Recommandations provisoires

CONTRÔLE QUALITÉ À DISTANCE DES ESSAIS CLINIQUES PENDANT LA CRISE SANITAIRE LIÉE A LA COVID-19

Avril 2021

Ce document est applicable jusqu'à un mois après la fin de l'état d'urgence sanitaire, tel que déclaré par le législateur.

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

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 à vérifier, par un « attaché de recherche clinique » (ARC) pour le compte du promoteur, les 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, à l'article 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 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 du patient reste dans le centre d'investigation 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 »*.

Dans le contexte de crise sanitaire actuelle, ce document propose des recommandations pour la consultation **des données sources à distance.**

Périmètre des recommandations

Lignes directrices européennes et essais concernés

Les agences sanitaires au niveau européen (incluant l'Agence Nationale de Sécurité du Médicament et des produits de santé - ANSM) ainsi que l'agence européenne du médicament (EMA) ont adopté des lignes directrices présentant un cadre acceptable à titre exceptionnel, pendant la période d'urgence sanitaire, pour la réalisation du « *monitoring* à distance ».

Le *monitoring* ne nécessitant pas la consultation des données sources (contenant des données nominatives) doit être, dans la période actuelle, toujours privilégié, dès que cela est possible (*monitoring* centralisé par exemple).

Les lignes directrices précisent également le périmètre, les modalités de mise en œuvre et les conditions **de la consultation des données sources à distance d'un patient**.

Elles prévoient **un périmètre restreint des essais concernés par la dérogation,** à savoir **:**

- les études liées à la COVID-19 (traitement ou prévention) ;
- les essais portant sur des maladies graves ou mettant en jeu le pronostic vital ;
- les essais pour lesquels l'absence de contrôle de qualité des documents sources contenant des données critiques est susceptible d'entraîner des risques inacceptables pour la sécurité des participants ou de remettre en cause la fiabilité et l'intégrité des résultats de l'essai ;
- les essais incluant des participants particulièrement vulnérables, tels que des enfants ou des participants incapables de donner leur consentement éclairé de façon temporaire (ex. : essais mis en œuvre dans des situations d'urgence) ou permanente (ex. : essais menés chez des patients atteints de démence avancée) ;
- les essais cliniques « pivots » (par exemple : essais cliniques de phase III confirmatoires en vue d'un dépôt d'AMM).

La CNIL considère que seuls ces essais peuvent bénéficier des dérogations prévues ci-dessous.

Durée de la dérogation

Les solutions alternatives (présentées ci-dessous) et les dérogations doivent être strictement limitées **à la durée de la crise sanitaire actuelle (un mois après la fin de l'état d'urgence sanitaire) et restreintes aux cas dans lesquels les vérifications sur place s'avèrent absolument impossibles.**

Elles ont pour objectif de faire face à la crise sanitaire actuelle, et ne préjugent pas de la volonté de la CNIL et des autres instances compétentes de pérenniser ces modalités.

Quelles formalités auprès de la CNIL ?

Le *monitoring* à distance ne répond pas strictement aux dispositions des méthodologies de références actuelles.

Cependant, **au regard du contexte sanitaire actuel et des circonstances exceptionnelles, la CNIL considère, à titre dérogatoire et strictement temporaire, qu'il n'est pas nécessaire de déposer une demande d'autorisation auprès d'elle si la mise en œuvre d'un *monitoring* à distance constitue le seul point de non-conformité aux MR, à la stricte condition de respecter l'ensemble des exigences prévues ci-dessous, en fonction de la solution retenue.**

La CNIL demande à l'ensemble des acteurs d'être extrêmement vigilants sur ce dispositif et de faire remonter, par le biais de leur fédérations professionnelles ou organismes les représentant les éventuelles difficultés ou incidents rencontrés, les pistes d'amélioration ainsi que les retours des personnes concernées.

Il reviendra au responsable de traitement (promoteur) et ses sous-traitants (société prestataire de services gérant la plateforme technologique, centre investigateur etc.) **de documenter les solutions qu'ils ont choisies** pendant cette période et d'être en mesure de démontrer qu'elles présentent des garanties suffisantes pour les droits et libertés des personnes concernées au regard de leur situation, ainsi que leur conformité aux présentes recommandations.

A noter : dans l'hypothèse où le traitement envisagé nécessite une autorisation de la CNIL, il conviendra de documenter dans le dossier de demande la conformité du *monitoring* à distance avec l'ensemble de ces exigences.

Avis du comité de protection des personnes (CPP) et information de l'ANSM

La CNRIPH considère que la mise en œuvre d'une modalité de contrôle de qualité par un *monitoring* dématérialisé pour une recherche en cours constitue une modification substantielle à adresser pour avis au comité de protection des personnes.

L'ANSM considère qu'elle devra être informée de la modification substantielle (**modification substantielle pour information - MSI),** conformément aux modalités habituelles prévues par l'ANSM.

Comment informer les personnes concernées ?

Les personnes concernées doivent être informées au préalable de cette nouvelle modalité de consultation et ne doivent pas s'y être opposées.

Pour les nouvelles études, les modalités de *monitoring* à distance devront être précisées dans le document d'information prévu à l'article L. 1122-1 du CSP.

Pour les études en cours, la note d'information délivrée devra 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 dossier médical d'une personne s'étant opposée ne pourra pas faire l'objet d'un contrôle qualité à distance.

Quelles sont les conditions générales à respecter ?

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

En outre, les lignes directrices européennes restreignent **le type de données** pouvant faire l'objet de ces mesures temporaires (données critiques concernant le critère principal d'évaluation, données de sécurité importantes, ainsi que les données importantes concernant les critères secondaires d'évaluation de l'efficacité si elles ne nécessitent pas l'accès à des documents complémentaires et si leur consultation n'alourdit pas la charge de travail du personnel du lieu de recherches).

Consultation du délégué à la protection des données et documentation

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

Des procédures spécifiques devront 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 de l'ARC et dates/horaires du contrôle etc.).

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

Au sein du lieu de recherche, **le DPO 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 *monitoring* à distance ne devrait 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.

Enfin, il sera 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 secret professionnel de l'ARC

L'ARC, en tout état de cause, 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, traitement, administration** des outils depuis l'Union européenne ;
- **absence de recours à des prestataires soumis au droit américain ou aux réglementations de pays n'encadrant pas suffisamment les accès aux données par les autorités judiciaires ou de renseignement**, sauf à ce que des mesures de sécurité parfaitement conformes aux recommandations du CEPD (Comité européen de la protection des données) soient mises en œuvre ;
- le recours à un **hébergeur de données de santé** (HDS) est recommandé ;
- **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 *monitoring* à distance ;
- **restriction de la durée des accès pour ces profils** (par 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** conformes à la recommandation de la CNIL, **logiciels de détection de logiciels malveillants à jour, connexion à un réseau sécurisé,** *etc.*) ;
- « surveillance » à posteriori ou en temps réel **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. *Monitoring* via une vidéoconférence avec le centre d'investigation (solution à privilégier)

La solution de vidéoconférence **a l'avantage de correspondre au mieux 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. Aucune fonctionnalité de type « prise en main à distance » ne doit pouvoir être utilisée par l'ARC.

Recommandations complémentaires :

- 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 mot de passe spécifique pour chaque session**

de vidéoconférence et utilisation d'une zone d'attente permettant à l'administrateur 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 forte** si cela est possible) ;
- **conservation des données de traçabilité pendant 6 mois** 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 qui seront consultées par les ARC doivent permettre d'assurer un contrôle qualité fiable, conformément aux bonnes pratiques cliniques et ne devraient pas, en principe, nécessiter de manipulation spécifique du centre d'investigation (par exemple, en étant contraint 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 devra contenir que les données strictement nécessaires au suivi, et devra permettre une traçabilité exhaustive des actions de l'ARC.

Recommandations complémentaires :

- **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 forte**, comprenant au moins deux facteurs d'authentification différents, 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 accès aux données** par le centre : enregistrement de traces d'accès permettant un audit complet des actions de l'ARC (horodatage des connexions réalisées pour chacun des comptes, des données accédées, des actions réalisées, *etc.*) ;
- **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 sauvegardes de ces données ;
- conservation des **données de traçabilité pendant 6 mois** ;
- **réalisation d'un audit préalable de la plateforme par un tiers indépendant,** afin de s'assurer que ces mesures de sécurité sont mises en place et fonctionnelles ;

3. Accès direct au dossier médical électronique (« *Electronic Medical Record* » - *EMR*) par l'ARC

Cette solution nécessite des précautions complémentaires et une surveillance accrue du centre d'investigation, au moment du contrôle qualité et **n'est pas celle devant être privilégiée.**

En aucun cas, l'ARC ne doit pouvoir visualiser les données de patients autres que ceux participant à l'étude. Ainsi, si le logiciel lié au dossier médical électronique ne permet pas de restreindre la visualisation des données aux seuls patients inclus dans l'étude faisant l'objet du contrôle de qualité des données, cette solution ne doit pas être retenue.

Recommandations complémentaires :

- mise en place de **comptes nominatifs** et d'une **authentification forte**, comprenant au moins deux facteurs d'authentification différents, pour l'ensemble des profils pouvant avoir accès au système d'information du centre d'investigation ;
- connexion au système d'information du centre d'investigation via l'utilisation d'un **réseau virtuel privé** (« VPN ») garantissant une authentification et un chiffrement des communications conformes à l'état de l'art, par exemple en utilisant les protocoles IPsec ou TLS ;
- mise en place de **mesures de filtrage** afin de s'assurer que les ARC n'auront accès qu'aux applications et données nécessaires à leur vérification ;
- **surveillance** par le centre d'investigation :
    - **en temps réel** : enregistrement et contrôle des actions de l'ARC en direct par un membre du centre d'investigation, par exemple via l'enregistrement de la session RDP de l'ARC par un bastion d'administration ou via l'installation d'un logiciel de capture vidéo sur le poste auquel l'ARC sera connecté ;
    - ou **à posteriori** : enregistrement des actions de l'ARC et/ou enregistrement de traces d'accès permettant un audit complet des actions de l'ARC (horodatage des connexions réalisées pour chacun des comptes, des données accédées, des actions réalisées, *etc.*)
- **analyse automatique ou manuelle régulière des données de traçabilité** (traces techniques et fonctionnelles, ou vidéo) pour détecter toute opération non légitime ;
- conservation des **données de traçabilité pendant 6 mois** ;
- **réalisation d'un audit préalable du système d'information** par le centre d'investigation afin de s'assurer que ces mesures de sécurité sont mises en place et fonctionnelles.