RÉFÉRENTIEL

RELATIF AUX TRAITEMENTS DE DONNÉES A CARACTÈRE PERSONNEL MIS EN ŒUVRE A DES FINS DE CRÉATION D'ENTREPÔTS DANS LE DOMAINE DE LA SANTÉ

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

1. À qui s'adresse ce référentiel ?

1.1 **Ce référentiel encadre exclusivement les traitements de données à caractère personnel constitués afin de permettre la réutilisation des données réunies à des fins de recherche ou d'évaluation en santé, de production d'indicateurs et le pilotage stratégique de l'activité d'un établissement ou centre où s'exercent des activités de prévention, de diagnostic et de soins**.

1.2 Ces traitements sont ci-après dénommés « entrepôts de données de santé ».

1.3 Ne sont pas concernés par ce référentiel : les traitements de données à caractère personnel nécessaires aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de services de santé et mis en œuvre par les professionnels de santé et les systèmes ou services de soins de santé, par application des dispositions du 1° de l'article 65 de la loi du 6 janvier 1978 modifiée.

1.4 Le référentiel s'applique également aux entrepôts mis en œuvre par des responsables conjoints qui définissent leurs obligations respectives conformément à l'article 26 du RGPD.

2. Portée du référentiel

2.1 Ce référentiel précise le cadre juridique, issu du règlement général sur la protection des données (RGPD) et des dispositions nationales, applicable aux entrepôts de données de santé.

2.2 Les responsables de traitement qui réalisent auprès de la CNIL un engagement de conformité au présent référentiel sont autorisés à mettre en œuvre un entrepôt de données de santé dans la mesure où le traitement est strictement conforme au référentiel.

2.3 Tout traitement de données à caractère personnel visant à mettre en œuvre un entrepôt de données de santé qui ne respecte pas l'ensemble des exigences définies par le présent référentiel doit faire l'objet d'une demande d'autorisation spécifique, conformément aux dispositions de l'article 66 III de la loi du 6 janvier 1978 modifiée.

2.4 Les responsables de traitement doivent mettre en œuvre toutes les mesures appropriées (techniques et organisationnelles) afin de garantir la protection des données à caractère personnel traitées, à la fois dès la conception du traitement et par défaut, comme prévu à l'article 25 du RGPD. Ils doivent, en outre, démontrer cette conformité tout au long de la vie des traitements. Les traitements mis en œuvre dans le cadre du référentiel doivent également être inscrits dans le registre des activités de traitement prévu à l'article 30 du RGPD.

2.5 Les principes posés par la CNIL dans ce référentiel constituent également une aide à la réalisation de l'analyse d'impact à la protection des données (AIPD) que les responsables de traitement concernés doivent mener conformément au point 13 du présent référentiel.

2.6 Par application de l'article 65.1 de la loi « informatique et libertés », les entrepôts mis en œuvre après recueil du consentement conforme à l'article 7 du RGPD sur la base de l'article 9.2.a du RGPD de chaque personne concernée ne sont pas soumis à une autorisation préalable de la Commission. La Commission rappelle toutefois que les principes et les mesures posés par le présent référentiel sont applicables à l'ensemble des traitements de données de santé de même nature, indépendamment de leur encadrement juridique.

2.7 Les traitements de données de santé à caractère personnel mis en œuvre à des fins de recherche dans le domaine de la santé, à partir des données contenues dans l'entrepôt, constituent des traitements distincts qui doivent faire l'objet des formalités nécessaires au titre des articles 66 et 72 et suivants de la loi « informatique et libertés ».

3. Objectif(s) poursuivi(s) par le traitement (Finalités)

3.1 Les traitements encadrés par le présent référentiel sont mis en œuvre afin de constituer un entrepôt de données de santé en vue de leur réutilisation à des fins :

- de recherche, d'étude ou d'évaluation dans le domaine de la santé ;
- de production d'indicateurs et de pilotage stratégique de l'activité du ou des établissements ou centre où s'exercent des activités de prévention, de diagnostic et de soins concernés.

3.2 Les données contenues dans les traitements réalisés dans le cadre de ce référentiel ne peuvent être exploitées à des fins de promotion des produits mentionnés au II de l'article L. 5311-1 du code de la santé publique en direction de professionnels de santé ou d'établissements de santé, ni à des fins d'exclusion de garanties des contrats d'assurance ni de modification de cotisations ou de primes d'assurance d'un individu ou d'un groupe d'individus présentant un même risque.

3.3 Une gouvernance spécifique à chaque entrepôt est mise en œuvre par le responsable de traitement. Une première instance (comité de pilotage ou équivalent) détermine les orientations stratégiques et scientifiques de l'entrepôt. Il est de son ressort de tenir une liste exhaustive des données de l'entrepôt et de justifier de leur nécessité, dans la limite des données listées au 5.1 du présent référentiel.

3.4 Une seconde instance (comité scientifique et éthique ou équivalent) rend, de manière systématique, un avis préalable et motivé sur les propositions de projets nécessitant la réutilisation des données de l'entrepôt. Seuls les projets ayant été examinés par cette instance peuvent avoir recours à l'entrepôt. Cette deuxième instance comprend notamment au moins une personne impliquée dans l'éthique en santé et indépendante du responsable de traitement, ainsi que plusieurs professionnels de santé et chercheurs.

4. Base(s) légale(s) du traitement

4.1 Les entrepôts de données de santé constitués dans le cadre du présent référentiel sont fondés sur l'exercice d'une mission d'intérêt public, au sens de l'article 6-1-e du RGPD.

5. Données à caractère personnel pouvant être incluses dans l'entrepôt

5.1 Dans le cas où des données directement identifiantes ou des tables de correspondance sont stockées dans l'entrepôt, celles-ci doivent être séparées logiquement des données pseudonymisées, en utilisant les procédés décrits dans les exigences de sécurité SEC-LOG-4 à SEC-LOG-6.

5.2 Seules des données à caractère personnel adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités du traitement peuvent être collectées et traitées. À ce titre, le responsable de traitement ne peut collecter et traiter que les catégories de données suivantes et lorsque :

- celles-ci figurent déjà dans le dossier médical des personnes concernées et que leur collecte était justifiée par leur prise en charge ;
- celles-ci sont issues de projets de recherche précédemment réalisés et que leur durée de conservation n'a pas expiré.

5.3 Les données traitées peuvent inclure :

5.3.1 Des données relatives aux patients :

5.3.1.1 Données directement identifiantes et administratives relatives aux patients devant être conservées dans un espace distinct des autres données :

- nom, prénom ;
- jour, mois, date et de lieu de naissance ;
- coordonnées téléphoniques, électroniques et adresse de résidence ;
- numéro d'identifiant permanent du patient (IPP).

5.3.1.2 Données sensibles :

- poids, taille, compte rendus médicaux, résultats d'examens, résultats issus d'analyse d'échantillons biologiques, imagerie médicale, données relatives aux effets et événements indésirables ;
- antécédents personnels ou familiaux, maladies ou événements associés ;
- données médico-administratives issues du PMSI local.

5.3.1.3 Autres catégories de données à caractère personnel :

- photographie et/ou vidéo et/ou enregistrements vocaux ne permettant pas l'identification directe des personnes concernées (par exemple, avec masquage du visage, des yeux, des signes distinctifs) et recueillies dans des conditions conformes aux dispositions applicables en matière de droit à l'image et de droit à la voix ;
- données génétiques strictement nécessaires pour répondre aux objectifs ou finalités de l'entrepôt, ne pouvant en aucun cas être utilisées aux fins d'identification ou de réidentification des personnes et recueillies dans le cadre de la prise en charge médicale de la personne concernée ou d'un projet de recherche, sous réserve que le consentement exprès de la personne concernée ait été recueilli préalablement à la réalisation de l'examen, conformément aux dispositions de l'article L. 1131-1 du code de la santé publique et qu'elle ait été informée à cette occasion de la possibilité de réutilisation des résultats obtenus à des fins de recherche ultérieure.
- données relatives à la vie professionnelle (profession, historique d'emploi, chômage, trajets et déplacements professionnels, expositions professionnelles, catégorie INSEE socioprofessionnelle, etc.) ;
- niveau de formation (par exemple : primaire, secondaire, supérieur) ;
- régime d'affiliation à la sécurité sociale, assurance complémentaire (mutuelle, assurance privée) ;
- déplacements (par exemple vers le lieu de soin ou de la recherche : mode, durée, distance) ;
- consommation de tabac, alcool, drogues ;
- habitudes de vie et comportements, par exemple : dépendance (seul, en institution, autonome, grabataire), assistance (aide-ménagère, familiale), exercice physique (intensité, fréquence, durée), régime et comportement alimentaire, loisirs ;
- mode de vie (par exemple : urbain, semi-urbain, nomade, sédentaire), habitat (maison particulière, immeuble, étage, ascenseur, etc.) ;
- vie sexuelle ;
- statut vital, lorsque cette information figure dans le dossier médical détenu par le responsable de traitement ou est connue par un professionnel de santé ayant participé à la prise en charge du patient ;
- échelle de qualité de vie ou autres informations sur la qualité de vie de la personne.

5.3.2 Des données relatives aux professionnels de santé

- données d'identification : nom, prénom, titre ;
- fonction, service et unité d'exercice ;
- coordonnées professionnelles (adresse électronique et numéro de téléphone professionnels) ;
- matricule (à l'exclusion du numéro ADELI ou numéro RPPS).

5.4 Le recours à chacune de ces données pour toute réutilisation devra être justifié dans le protocole soumis à la gouvernance de l'entrepôt.

5.5 Les données directement identifiantes mentionnées au point 5.3.1.1 ne peuvent être collectées dans l'entrepôt que pour les finalités suivantes :

- recontacter les patients pour leur proposer de participer à des études ;
- recontacter les patients à la suite de découvertes annexes liées à l'analyse de leurs caractéristiques génétiques, à l'exception des cas dans lesquels le patient a exprimé par écrit sa volonté d'être tenu dans l'ignorance du diagnostic, conformément à l'article L. 1131-1-2 du code de la santé publique ;
- avertir une personne d'un risque sanitaire grave auquel elle est exposée.

5.6 Les données indirectement identifiantes mentionnées au point 5.3.1.1 ne peuvent être utilisées que si les finalités du traitement le justifient. À titre d'exemple, le jour de naissance ne pourra être utilisé que s'il est nécessaire à la réalisation d'une recherche impliquant des personnes âgées de moins de deux ans.

5.7 La pertinence des données comprises dans l'entrepôt doit être ré-évaluée régulièrement, et les données n'apparaissant plus nécessaires doivent être supprimées.

5.8 Les entrepôts mis en œuvre dans le champ du présent référentiel ne peuvent faire l'objet d'un appariement pérenne avec les données du Système national des données de santé tel que défini à l'article L. 1461-1 du code de la santé publique.

6. Destinataires des informations

6.1 Le responsable de traitement d'un entrepôt de données de santé doit prêter une attention particulière à la gestion des droits d'accès des personnes habilitées à accéder aux données contenues dans l'entrepôt.

6.2 L'accès et l'usage des données directement identifiantes doit être restreint aux finalités listées au point 5.5 et aux seules personnes chargées de la réalisation des opérations nécessaires à l'accomplissement de ces finalités.

6.3 Peuvent être destinataires de données pseudonymisées strictement nécessaires à la réalisation des objectifs de leurs projets de recherche, d'étude ou d'évaluation, les équipes de recherche internes ou externes au responsable de traitement habilitées à cet effet.

6.4 Le personnel interne au responsable de traitement habilité à cet effet peut être destinataire de données pseudonymisées strictement nécessaires à l'accomplissement de leurs missions correspondant aux finalités de l'entrepôt.

6.5 Lorsque les données font l'objet d'un processus d'anonymisation[1] au sein d'un espace projet de l'entrepôt, les données anonymes en résultant peuvent être transmises à tout destinataire.

7. Durées de conservation

7.1 La durée de conservation des données de l'entrepôt de données de santé doit répondre aux exigences prévues à l'article 5 1.e du RGPD.

7.2 Les données mentionnées aux points 5.3.1.2 et 5.3.1.3 peuvent être conservées 20 ans maximum à compter de leur collecte dans le cadre des soins ou des recherches. Les données mentionnées au point 5.3.1.1 doivent être supprimées lorsque le délai de conservation des données mentionnées aux points 5.3.1.2 et 5.3.1.3 a expiré.

7.3 Au-delà de ces durées, toute donnée doit être irréversiblement anonymisée ou détruite.

8. Information des personnes

8.1 L'information des patients :

Les personnes doivent être informées par l'établissement ou centre où s'exercent des activités de prévention, de diagnostic et de soins que les données collectées lors de leur prise en charge sont versées au sein de l'entrepôt. L'information relative à la constitution de l'entrepôt ne saurait se substituer à l'information individuelle préalable prévue par les dispositions du RGPD et de la loi « informatique et libertés », qui devra être réalisée pour chaque traitement de données réalisé à partir des données de l'entrepôt à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé.

8.2 L'information relative à la constitution de l'entrepôt pour les données issues de dossiers médicaux

8.2.1 Lors de la constitution d'un entrepôt, une première information relative à la constitution d'un entrepôt doit être transmise aux personnes concernées. Lors de la réutilisation des données de l'entrepôt à des fins de recherche, une autre information devra être transmise aux personnes concernées (point 13).

[1] Conformément aux critères du G29 ou tout avis futur du CEPD.

8.2.2 *Collecte des informations auprès des nouveaux patients et de ceux en cours de suivi (article 13)*

8.2.2.1 Les nouveaux patients ainsi que ceux en cours de suivi sont informés individuellement de la constitution de l'entrepôt. Le ou les supports d'information utilisés comprennent l'ensemble des éléments prévu à l'article 13 du RGPD.

8.2.2.2 La réutilisation des données ainsi que les modalités d'exercice des droits d'accès et d'opposition doivent être particulièrement mis en avant dans la note d'information.

8.2.3 Collecte des informations issues de dossiers médicaux de patients n'étant plus suivis (article 14)

8.2.3.1 Les patients n'étant plus suivis sont informés individuellement de la constitution de l'entrepôt. Le ou les supports d'information utilisés comprennent l'ensemble des éléments prévu à l'article 14 du RGPD.

8.2.3.2 Ces mentions d'information doivent également intégrer la politique de protection des données à caractère personnel du responsable de traitement.

8.2.3.3 La réutilisation des données ainsi que les modalités d'exercice des droits d'accès et d'opposition doivent être particulièrement mis en avant dans la note d'information.

8.2.3.4 Le responsable de traitement peut faire valoir une exception à l'obligation d'information individuelle s'il justifie dans son registre d'activité de traitement que la fourniture des informations exigerait des efforts disproportionnés, conformément à l'article 14.5.b du RGPD.

8.2.3.5 À ce titre, peuvent notamment être invoqués, au vu de sa situation :

- le nombre de personnes concernées ;
- l'ancienneté des données ;
- le coût et le temps de la délivrance des informations[2].

Une telle exception doit s'entendre strictement et, en tout état de cause, ne peut s'appliquer à la totalité des personnes concernées par le traitement. À titre d'exemple, elle peut s'appliquer aux personnes pour lesquelles le responsable de traitement dispose d'un dossier médical mais qui ne se sont plus suivies au sein de l'établissement ou centre où s'exercent des activités de prévention, de diagnostic et de soins.

8.2.3.6 En cas de recours à l'exception à l'obligation d'information individuelle, le responsable de traitement rend les informations publiquement disponibles, notamment en :

- diffusant la note d'information relative à la constitution de l'entrepôt sur son site web, dans une rubrique dédiée et accessible depuis la page d'accueil, complétée par des informations détaillées sur chaque traitement mis en œuvre à partir des données de l'entrepôt ;
- communiquant sur l'entrepôt sur les réseaux sociaux, dans les médias régionaux, auprès des associations de patients ;
- diffusant un communiqué de presse informant de la mise en place de l'entrepôt.

8.3 L'information relative à l'intégration dans l'entrepôt de données issues de la recherche

8.3.1 Si l'entrepôt intègre des données issues de recherches, les personnes concernées doivent être informées individuellement de la réutilisation des données issues de la recherche afin de constituer un entrepôt conformément aux dispositions de l'article 14 du RGPD. Dans cette hypothèse, le recours à l'exception à l'information individuelle est possible, dans les conditions mentionnées aux points 8.4.4.4 à 8.4.4.6.

8.3.2 Seules des données issues de traitements dont la durée de conservation n'a pas expiré pourront être intégrées dans l'entrepôt de données de santé.

[2] G29, Lignes directrices sur la transparence au sens du règlement (UE) 2016/679, adoptées le 11 avril 2018.

8.4 **Les personnes concernées doivent en outre être informées de <u>de chacune des réutilisations</u> des données la concernant à des fins de recherche, d'étude ou d'évaluation, sauf lorsque les responsables de traitement se trouvent dans l'impossibilité de réaliser l'information ou qu'elle exigerait des efforts disproportionnés.**

8.5 L'information de professionnels de santé

8.6 Concernant l'information des professionnels de santé exerçant au sein des établissements du responsable de traitement :

- Les professionnels dont les données sont versées dans l'entrepôt doivent être informés individuellement par écrit des mentions prévues par l'article 13 du RGPD.
- Si le responsable de traitement est l'employeur des personnels, la fiche d'information pourra prendre la forme d'un courrier joint au bulletin de paie. L'information devra également être diffusée en commission ou conférence médicale d'établissement, sur l'intranet de celui-ci et à l'aide d'affiches dans les lieux de repos des personnels.

8.7 Concernant l'information des professionnels de santé n'exerçant pas au sein des établissements du responsable de traitement :

- Si le responsable de traitement n'est pas l'employeur des personnels dont les données sont collectées dans l'entrepôt, il devra réaliser une information individuelle par écrit de chacun des professionnels, comportant les mentions prévues à l'article 14 du RGPD.

9. Droits des personnes

9.1 Le responsable de traitement diffuse une information générale, via une campagne d'information publique, préalablement à la mise en place de l'entrepôt afin de garantir qu'une période de temps raisonnable s'écoule entre la notification des patients et le commencement du traitement de leurs données afin que ceux-ci puissent faire valoir leur droit d'opposition.

9.2 Les personnes concernées par le traitement (professionnels de santé et patients) disposent des droits suivants, qu'elles exercent dans les conditions prévues par le RGPD :

- droit d'accès ;
- droit de rectification ;
- droit à l'effacement ;
- droit à la limitation du traitement ;
- droit d'opposition.

9.3 Le droit d'opposition des professionnels de santé s'exerce sous réserve des conditions d'exercice de ce droit en application des dispositions de l'article 21 du RGPD.

9.4 Le droit d'opposition des patients doit pouvoir s'exercer dès leur information, par la transmission d'un document papier pouvant être rempli immédiatement ou par une case à cocher par le professionnel, attestant de l'exercice du droit d'opposition.

9.5 Ces droits s'exercent auprès de toute personne spécifiquement formée et habilitée à cette fin par le responsable de traitement, et dont les coordonnées sont communiquées aux personnes concernées. Le cas échéant, il peut s'agir du délégué à la protection des données du responsable de traitement.

9.6 Le responsable de traitement ne peut se prévaloir des dispositions de l'article 11 du RGPD pour limiter l'exercice des droits des personnes concernées. En effet, lorsque les modalités de constitution de l'entrepôt n'impliquent pas la conservation de données identifiantes ou de moyens de correspondance avec l'identité des personnes, le responsable de traitement reste en capacité de répondre aux demandes des personnes si celles-ci fournissent des informations complémentaires permettant la réidentification de leurs données dans l'entrepôt. Le responsable de traitement précisera dans la note d'information les informations qui devront lui être transmises pour l'exercice des droits.

9.7 Dans le cas exceptionnel où les mesures de pseudonymisation mises en œuvre rendent impossible la réidentification fiable d'une personne à partir des informations qu'elle aura transmises, le responsable de traitement en informera la personne en réponse à sa demande.

9.8 En tout état de cause les mécanismes d'alimentation de l'entrepôt doivent permettre aux personnes d'exercer de façon pérenne leur droit d'opposition et peuvent constituer un moyen de réidentifier les données des personnes exerçant leurs autres droits.

10. Sécurité

10.1 De manière générale, le responsable de traitement doit prendre toutes les précautions utiles au regard des risques présentés par son traitement pour préserver la sécurité des données à caractère personnel et, notamment, au moment de leur collecte, durant leur transmission et leur conservation, empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès.

10.2 En particulier, dans le contexte particulier du présent référentiel, le responsable de traitement doit adopter les mesures techniques et organisationnelles suivantes :

Numéros d'exigence	Exigences de sécurité
Cloisonnement réseau	
SEC-RES-1	Le réseau de communication sur lequel l'entrepôt est hébergé ou rendu accessible doit faire l'objet de mesures de cloisonnement séparant les flux réseau spécifiques à l'entrepôt du reste des flux du système d'information.
SEC-RES-2	Des mesures de filtrage doivent également restreindre l'émission et la réception de ces flux réseau aux machines spécifiquement identifiées et autorisées pour le fonctionnement de l'entrepôt.
SEC-RES-3	Toutes les transmissions de données depuis ou vers l'entrepôt doivent faire l'objet de mesures de chiffrement conformes à l'annexe B1 du référentiel général de sécurité (« RGS ») afin d'en garantir la confidentialité.
Cloisonnement logique et cryptographique	
SEC-LOG-1	Le responsable de traitement doit collecter et stocker les données à caractère personnel faisant partie de l'entrepôt sur des systèmes et bases de données distincts de ceux assurant la prise en charge des patients.
SEC-LOG-2	Les données à caractère personnel doivent être chiffrées au repos par des algorithmes et tailles de clé conformes à l'annexe B1 du RGS. Une procédure opérationnelle de gestion des clés doit être formalisée.
SEC-LOG-3	Les sauvegardes de ces données doivent également faire l'objet d'un chiffrement conforme à l'annexe B1 du RGS.

SEC-LOG-4	Dans le cas où des données directement identifiantes ou des tables de correspondance sont stockées dans l'entrepôt, celles-ci doivent être séparées logiquement des données

	pseudonymisées par des moyens cryptographiques. Par exemple, les données administratives des patients et les tables de correspondance doivent être chiffrées différemment des données de santé de l'entrepôt.
SEC-LOG-5	L'accès aux deux catégories de données séparées définies à l'exigence SEC-LOG-4 doit être effectué *via* des moyens d'authentification différents.
SEC-LOG-6	Dans le cas où des données génétiques sont collectées, celles-ci doivent faire l'objet d'un chiffrement distinct avec une clé spécifique par rapport aux autres données de l'entrepôt. La clé de déchiffrement des données génétiques ne doit être mobilisable que par les profils d'habilitation responsables de l'alimentation de l'entrepôt et de l'exportation de données vers un espace de travail.
Constitution et alimentation de l'entrepôt	
SEC-ALI-1	Les circuits de collecte des données doivent faire l'objet de mesures de sécurité appropriées, en particulier le chiffrement des flux, la purge régulière des répertoires de transit et un contrôle d'accès strict aux données collectées.
SEC-ALI-2	Dans le cas où l'entrepôt est alimenté par des logiciels de saisie autorisant également la consultation des données saisies, les accès à ces logiciels doivent être sécurisés *via* une authentification forte conforme à l'exigence SEC-AUT-1.
Pseudonymisation des données	
SEC-PSE-1	Aucun numéro interne tel qu'un numéro de dossier patient ne peut être directement réutilisé comme identifiant au sein de l'entrepôt. Seul un numéro pseudonyme unique peut être utilisé, permettant le cas échéant la correspondance entre les données pseudonymisées stockées dans l'entrepôt et des données directement identifiantes. Ce numéro doit être dédié à un seul entrepôt. Il doit être généré par une fonction de hachage cryptographique résistante aux attaques par force brute ou un générateur de nombres pseudo-aléatoires cryptographiquement sûr.
SEC-PSE-2	Dans le cas où l'entrepôt intègre des jeux de données existants déjà pseudonymisés, un nouveau numéro pseudonyme unique respectant les conditions de l'exigence SEC-PSE-1 doit être généré lors de l'alimentation de l'entrepôt.
SEC-PSE-3	Dans le cas où des données relatives aux professionnels de santé sont collectées, le responsable de traitement doit pseudonymiser ces données.
SEC-PSE-4	Les documents non structurés ajoutés à l'entrepôt, par exemple les comptes-rendus médicaux ou les zones de commentaires libres, doivent faire l'objet d'un processus de floutage avant leur intégration dans l'entrepôt, qui remplacera les données identifiantes des patients et professionnels de santé par des termes génériques. Par exemple, les NIR, nom de naissance, prénom, code postal, ville ou numéro de téléphone seront remplacés par des termes génériques tels que « NIR », « NOM_DE_NAISSANCE », « PRENOM », « CODE_POSTAL », « VILLE » ou « TEL ».
Accès physique aux données	

SEC-PHY-1	L'accès physique aux serveurs et aux locaux hébergeant les infrastructures de l'entrepôt doit être sécurisé par des mesures de protection adéquates. En particulier, des mesures de contrôle d'accès physique doivent être mises en place.
Gestion des habilitations et accès logique aux données	
SEC-HAB-1	Différents profils d'habilitation doivent être prévus afin de gérer les accès aux données en tant que besoin et de façon exclusive.
SEC-HAB-2	Une granularité des accès aux données doit être prévue pour chaque type de profil, par exemple un accès uniquement à des données agrégées, un accès à des données pseudonymisées et un accès à des données directement identifiantes.
SEC-HAB-3	Les personnes habilitées à accéder aux données à caractère personnel doivent être individuellement habilitées selon une procédure impliquant une validation par : - une des instances assurant la gouvernance de l'entrepôt ; ou - par leur responsable hiérarchique dans le cas des ingénieurs et administrateurs système et réseau.
SEC-HAB-4	Les accès privilégiés disposant de droits étendus, notamment pour l'administration et la maintenance doivent être réservés à une équipe restreinte et être limités au strict nécessaire.
SEC-HAB-5	Une revue des habilitations doit être réalisée régulièrement et *a minima* annuellement, ainsi qu'à la fin de chaque projet de recherche utilisant les données de l'entrepôt.
SEC-HAB-6	Les permissions d'accès doivent être retirées dès le retrait des habilitations, par exemple après le départ d'un collaborateur ou une modification de ses missions.
Authentification pour la consultation et l'administration de l'entrepôt	
SEC-AUT-1	L'accès aux données à caractère personnel doit être subordonné à une authentification forte faisant intervenir *a minima* deux facteurs d'authentification distincts. Si un de ces facteurs est un mot de passe, celui-ci doit être conforme à la délibération de la CNIL n° 2017-012 du 19 janvier 2017 portant adoption d'une recommandation relative aux mots de passe.
SEC-AUT-2	Cette authentification forte doit être mise en place à la fois pour les accès internes et externes à l'entrepôt.

Espace de travail	
SEC-ESP-1	Les données de l'entrepôt doivent être manipulées par les chercheurs uniquement dans des espaces de travail spécifiques à chaque projet de recherche, étanches avec la base de données de l'entrepôt et étanches les uns des autres.
SEC-ESP-2	Les jeux de données importées dans un espace de travail spécifique à un projet de recherche doivent être minimisés et limités aux seules données nécessaires au projet. Un numéro pseudonyme unique spécifique à chaque espace de travail devra être généré dans les mêmes conditions qu'à l'exigence SEC-PSE-1.
SEC-ESP-3	En cas de suivi de cohorte, le même numéro pseudonyme unique peut être réutilisé dans plusieurs espaces de travail.
Exportation de données hors de l'entrepôt et hors des espaces de travail	
SEC-EXP-1	Seuls des jeux de données anonymes peuvent faire l'objet d'une exportation hors de l'entrepôt ou d'un espace de travail. Le processus d'anonymisation doit produire un jeu de données conforme aux trois critères définis par l'avis du G29 n° 05/2014 ou à tout avis ultérieur du CEPD relatif à l'anonymisation. Cette conformité doit être documentée. À défaut, si ces trois critères ne peuvent être réunis, une étude des risques de ré-identification devra être menée et documentée.
SEC-EXP-2	Les exports de données doivent être soumis à la validation préalable d'un responsable afin d'en valider le principe, notamment au regard de l'exigence SEC-EXP-1.
SEC-EXP-3	Les exports doivent faire l'objet d'une surveillance automatique ou manuelle par un opérateur spécialisé afin d'en vérifier le caractère anonyme. Dans le cas où cette surveillance est automatique, tout export identifié comme non conforme doit faire l'objet d'une remontée d'alerte et d'une mise en quarantaine dans un espace cloisonné et dédié, puis doit être vérifié manuellement par un responsable spécifiquement formé et habilité.
SEC-EXP-4	Les systèmes mis en place dans l'entrepôt relatifs à la production d'indicateurs et au pilotage stratégique de l'activité d'un établissement de santé ne doivent permettre que des restitutions anonymes, y compris en tenant compte des fonctionnalités de filtrage et de sélection de ces restitutions. Ce processus de restitution doit être conforme aux trois critères définis par l'avis du G29 n° 05/2014 ou à tout avis ultérieur du CEPD relatif à l'anonymisation. Cette conformité doit être documentée. À défaut, si ces trois critères ne peuvent être réunis, une étude des risques de ré-identification devra être menée et documentée.
SEC-EXP-5	Les restitutions mentionnées à l'exigence SEC-EXP-4 doivent être exportées conformément aux exigences SEC-EXP-2 et SEC-EXP-3.
Sensibilisation des utilisateurs et sécurité des postes de travail	
SEC-SEN-1	Chaque personne habilitée à accéder à l'entrepôt doit être formée au respect du secret médical et sensibilisée régulièrement aux risques et obligations inhérents au traitement de données de santé.

SEC-SEN-2	Chaque personne habilitée à accéder à l'entrepôt doit signer une charte de confidentialité précisant notamment ses obligations au regard de la protection des données à caractère personnel de santé et au regard des mesures de sécurité mises en place dans l'entrepôt, ainsi que les sanctions afférentes au non-respect de ces obligations.
SEC-SEN-3	Les postes de travail des personnes habilitées à accéder à l'entrepôt y compris les utilisateurs externes accédant uniquement aux espaces de travail, doivent faire l'objet de mesures de sécurité spécifique, par exemple en mettant en place des comptes nominatifs, une authentification adéquate, un verrouillage automatique des sessions, un chiffrement des supports de stockage et des mesures de filtrage. Dans le cas où les postes de travail ne sont pas sous le contrôle du responsable de traitement, les mesures de sécurité à mettre en place sur les postes de travail doivent être encadrées au moyen d'une convention entre les parties concernées.
Journalisation	
SEC-JOU-1	Les actions des utilisateurs des espaces de travail de l'entrepôt doivent faire l'objet de mesures de journalisation. En particulier, les connexions à l'entrepôt (identifiants, date et heure), les requêtes et opérations réalisées doivent être tracées.
SEC-JOU-2	Les accès des ingénieurs et administrateurs système et réseau doivent être effectués à travers un système spécifique assurant une authentification forte ainsi que la traçabilité détaillée des accès et actions réalisés. Par exemple, un bastion d'administration peut être utilisé pour contrôler les accès et enregistrer les sessions.
SEC –JOU-3	Un contrôle des traces doit être réalisé régulièrement et *a minima* mensuellement, ainsi qu'à la fin de chaque période d'habilitation liée à un projet de recherche. Ce contrôle doit être réalisé par : - une solution réalisant une surveillance automatique avec une remontée d'alertes traitées manuellement par un opérateur habilité ; - ou par un contrôle semi-automatique *via* exécution de programmes permettant une sélection des traces anormales, suivi d'une relecture manuelle par un opérateur habilité.
SEC-JOU-4	Les traces de journalisation définies aux exigences SEC-JOU-1 et SEC-JOU-2 doivent être conservées pendant une durée de six mois.
Exercice des droits	
SEC-EXC-1	Le responsable de traitement met en place une procédure opérationnelle sécurisée afin d'assurer l'exercice des droits des personnes et le cas échéant la levée du pseudonymat et la bonne ré-identification des personnes concernées. Cette procédure permet, à partir des informations supplémentaires nécessaires à l'identification unique de la personne, de retrouver ou de calculer le numéro pseudonyme unique correspondant, puis de sélectionner dans l'entrepôt, avec ce seul numéro pseudonyme unique, les données correspondant au demandeur et d'effectuer les opérations nécessaires au bon exercice de ses droits (suppression des données ou extraction pour transmission).

SEC-EXC-2	Les habilitations et accès relatifs à la procédure de ré-identification définie à l'exigence SEC-EXC-1 doivent être réservés à une équipe restreinte et être limités au strict nécessaire. Les membres de cette équipe restreinte doivent être formés spécifiquement à cette procédure.
SEC-EXC-3	Le responsable de traitement met en œuvre les mesures adéquates pour gérer les risques inhérents à cette procédure de ré-identification et notamment pour garantir qu'elle ne soit utilisable que dans le cas d'une demande émanant effectivement d'une personne concernée.
Gestion des incidents de sécurité et des violations de données à caractère personnel	
SEC-INC-1	Le responsable de traitement prévoit une procédure 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.
SEC-INC-2	Tout incident de sécurité, d'origine malveillante ou non et se produisant de manière intentionnelle ou non, ayant comme conséquence, même temporaire, de compromettre l'intégrité, la confidentialité ou la disponibilité de données personnelles, doit faire l'objet d'une documentation en interne dans un registre des violations.
SEC-INC-3	Toute violation de données doit être notifiée à la CNIL dans les conditions prévues à l'article 33 du RGPD.
SEC-INC-4	Dans l'hypothèse où la violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable de traitement est tenu de communiquer la violation des données aux personnes concernées dans les meilleurs délais, conformément à l'article 34 du RGPD.

10.3 Ces mesures ne sont pas exhaustives et devront être complétées par les éventuelles mesures qui auront été jugées nécessaires lors de la réalisation de l'analyse d'impact sur la protection des données menée tel que détaillé dans la section 13 du présent référentiel.

10.4 Les articles 5-1-f et 32 du RGPD nécessitent la mise à jour des mesures de sécurité au regard de la réévaluation régulière des risques afin que celles-ci soient conformes à l'état de l'art.

11. Sous-traitants

11.1 En cas de recours à un prestataire, la prestation doit s'effectuer dans les conditions prévues à l'article 28 du RGPD. Un contrat de sous-traitance doit être conclu entre le prestataire et le responsable de traitement. Ce contrat doit notamment spécifier la répartition des responsabilités relatives aux mesures de sécurité et à la gestion des violations de données entre les différents acteurs.

11.2 Le prestataire doit, en sa qualité de sous-traitant, tenir un registre des activités de traitement dans les conditions de l'article 30.2 du RGPD.

11.3 Seuls les entrepôts ayant recours à un sous-traitant relevant exclusivement des juridictions de l'Union européenne sont conformes au présent référentiel.

11.4 Dans le cas où le responsable de traitement a recours aux services d'un sous-traitant pour l'hébergement, le stockage ou la conservation des données de santé, ce sous-traitant doit être un hébergeur de données de santé agréé ou certifié selon les dispositions du CSP.

12. Transfert de données hors de l'Union européenne

12.1 La mise en place d'un entrepôt ne peut entrainer le transfert de données à caractère personnel, directement ou indirectement identifiantes hors de l'Union européenne ou à destination d'un pays ne disposant pas d'un niveau de protection adéquat. Est considéré comme transfert tout accès distant aux données depuis l'extérieur du territoire européen.

13. Analyse d'impact sur la protection des données

13.1 Le responsable de traitement doit réaliser et documenter une analyse d'impact sur la protection des données.

13.2 Pour réaliser et documenter son analyse d'impact, le responsable de traitement pourra se reporter :

- aux principes contenus dans ce référentiel ;
- aux outils méthodologiques proposés par la CNIL sur son site web.

13.3 Le cas échéant, le responsable de traitement pourra élaborer une procédure relative à l'AIPD permettant d'impliquer les acteurs et les personnes pertinentes pour sa réalisation, notamment le délégué à la protection des données (DPD/DPO) qui devra être consulté.

13.4 L'AIPD devra être réexaminée et mise à jour régulièrement, notamment si des changements importants sont prévus dans le traitement ou si les risques pour les personnes concernées ont évolué (comme la poursuite d'une finalité supplémentaire, le recours à un nouveau sous-traitant, de nouvelles données collectées, une fuite de données permettant la réidentification, etc.).