CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Annexe sécurité

Pour les méthodologies de référence (MR)

Version avril 2026

Table des matières

I. Objectif du document

Les exigences de sécurité décrites dans cette annexe 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. Ces méthodologies de référence peuvent également comporter des mesures de sécurité spécifiques.

En outre, ces mesures constituent un état de l'art auquel peut se référer tout responsable de traitement de données dans le cadre de recherches en santé.

II. Mesures générales de sécurité

Numéro	Titre	Exigence de sécurité
Préparation et conception		
MR-SEC-01	Piloter la protection des données	Identifier les acteurs compétents en matière de protection des données et de sécurité informatique, dont le délégué à la protection des données et le responsable de la sécurité des systèmes d'information. S'assurer que le projet de recherche est conforme à la politique générale de protection des données de l'organisme.
MR-SEC-02	Sécurité dès la conception	Intégrer la protection des données et les mesures de sécurité dès la phase de conception de la recherche. Associer les acteurs compétents en matière de protection des données et de sécurité informatique à la conception des protocoles de recherche et au suivi du projet.
MR-SEC-03	Évaluation des risques	À partir de l'analyse des risques pour les droits et libertés des personnes concernées, définir un plan d'action et mettre en œuvre les mesures techniques et organisationnelles spécifiques pour assurer la protection des données du projet. Revoir régulièrement l'analyse de risques, en particulier en cas de modification du système ou du contexte du traitement.

Numéro	Titre	Exigence de sécurité
Minimisation et pseudonymisation		
MR-SEC-04	Minimisation des données	Minimiser les données traitées (filtrage, transformation, réduction, agrégation, purge, etc.) dès que possible et à toutes les étapes de la recherche.
MR-SEC-05	Séparation par nature de donnée	Dans le cas d'une recherche nécessitant un suivi individuel des personnes se prêtant à la recherche, séparer les données administratives (nom, prénom, identifiant patient permanent, etc.) et les données de santé concernant ces personnes.
MR-SEC-06	Pseudonymisation	Indexer les données de la recherche à l'aide d'un code non signifiant, en appliquant les exigences MR-CNS-01 à 04. Définir les modalités de réidentification des personnes se prêtant à la recherche.
MR-SEC-07	Images médicales	Pseudonymiser les images médicales par masquage des données identifiantes et suppression des métadonnées identifiantes. Prendre en compte dans l'évaluation des risques la présence de particularités visuelles permettant la réidentification des personnes (par exemple, tatouages, prothèses, malformations) et mettre en œuvre les mesures appropriées pour réduire la possibilité de réidentification (par exemple, exclure certaines images, masquer les particularités qui ne sont pas utiles à la recherche).
MR-SEC-08	Purge des données	Effacer les données de la base active à l'expiration de leur durée de conservation.

Numéro	Titre	Exigence de sécurité
Protection des données		
MR-SEC-09	Chiffrement des données	Sécuriser les données au repos et en transit, à l'aide de chiffrement ou de mesures de sécurité équivalentes. Utiliser des algorithmes cryptographiques à l'état de l'art, reconnus et sûrs. Définir une politique de gestion des clés secrètes. Protéger les clés secrètes avec des droits d'accès restrictifs et des mots de passe sûrs.
MR-SEC-10	Identification des utilisateurs	Définir un identifiant unique par utilisateur et interdire les comptes partagés entre plusieurs utilisateurs.
MR-SEC-11	Mots de passe	Respecter la recommandation de la CNIL relative aux mots de passe1.
MR-SEC-12	Authentification multifacteur	Conditionner l'accès aux données à caractère personnel des personnes se prêtant à la recherche à une authentification multifacteur2 faisant intervenir a minima deux facteurs d'authentification distincts.
MR-SEC-13	Gestion des accès	Définir des profils d'accès en séparant les tâches et les domaines de responsabilité, afin de limiter l'accès des utilisateurs aux seules données strictement nécessaires à l'accomplissement de leurs missions. Faire valider toute demande d'attribution de profil d'accès par un responsable hiérarchique. Limiter l'accès aux outils et interfaces d'administration fonctionnelle aux seules personnes autorisées. Modifier les profils d'accès des utilisateurs en cas de changement de mission, de poste ou à la fin de leur contrat. Réaliser une revue régulière, au moins annuelle, des droits d'accès.
MR-SEC-14	Journalisation	Mettre en place un système de journalisation des activités métier des utilisateurs, des interventions techniques, des anomalies et des évènements liés à la sécurité. Identifier les données de santé éventuellement présentes dans les traces, les minimiser et sécuriser les traces en conséquence. Analyser de manière proactive, en temps réel ou à court terme, les traces collectées pour être en mesure de détecter la survenue d'un incident.
MR-SEC-15	Documents papier	Sécuriser les documents papier existants (stockage, transmission, destruction).

[1] Recommandation relative aux mots de passe et autres secrets partagés - délibération 2022-100 du 21 juillet 2022
[2] Au sens où elle est définie au 2.2 de la recommandation relative à l'authentification multifacteur - délibération

Numéro	Titre	Exigence de sécurité
Sécurisation des outils et équipements		
MR-SEC-16	Sécurisation du parc informatique	Activer le verrouillage automatique des appareils et exiger un secret pour les déverrouiller. Chiffrer les appareils. Désactiver l'exécution automatique de programmes. Limiter au strict besoin opérationnel les droits d'administration.
MR-SEC-17	Sécurité physique	Restreindre et contrôler les accès physiques aux locaux hébergeant les données.
MR-SEC-18	Protection contre les logiciels malveillants	Installer et mettre à jour régulièrement des antivirus, pare-feu et systèmes de détection d'intrusions sur l'ensemble des serveurs et postes de travail maîtrisés par le responsable de traitement. Déployer rapidement les mises à jour de sécurité, et particulièrement lorsqu'elles viennent corriger des failles critiques publiques.
MR-SEC-19	Cloisonnement des données de santé	Cloisonner le traitement des données de santé par rapport au reste du système d'information de l'organisme. Utiliser des logiciels dédiés à la recherche (cahiers d'observation électroniques, questionnaires, etc.) et hébergés sur des serveurs dédiés à la recherche.
MR-SEC-20	Gestion des supports amovibles	Interdire l'utilisation de supports amovibles (clés USB, disques durs externes, etc.) non maîtrisés par le responsable de traitement. En cas d'utilisation de supports amovibles maîtrisés, chiffrer les données sur ces supports et les supprimer après utilisation. Déployer des solutions permettant d'inspecter le contenu des supports dès la connexion.
MR-SEC-21	Équipements non maîtrisés	Interdire l'utilisation d'équipements personnels (« bring your own device ») pour l'accès aux données de la recherche. En cas d'utilisation de matériels professionnels non contrôlés par le responsable de traitement, évaluer les risques liés, définir des mesures spécifiques de réduction des risques et limiter en conséquence les données et les applications accessibles sur ces appareils. Formaliser par écrit les responsabilités et les précautions à respecter.

Numéro	Titre	Exigence de sécurité
Collaboration et sous-traitance		
MR-SEC-22	Encadrement des sous-traitants	Prévoir les obligations des parties concernant la sécurité du traitement dans le contrat avec les sous-traitants. S'assurer que les sous-traitants sont contractuellement tenus de notifier dans les plus brefs délais toute anomalie ou tout incident de sécurité au responsable de traitement.
MR-SEC-23	Échanges distants	Protéger les flux et les enregistrements lors des téléconsultations et entretiens à distance. Vérifier l'identité des personnes contactées. Sécuriser l'envoi dématérialisé de documents, en particulier les notes d'information et le contrôle qualité à distance.
MR-SEC-24	Transmission de données	Sécuriser les échanges de données (par exemple, transferts depuis les centres investigateurs). En cas d'envoi sur un réseau public (par exemple, internet, messagerie électronique), chiffrer les données avec des algorithmes cryptographiques à l'état de l'art, reconnus et sûrs. Assurer la confidentialité de la clé de chiffrement en la transmettant via un canal distinct.

Numéro	Titre	Exigence de sécurité
Documentation et sensibilisation		
MR-SEC-25	Documentation	Documenter les procédures d'exploitation des données. Les tenir à jour et les rendre disponibles à tous les utilisateurs concernés, dans un langage clair et adapté à chaque catégorie d'utilisateurs.
MR-SEC-26	Sensibilisation des utilisateurs	Sensibiliser tous les utilisateurs (internes et externes) travaillant avec des données personnelles aux risques liés aux libertés et à la vie privée des personnes, ainsi qu'aux obligations liées au secret médical et au traitement de données de santé. Les informer des mesures prises pour traiter ces risques et des conséquences potentielles en cas de manquement. S'assurer qu'ils ont assimilé les bonnes pratiques relatives à la protection des données personnelles à mettre en œuvre au quotidien.

Numéro	Titre	Exigence de sécurité
Gestion des incidents et sauvegardes		
MR-SEC-27	Gestion des incidents	Diffuser à tous les utilisateurs, internes comme externes, la conduite à tenir et la liste des personnes à contacter en cas de violation de données, d'incident de sécurité ou de survenance d'un évènement inhabituel touchant aux systèmes d'information et de communication de l'organisme. Sensibiliser les utilisateurs à l'importance de signaler tout évènement suspect.
MR-SEC-28	Sauvegardes régulières	Effectuer des sauvegardes fréquentes des données. Protéger les données sauvegardées avec des mesures de sécurité appropriées pour un niveau de risque équivalent à celui des données d'exploitation. Vérifier régulièrement leur intégrité et la capacité de les restaurer. Supprimer les sauvegardes une fois la durée de conservation expirée.

Numéro	Titre	Exigence de sécurité
Fin de cycle		
MR-SEC-29	Gestion des données après publication	Définir une politique d'archivage sécurisé des données après publication, précisant en particulier les durées de conservation, les conditions d'accès, ainsi que les procédures de purge ou de versement aux Archives nationales.
MR-SEC-30	Destruction sécurisée des données	À la fin du projet de recherche, effacer de façon sécurisée les données présentes sur l'ensemble du matériel informatique (par exemple, poste de travail, serveur, disque dur) et ne conserver que les données prévues par la politique d'archivage définie (MR-SEC-29). En cas de réaffectation ou mise au rebut d'un matériel informatique au cours du projet, effacer préalablement de façon sécurisée les données présentes sur celui-ci.

III. Mesures de sécurité pour la délivrance de la note d'information au format électronique

Numéro	Titre	Exigence de sécurité
MR-INF-01	Note d'information dématérialisée	L'information individuelle des personnes se prêtant à la recherche est délivrée au format électronique dans le respect des conditions définies aux exigences MR-INF-02 à 04.
MR-INF-02	Information par courrier électronique simple	Dans le cas où la note d'information ne révèle aucune information sur l'état de santé de la personne se prêtant à la recherche, elle peut être transmise par simple courrier électronique sous réserve que le responsable de traitement s'assure que les coordonnées électroniques constituent une adresse personnelle et individuelle et soient effectivement utilisées par la personne se prêtant à la recherche ou ses représentants légalement habilités.
MR-INF-03	Information par courrier électronique avec un code d'accès	Dans le cas où la note d'information est susceptible de révéler des informations sur l'état de santé de la personne se prêtant à la recherche, elle peut être transmise par courrier électronique à condition de respecter les conditions cumulatives suivantes : - le corps et l'objet du message ne doivent contenir aucune information susceptible de révéler des informations sur l'état de santé de la personne se prêtant à la recherche ; - l'accès à la note d'information doit être conditionné à la possession d'un facteur de connaissance (par exemple, la note d'information peut être une pièce jointe chiffrée, ou le message peut contenir un lien vers une plateforme sécurisée de téléchargement exigeant un code secret) ; - le code de déchiffrement ou de téléchargement doit être transmis par un canal de confiance séparé (par exemple, remise en main propre, appel téléphonique ou SMS vers un numéro de téléphone vérifié, pli postal sécurisé) ; - dans le cas d'utilisation d'une plateforme sécurisée de téléchargement, une durée limitée de mise à disposition doit être paramétrée.
MR-INF-04	Information via une plateforme sécurisée	Dans le cas où la note d'information est susceptible de révéler des informations sur l'état de santé de la personne se prêtant à la recherche, elle peut être transmise via une plateforme sécurisée pour laquelle la personne se prêtant à la recherche dispose d'une connexion authentifiée, permettant de s'assurer que le message sera lu uniquement par son destinataire. Une notification doit être envoyée par la plateforme au destinataire pour l'inviter à se connecter. Cette notification ne doit contenir aucune information susceptible de révéler des informations sur l'état de santé de la personne se prêtant à la recherche.

IV. Mesures de sécurité pour la revue et la publication des résultats

Numéro	Titre	Exigence de sécurité
MR-PUB-01	Minimisation des données pour la revue des résultats	Pour la revue des résultats, les données mises à disposition des experts indépendants doivent être constituées uniquement des données minimisées (MR-SEC-04) et pseudonymisées (MR-SEC-06) utilisées pour obtenir les résultats publiés et strictement nécessaires à leur revue.
MR-PUB-02	Solution sécurisée pour la revue des résultats	La solution de mise à disposition des données pour la revue doit assurer : - la délivrance d'habilitations offrant des accès différenciés aux données ; - une authentification des utilisateurs ; - le recours à des canaux de communication chiffrés ; - le recours à des algorithmes de chiffrement et des procédures de gestion des secrets à l'état de l'art ; - la mise en œuvre de mesures de traçabilité des accès aux données.
MR-PUB-03	Restrictions des possibilités de copie de données	Les accédants aux données mises à disposition ne doivent pas pouvoir procéder à leur copie ou à leur extraction (par exemple, bloquer les copies d'écran, les copier/coller, les téléchargements).

V. Code non signifiant

Numéro	Titre	Exigence de sécurité
MR-CNS-01	Indexation des données par un code non signifiant	Lorsqu'il est nécessaire de relier entre elles les données se rapportant à une même personne se prêtant à la recherche, au sein d'un jeu de données pseudonymisées ou entre plusieurs jeux de données pseudonymisées, l'indexation doit se faire uniquement à l'aide d'un code non signifiant répondant aux exigences MR-CNS-02 à 04.
MR-CNS-02	Code non signifiant	Un code non signifiant ne doit pas révéler d'information sur la personne concernée ou des identifiants préexistants liés à cette personne. Il ne doit pas contenir d'identifiants préexistants, ni une troncature ou une concaténation de ceux-ci. En particulier, il ne doit pas contenir d'information liée aux traits d'identité des personnes concernées (par exemple, les initiales, la date de naissance), au soin (NIR-INS, IPP, IEP), à la phase de collecte des données (numéro d'inclusion, numéro de tube d'un prélèvement biologique) ou à l'identifiant dans un jeu de données source. Il doit être généré spécifiquement pour le jeu de données.
MR-CNS-03	Méthodes de génération du code non signifiant	Un code non signifiant doit être généré au moyen de l'une des deux méthodes suivantes : - utilisation d'un générateur de valeurs aléatoires (par exemple, un générateur de nombres pseudo-aléatoires, « PRNG ») ; - dérivation à partir d'un identifiant préexistant au moyen d'une fonction de hachage paramétrée par une clé secrète. La fonction de hachage utilisée doit être une fonction cryptographique à l'état de l'art. La clé secrète doit être encadrée par une politique de gestion de clé.
MR-CNS-04	Encadrement des moyens de réidentification	Le responsable de traitement doit s'assurer qu'il ne soit pas possible de faire le lien entre un code non signifiant et d'autres identifiants concernant les personnes se prêtant à la recherche, sans avoir accès à une information supplémentaire, à savoir la table de correspondance entre le code non signifiant et un identifiant préexistant, ou la clé secrète utilisée pour générer le code à l'aide d'une fonction de hachage. Cette information supplémentaire ne doit être conservée que s'il est strictement nécessaire d'être en mesure de faire ultérieurement le lien entre le code non signifiant et d'autres identifiants concernant les personnes se prêtant à la recherche. Son accès doit être strictement encadré et limité à un nombre restreint de personnes dûment habilitées.