Commission nationale de l'informatique et des libertés

Délibération n° 2021-118 du 7 octobre 2021 portant adoption d'un référentiel relatif aux traitements de données à caractère personnel mis en œuvre à des fins de création d'entrepôts de données dans le domaine de la santé

NOR : *CNIL2131763X*

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 (règlement général sur la protection des données), notamment son article 58 ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son articles 8 I 2° *b* ;

Après avoir entendu le rapport de Mme Valérie PEUGEOT, commissaire, et les observations de M. Benjamin TOUZANNE, commissaire du Gouvernement,

Adopte un référentiel relatif aux traitements de données à caractère personnel mis en œuvre à des fins de création d'entrepôts de données dans le domaine de la santé.

La présidente,
M.-L. Denis

ANNEXE

RÉFÉRENTIEL

1. **A qui s'adresse ce référentiel ?**

Ce référentiel s'adresse aux responsables de traitements qui souhaitent, dans le cadre de leurs missions d'intérêt public, réunir des données en vue de leur réutilisation, pour les finalités mentionnées au point 3.1.

1.1. De tels traitements sont ci-après dénommés « entrepôts de données de santé ».

1.2. 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.

1.3. Ne sont pas concernés par ce référentiel :

– les entrepôts mis en œuvre par une société privée sur le fondement de son intérêt légitime ;
– les traitements de données à caractère personnel mis en œuvre uniquement 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 (p. ex. : les dossiers médicaux dématérialisés) ;
– les traitements de données à caractère personnel mis en œuvre lorsque la personne a donné son consentement explicite à cette fin ;
– les entrepôts appariés avec la base principale du système national des données de santé tel que défini à l'article L. 1461-1 du code de la santé publique.

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 Commission une déclarationde conformité au présent référentiel sont autorisés à mettre en œuvre un entrepôt de données de santé lorsque le traitement est strictement conforme au référentiel.

Pour déclarer sa conformité au référentiel :

– « Déclarer un fichier » - rubrique « déclaration de conformité »

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 « informatique et libertés ».

Pour demander une autorisation :

« Déclarer un fichier » - rubrique « demande d'autorisation santé – finalité d'intérêt public »

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 entrepôts 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 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 (v. point 13 du présent référentiel).

2.6. En 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 chacune des personnes concernées ne sont pas soumis à une autorisation préalable de la Commission ni à une déclaration de conformité au présent référentiel. La Commission rappelle toutefois que les principes et les mesures posés par le présent référentiel peuvent s'appliquer 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, d'études ou d'évaluation 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) et gouvernance**

3.1. **Les finalités couvertes par le référentiel**

3.1.1. Les entrepôts encadrés par le présent référentiel sont mis en œuvre afin de permettre la réutilisation des données qu'ils contiennent.

3.1.2. Lorsqu'ils sont mis en œuvre exclusivement à partir des données de l'entrepôt par les personnels habilités du responsable de traitement et pour son usage exclusif, les traitements répondant aux finalités suivantes peuvent être mis en œuvre dans le cadre de la déclaration de conformité au présent référentiel :

- la production d'indicateurs et le pilotage stratégique de l'activité, sous la responsabilité du médecin responsable de l'information médicale (département de l'information médicale - DIM) (p. ex : analyses médico-économiques de parcours de soins, évaluation de la qualité et de la pertinence des prises en charge) ;
- l'amélioration de la qualité de l'information médicale ou l'optimisation du codage dans le cadre du programme de médicalisation des systèmes d'information (PMSI) ;
- le fonctionnement d'outils d'aide au diagnostic médical ou à la prise en charge ;
- la réalisation d'études de faisabilité (*pré-screening*).

3.1.3. Les données peuvent également être réutilisées à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé. Ces traitements devront faire l'objet des formalités adéquates : s'ils sont conformes à une méthodologie de référence, ils peuvent être mis en œuvre à la condition que leur responsable adresse préalablement à la Commission une déclaration attestant de cette conformité. A défaut, ils devront solliciter une « autorisation recherche » sur le fondement de l'article 66 III de la loi « informatique et libertés ».

3.1.4. Les données contenues dans les traitements réalisés dans le cadre de ce référentiel ne peuvent être exploitées ni 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.

3.2. **La gouvernance de l'entrepôt**

3.2.1. Afin de vérifier le respect des finalités poursuivies, le responsable de traitement met en œuvre une gouvernance pour chaque entrepôt qu'il constitue. Les instances constituées à cette fin peuvent être mutualisées si le responsable de traitement met en œuvre plusieurs entrepôts.

3.2.2. Une première instance (comité de pilotage ou équivalent) détermine les orientations stratégiques et scientifiques de l'entrepôt.

3.2.2.1. 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.

3.2.2.2. Dans le cadre d'une structure dotée d'un DIM, cette gouvernance doit faire intervenir ce dernier, ainsi qu'un représentant de la conférence ou de la commission médicale d'établissement.

3.2.3. 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.

3.2.3.1. Seuls les projets ayant été examinés par cette instance peuvent avoir recours à l'entrepôt. L'avis doit être communiqué sans délai au porteur de projet souhaitant réutiliser les données de l'entrepôt.

3.2.3.2. Une liste des traitements sur lesquels ce comité s'est prononcé est communiquée de façon périodique, au moins une fois par an, au délégué à la protection des données du responsable de traitement.

3.2.3.3. Pour les traitements qui relèvent du point 3.1.3, le comité peut choisir, pour certains dossiers qui portent sur des catégories de données et de destinataires identiques, de rendre un avis unique. Il peut également choisir de ne pas se prononcer de façon systématique pour les recherches « internes » au sens de l'article 65 (2°) de la loi « informatique et libertés ».

3.2.3.4. Cette deuxième instance comprend notamment :

– au moins une personne impliquée dans l'éthique en santé ;
– une personne indépendante du responsable de traitement (par exemple : non salariée) ;
– des professionnels de santé et professionnels médico-sociaux ;
– des chercheurs ;
– un représentant des usagers ou d'une association de patients.

4. **Base(s) légale(s) du traitement**

4.1. Le référentiel ne s'applique qu'aux entrepôts de données de santé dont la constitution se fonde sur l'exercice d'une mission d'intérêt public, au sens de l'article 6-1-e du RGPD. Ainsi, l'entrepôt doit être nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement.

4.2. Le caractère d'intérêt public de la mission du responsable de traitement doit être distingué de l'exigence d'intérêt public imposée pour les finalités des traitements mis en œuvre dans le domaine de la santé, conformément à l'article 66 de la loi n° 78-17 du 6 janvier 1978 modifiée.

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

5.1. 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. A ce titre, le responsable de traitement ne peut collecter et traiter que :

– **des données qui figurent dans le dossier médical et administratif** ou dossier unique informatisé de la personne concernée et que leur collecte est justifiée par sa prise en charge ; et/ou
– des données issues de projets de recherches, études et évaluations dans le domaine de la santé précédemment réalisés et dont leur durée de conservation n'a pas expiré.

5.2. Les données pouvant être traitées incluent :

5.2.1. Des données relatives aux patients :

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

– nom, prénoms ;
– sexe, genre, civilité ;
– statut matrimonial ;
– jour, mois, date et lieu de naissance ;
– date, lieu et cause de décès, si présents dans le dossier médical ;
– coordonnées téléphoniques, électroniques et adresse de résidence ;
– numéro d'identifiant permanent du patient (IPP) ;
– numéro d'identifiant de l'épisode de soin (IEP) ;
– numéro d'identification au répertoire des personnes physiques – identifiant national de santé (NIR-INS).

5.2.1.2. Autres catégories de données à caractère personnel, comprenant des données sensibles :

– poids, taille, comptes rendus (médicaux, RCP, etc.), résultats d'examens, résultats issus d'analyse d'échantillons biologiques, imagerie médicale, données relatives aux effets et événements indésirables ; prescriptions ; observations médicales et paramédicales ; données issues de dispositifs médicaux ou d'appareils de mesure et tout élément constitutif du dossier médical ;
– antécédents personnels ou familiaux, maladies ou événements associés ;
– données médico-administratives issues du PMSI local (1) ;
– données génétiques strictement nécessaires pour répondre aux objectifs ou finalités de l'entrepôt et ayant été interprétées préalablement à leur versement dans l'entrepôt, ne pouvant en aucun cas être utilisées aux fins d'identification ou de réidentification des personnes ; elles doivent avoir été recueillies dans le cadre de la prise en charge médicale de la personne concernée ou d'un projet de recherche, sous réserve que la personne concernée ne s'y soit pas opposée préalablement à la réalisation de l'examen, conformément aux dispositions des articles L. 1130-5 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 ;
– vie sexuelle ;
– données révélant l'origine ethnique ;
– 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 relatives à la vie professionnelle (profession, historique d'emploi, chômage, trajets et déplacements professionnels, expositions professionnelles, catégorie INSEE socioprofessionnelle, etc.) ;
– niveau de formation (p. ex. : primaire, secondaire, supérieur) ;

– régime d'affiliation à la sécurité sociale, assurance complémentaire (mutuelle, assurance privée) ;
– déplacements (p. ex. : vers le lieu de soin ou de la recherche : mode, durée, distances ou voyages) ;
– 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 (p.ex. : urbain, semi-urbain, nomade, sédentaire), habitat (maison particulière, immeuble, étage, ascenseur, etc.) ;
– statut vital et cause du décès ;
– échelle de qualité de vie ou autres informations sur la qualité de vie de la personne ;
– exposition à des risques sanitaires connus (physiques, chimiques, biologiques et environnementaux, etc.).

5.2.2. 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) ;
– numéro ADELI ou numéro RPP (à l'exclusion du numéro du matricule).

5.3. Aucune donnée ne peut être collectée uniquement afin d'alimenter l'entrepôt. Ainsi, est proscrit le versement dans l'entrepôt de données dont la collecte ne serait pas scientifiquement justifiée par la prise en charge sanitaire ou médico-sociale ou par la réalisation d'un projet de recherche, d'étude ou d'évaluation spécifique et prévue par un protocole.

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

5.5. Les données directement identifiantes mentionnées au point 5.2.1.1 ne peuvent être réunies dans l'entrepôt que pour les finalités suivantes :

– recontacter les patients pour leur proposer de participer à des études ou pour les informer régulièrement des projets de recherche n'impliquant pas la personne humaine, réutilisant les données de l'entrepôt les concernant ;
– recontacter les patients à la suite de découvertes de caractéristiques génétiques pouvant être responsables d'une affection justifiant des mesures de prévention ou de soins à leur bénéfice ou au bénéfice de leur famille, à l'exception des cas dans lesquels le patient s'y est opposé, conformément à l'article L. 1130-5 du code de la santé publique ;
– recontacter les patients à la suite de découvertes annexes liées à l'identification de facteurs de risques et/ou d'identification syndromiques à même de modifier leur prise en charge (thérapeutique ou de suivi) ;
– avertir une personne d'un risque sanitaire auquel elle est exposée.

5.6. Les données directement identifiantes mentionnées au point 5.3.1.1 ne peuvent être utilisées que si les finalités du traitement le justifient. A 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 par la gouvernance de l'entrepôt, notamment au regard de l'utilisation qui en est faite pour les divers projets menés. Les données n'apparaissant plus nécessaires doivent être supprimées.

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

6. **Accès aux 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 validés par la gouvernance de l'entrepôt, les équipes de recherche internes (p. ex. : composées de salariés du responsable de traitement) ou externes (p. ex. : composées de partenaires du responsable de traitement) 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 (2) au sein d'un espace projet de l'entrepôt, les données anonymes en résultant peuvent être publiées ou 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 5.2.1.2 et 5.2.1.3 peuvent être conservées 20 ans maximum à compter de leur collecte dans le cadre des soins ou des recherches. Les données mentionnées au point 5.2.1.1 doivent être supprimées lorsque le délai de conservation des données mentionnées aux points 5.2.1.2 et 5.2.1.3 a expiré.

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

8. **Information des personnes**

8.1. **L'information des patients :**

Les personnes doivent être informées par le ou les responsables de traitement que les données collectées lors de leur prise en charge sont versées au sein de l'entrepôt.

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.

8.2.2. ***Collecte des informations auprès des patients admis ou réadmis postérieurement à la constitution de l'entrepôt***

8.2.2.1. Les nouveaux patients ainsi que ceux en cours de suivi sont informés individuellement de la constitution de l'entrepôt (p. ex. : par courrier). Le ou les supports d'information utilisés comprennent l'ensemble des éléments prévus 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 de patients admis antérieurement à la constitution de l'entrepôt et n'étant plus suivis***

8.2.3.1. Les patients n'étant plus suivis sont informés individuellement de la constitution de l'entrepôt (p. ex. : par courrier). 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 intégrer la politique de protection des données à caractère personnel du responsable de traitement et être présentées dans une section dédiée.

8.2.3.3. La réutilisation des données ainsi que les modalités d'exercice des droits d'accès et d'opposition doivent faire l'objet d'une mise en avant spécifique dans la note d'information.

8.2.3.4. Le responsable de traitement peut faire valoir une exception à l'obligation d'information individuelle pour la constitution de l'entrepôt, 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. A 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 (3).

Dans la plupart des cas, l'exception à l'obligation d'information ne sera justifiée que pour une catégorie de personnes concernées. A titre d'exemple, cette exception peut s'appliquer aux personnes pour lesquelles le responsable de traitement dispose d'un dossier médical mais qui ne sont plus suivies au sein de l'établissement ou centre où s'exercent des activités de prévention, de diagnostic et de soins. L'exception ne pourrait cependant être invoquée afin de ne pas informer les personnes qui viendraient consulter après la mise en œuvre de l'entrepôt.

L'AIPD devra détailler précisément en quoi l'information individuelle des personnes concernées constituerait un effort disproportionné, ainsi que les garanties mises en œuvre par le responsable de traitement afin de protéger les droits et libertés ainsi que les intérêts légitimes des personnes concernées.

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 au sujet de 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 8.2.3.4 à 8.2.3.6.

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.

8.4. **Les personnes concernées doivent en outre être informées de chacune des réutilisations des données les 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 des professionnels**

8.5.1. Concernant l'information des professionnels exerçant au sein des établissements du responsable de traitement postérieurement à la mise en œuvre de l'entrepôt :

– les professionnels dont les données sont versées dans l'entrepôt doivent être informés individuellement et par écrit des mentions prévues par l'article 13 du RGPD ;
– si le responsable de traitement est l'employeur des professionnels, la fiche d'information pourra prendre la forme d'un courrier ou d'un courriel joint au bulletin de paie ou au contrat de travail. 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.

8.5.2. Concernant l'information des professionnels n'exerçant pas ou plus au sein des établissements du responsable de traitement lors de la mise en œuvre de l'entrepôt :

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

9. **Droits des personnes**

9.1. En complément de l'information individuelle, le responsable de traitement diffuse une information générale, *via* une campagne d'information publique (p.ex. : sur les réseaux sociaux, au sein de l'établissement et par la publication d'encarts dans la presse régionale), préalablement à la mise en place de l'entrepôt afin de garantir qu'une période de temps raisonnable (p.ex. : un mois) 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 (professionnels et patients) dont les données figurent dans l'entrepôt 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 par tout moyen. Dans le cadre du présent référentiel, le responsable de traitement doit permettre aux personnes de s'opposer au traitement dès leur information (p. ex., 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. Il devra pour cela mettre en place un mécanisme garantissant la correspondance entre les données transmises par la personne exerçant ses droits et les données de l'entrepôt la concernant. Le responsable de traitement précisera dans la note d'information les informations qui devront lui être transmises pour l'exercice des droits.

9.7. 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, ainsi que les sous-traitants auxquels il fait appel, doivent 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, ainsi que tous les flux de données internes à 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 avec des clés différentes de celles utilisées pour chiffrer les 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 comptes utilisateur différents, ou *via* un seul compte utilisateur devant choisir à la connexion un des profils d'habilitation différents qui lui sont attribués.
SEC-LOG-6	Dans le cas où des données génétiques ou de suivi de localisation 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 ou de suivi de localisation 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 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 manuellement *via* 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 identifiant pseudonyme unique peut être utilisé, permettant le cas échéant la correspondance entre les données pseudonymisées stockées dans l'entrepôt et des données directement identifiantes. Cet identifiant 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. Les données doivent être pseudonymisées préalablement à leur intégration dans l'entrepôt.
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 doivent faire l'objet d'une étape de suppression ou de masquage avant leur intégration dans l'entrepôt. Cette étape consiste à supprimer les données identifiantes des patients et des professionnels de santé ou à les remplacer par des termes génériques ou des données fictives. 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 ». Cette exigence s'applique notamment aux documents bureautiques et aux fac-similés d'impression (comme les comptes rendus médicaux et les prescriptions), aux numérisations de documents, à l'imagerie médicale et à toute forme de résultats d'analyse biomédicale. Elle concerne également les commentaires en saisie libres contenus dans les bases de données. L'opération de masquage ou suppression devra s'appliquer au contenu visible des documents (comme les entêtes des courriers et les cartouches des images), aux métadonnées contenues dans ces fichiers (comme le nom de l'opérateur d'imagerie) et aux attributs des fichiers (comme leur nom).
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.

Numéros d'exigence	Exigences de sécurité
SEC-HAB-2	Une granularité des accès aux données doit être prévue pour chaque profil d'habilitation, tout en respectant l'exigence SEC-LOG-5 relative au cloisonnement des tables de correspondance et données directement identifiantes. Par exemple, un profil peut contenir soit un accès uniquement à des données agrégées et/ou un accès à des données pseudonymisées, soit un accès uniquement à des données directement identifiantes.
SEC-HAB-3	Les personnes autorisées 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 manuelle ou automatique 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 aux recommandations de la CNIL en matière de mot de passe (délibération n° 2017-012 du 19 janvier 2017 à la date de rédaction de ce référentiel).
SEC-AUT-2	Cette authentification forte doit être mise en place à la fois pour les accès internes et externes à l'entrepôt.
SEC-AUT-3	Toutes les transmissions de données depuis ou vers l'entrepôt, ainsi que tous les flux internes à l'entrepôt, réalisés automatiquement sans action d'un utilisateur, doivent être effectués par des serveurs mutuellement authentifiés par certificat ou dispositif d'authentification équivalent (4).
Espace de travail	
SEC-ESP-1	Les données de l'entrepôt doivent être manipulées par les chercheurs uniquement dans des espaces de travail internes à l'entrepôt et spécifiques à chaque projet de recherche, étanches avec la base de données de l'entrepôt et étanches les uns des autres. Des capacités d'échange entre les espaces de travail sont néanmoins possibles pour le partage de données qui auront subi le processus d'anonymisation détaillé à l'exigence SEC-EXP-1.
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	A l'exception des données relatives aux procédures de ré-identification SEC-REI-1 à SEC-REI-3, 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 et démontrable. A 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 avaliser 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 l'entrepôt, puis doit être vérifié manuellement par un responsable spécifiquement formé et spécifiquement 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. A 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 spécifiques, par exemple en mettant en place des comptes nominatifs, une

Numéros d'exigence	Exigences de sécurité
	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* bimestriellement, 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 comprise entre 6 mois et un an.
Procédures de ré-identification	
SEC-REI-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 (5), 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-REI-2	Le cas échéant, et en cas de nécessité dûment justifiée et documentée, le responsable de traitement met en place une procédure opérationnelle sécurisée afin de recontacter des patients pour leur proposer de participer à des recherches. Cette procédure permet, à partir d'une liste de critères médicaux, de sélectionner les identifiants pseudonymes uniques correspondants aux patients visés, puis, en mobilisant la ou les tables de correspondance de l'entrepôt avec ces seuls pseudonymes, de sélectionner les données identifiantes correspondant à ces patients afin de les exporter pour cette seule finalité.
SEC-REI-3	Le cas échéant, le responsable de traitement met en place une procédure opérationnelle sécurisée afin de ré-identifier des patients en cas d'urgence médicale. Cette procédure permet, en mobilisant la ou les tables de correspondance de l'entrepôt, de sélectionner les données identifiantes des patients concernés à partir de leur numéro pseudonyme unique, et de les exporter pour cette seule finalité.
SEC-REI-4	Les habilitations et accès relatifs aux procédures de ré-identification définies aux exigences SEC-EXC-1 à SEC-EXC-3 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-REI-5	Le responsable de traitement met en œuvre les mesures adéquates pour gérer les risques inhérents à ces procédures de ré-identification et notamment pour garantir qu'elles ne soient utilisables que dans le cas d'une demande émanant effectivement d'une personne concernée ou d'un professionnel de santé dûment habilité.
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 à caractère personnel, 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 à caractère personnel, doit faire l'objet d'une documentation en interne dans un registre des violations.
SEC-INC-3	Lorsqu'un tel incident est susceptible d'engendrer un risque pour les droits et libertés des personnes concernées, la violation de données qui en résulte doit être notifiée à la Commission 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 dispositions 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 ou d'un pays considéré comme adéquat au sens de l'article 45 du RGPD 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. Est considéré comme transfert tout accès distant aux données depuis l'extérieur du territoire européen.

12.2. La mise en place et le fonctionnement 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.

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. A cette fin, le responsable de traitement pourra se reporter :

– aux principes contenus dans ce référentiel ;

– aux outils méthodologiques proposés par la Commission 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.).

---

(1) Le PMSI local correspond au PMSI de l'établissement, sauf dans le cas d'un GHT dans lequel l'établissement chef de file pourrait disposer du PMSI du GHT.

(2) Conformément aux critères du G29 ou tout avis futur du CEPD.

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

(4) Un mot de passe seul n'est pas considéré comme un dispositif d'authentification équivalent à un certificat.

(5) Y compris en mobilisant les sels, clés de hachage ou les tables de correspondance.