle à distance peut s'effectuer dans des conditions de nature à satisfaire les exigences détaillées ci-après.

Des procédures spécifiques doivent être mises en place, en tant que de besoin, entre le promoteur et le centre d'investigation pour préciser les modalités de réalisation du contrôle qualité (signature d'un accord de confidentialité, identité du ou des ARC et dates/horaires du contrôle, etc.).

La solution retenue doit être documentée par le responsable de traitement pour réaliser cette surveillance à distance, ainsi que l'ensemble des garanties mises en place. Les recommandations du DPO doivent être intégrées à cette documentation.

Au sein du lieu de recherche, **le DPD ou toute personne habilitée doit pouvoir consulter les spécifications détaillées du dispositif envisagé** ainsi que, le cas échéant, le dossier de validation des systèmes informatisés afin de s'assurer des conditions de sécurité.

Le recours au contrôle qualité à distance ne doit pas être imposé aux centres investigateurs, à plus forte raison lorsque l'étude a déjà débuté, sans que ces modalités n'aient été envisagées au préalable.

Le cas échéant, il est nécessaire de mettre à jour l'analyse d'impact sur la protection des données (AIPD) réalisée dans le cadre de l'étude.

Précautions sur la consultation à distance et le secret professionnel de l'ARC

L'ARC est soumis au secret professionnel.

La consultation en dehors du centre d'investigation des données par l'ARC doit s'accompagner de **mesures de confidentialité renforcées que ce dernier doit s'engager à respecter**, et qui seront préalablement rappelées par le promoteur lors d'une formation spécifique.

Ainsi, la **signature d'un accord de confidentialité complémentaire de la part de l'ARC** est recommandée afin que ce dernier s'engage notamment à ne pas effectuer d'impression écran ou de photos, à consulter dans un endroit clos sans passage de tiers, à utiliser uniquement du matériel informatique maîtrisé fourni par le promoteur et suffisamment sécurisé.

Quelles garanties de sécurité mettre en place ?

Les modalités de consultation à distance ne doivent pas impliquer un affaiblissement du niveau de sécurité habituellement mis en œuvre lors d'une visite sur site et les technologies doivent être maintenues à l'état de l'art.

Conditions de sécurité communes

Quelle que soit la modalité choisie, les conditions ci-dessous doivent être respectées :

- **hébergement du traitement dans l'Union européenne** ou dans un pays disposant d'un niveau de protection adéquat ;
- tout accès distant aux données (y compris une visualisation) depuis l'extérieur du territoire de l'Union européenne est à encadrer comme un transfert de données hors UE ;
- **transmission sécurisée des données** par des algorithmes cryptographiques à l'état de l'art, par exemple via le protocole TLS et l'algorithme AES-256 ;
- mise en place de **comptes nominatifs** et de **profils spécifiques** pour les ARC ;
- **accès en lecture seule** aux **seules données** nécessaires au contrôle qualité ;
- **impossibilité pour l'ARC d'exporter** les données à caractère personnel ou de télécharger les fichiers faisant l'objet du contrôle qualité. En particulier, aucun fichier, même temporaire, contenant des données personnelles ne doit être accessible sur le terminal de l'ARC après une session de contrôle qualité à distance ;
- **restriction de la durée des accès pour ces profils** (ex. : désactivation du compte à la fin de la phase de consultation des données) ;
- mise en place de **procédures de gestion et de traitement des incidents de sécurité et des violations de données** personnelles précisant les rôles et responsabilités et les actions à mener en cas de survenue de tels incidents ;
- mise en œuvre de mesures techniques et organisationnelles afin de sécuriser le poste de travail de l'ARC (**mots de passe** pour accéder au poste conformes à [la recommandation de la CNIL](#), **logiciels de détection de logiciels malveillants à jour**, **connexion à un réseau sécurisé**, etc.) ;
- « surveillance » en temps réel ou *a posteriori* **systématique** du contrôle qualité par le centre d'investigation, en fonction des solutions choisies (voir ci-dessous).

Conditions de sécurité spécifiques à la solution choisie, en complément des garanties précédentes

1. Contrôle qualité via une vidéoconférence avec le centre d'investigation

La solution de vidéoconférence **a l'avantage de correspondre davantage à une visite « physique »** de l'ARC dans le centre, conformément aux principes de la MR.

Concrètement, il est recommandé d'utiliser des solutions de vidéoconférence ayant déjà fait l'objet d'une [certification appropriée, par exemple par l'ANSSI](#) (Agence nationale de sécurité des systèmes d'information), ou qui font déjà partie de référentiels existants, comme le [socle interministériel des logiciels libres](#).

La fonctionnalité de partage d'écrans permet au centre d'investigation d'afficher uniquement les documents sources dont l'ARC a besoin.

Recommandations complémentaires :

- **aucune fonctionnalité de type « prise en main à distance » ne doit être utilisée** ;
- présence d'un membre du centre d'investigation **pendant toute la durée** de la vidéoconférence ;
- création de **comptes nominatifs avec authentification** pour chacune des personnes participant à une vidéoconférence ou à défaut, **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 ;

- **politique de mots de passe** conforme à la **recommandation précitée** pour se connecter à la plateforme de vidéoconférence (et utilisation recommandée d'une **authentification multifacteur** si cela est possible) ;
- **absence d'enregistrement** de la session de vidéoconférence ;
- **conservation des données de journalisation des accès pendant 6 mois à un an**, si la solution de vidéoconférence le permet, ou **tenue d'une main courante** par le centre d'investigation détaillant les horaires et personnes ayant participé aux vidéoconférences.

2. Envoi de données par les centres à l'ARC du promoteur via une plateforme sécurisée

Les données consultées par les ARC doivent permettre d'assurer un contrôle qualité fiable, conformément aux bonnes pratiques cliniques ; notamment, le contrôle qualité à distance ne requiert pas de pseudonymiser les données.

En revanche, la sensibilité des données susceptibles d'être traitées dans ce cadre impose la mise en place d'une solution technique particulièrement robuste. Ainsi, les données mises à disposition de l'ARC ne doivent pas directement être envoyées à celui-ci, mais une plateforme intermédiaire de visualisation de données devrait être utilisée. Cette plateforme sécurisée ne doit contenir que les données strictement nécessaires au suivi, et doit permettre une traçabilité exhaustive des actions de l'ARC.

Recommandations complémentaires :

- recours à un **hébergeur de données de santé** (HDS) ;
- **impossibilité d'accéder** aux documents transmis après un certain délai, par exemple via une suppression automatique des données ;
- mise en place de **comptes nominatifs** et d'une **authentification multifacteur** pour se connecter à la plateforme de visualisation ;
- **chiffrement au repos des données envoyées** vers cette plateforme et des sauvegardes par des algorithmes cryptographiques à l'état de l'art, par exemple l'algorithme AES-256 ;
- mise en place d'un **cloisonnement des données** entre les différentes études ;
- **surveillance des actions des ARC** par le centre investigateur : conservation des données de [journalisation](#) permettant un audit complet des accès et des actions de l'ARC (enregistrement comprenant l'auteur individuellement identifié, l'horodatage, la nature de l'opération réalisée ainsi que la référence des documents accédés par l'opération.) ;
- **analyse automatique ou manuelle régulière des données de traçabilité** pour détecter toute opération non légitime ;
- **durée de conservation des données envoyées sur la plateforme** strictement limitée à la durée des vérifications (les données envoyées seront effacées à la fin des vérifications, ainsi que les éventuelles sauvegardes de ces données) ;
- conservation des **données de traçabilité pendant 6 mois à un an** ;
- **réalisation d'un audit préalable et formalisé de la plateforme**, afin de s'assurer que ces mesures de sécurité sont mises en place et fonctionnelles.