Commission nationale de l'informatique et des libertés

Délibération n° 2023-082 du 20 juillet 2023 portant homologation d'une méthodologie de référence relative aux traitements de données de la base principale du Système national des données de santé mis en œuvre à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé par les organismes agissant dans le cadre de leur mission d'intérêt public (MR-007)

NOR : *CNIL2326885X*

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, et abrogeant la directive 95/46/CE ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 66 et 72 et suivants ;

Vu le code de la santé publique, notamment son article L. 1461-3 ;

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

Adopte une méthodologie de référence relative aux traitements de données de la base principale du Système national des données de santé mis en œuvre à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé par les organismes agissant dans le cadre de leur mission d'intérêt public (MR-007).

La présidente,
M.-L. Denis

MÉTHODOLOGIE DE RÉFÉRENCE RELATIVE AUX TRAITEMENTS DE DONNÉES DE LA BASE PRINCIPALE DU SYSTÈME NATIONAL DES DONNÉES DE SANTÉ MIS EN ŒUVRE À DES FINS DE RECHERCHE, D'ÉTUDE OU D'ÉVALUATION DANS LE DOMAINE DE LA SANTÉ PAR LES ORGANISMES AGISSANT DANS LE CADRE DE LEUR MISSION D'INTÉRÊT PUBLIC (MR-007)

Le règlement (UE) n° 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 (le RGPD) prévoit, notamment en son article 5, point 2, que le responsable de traitement doit être en mesure de démontrer que les principes du règlement sont respectés.

L'article 9, paragraphe 4 du RGPD précise que les Etats membres peuvent maintenir ou introduire des conditions supplémentaires, y compris des limitations, en ce qui concerne le traitement des données génétiques ou des données concernant la santé.

Ainsi, en application de la loi n° 78-17 du 6 janvier 1978 modifiée (loi « informatique et libertés »), les traitements de données à caractère personnel à des fins de recherche, étude ou évaluation dans le domaine de la santé peuvent être mis en œuvre à condition que le responsable de traitement ait réalisé une déclaration de conformité à une méthodologie de référence. En l'absence de conformité à une méthodologie de référence, le traitement doit faire l'objet d'une demande d'autorisation auprès de la Commission nationale de l'informatique et des libertés (la CNIL).

La CNIL peut homologuer et publier des méthodologies de référence, au titre des référentiels mentionnés au II de l'article 66 de la loi « informatique et libertés », établies en concertation avec la Plateforme des données de santé (PDS), ainsi qu'avec les organismes publics et privés représentatifs des acteurs concernés.

Compte tenu de leurs missions d'intérêt public, un grand nombre d'organismes réalisent des recherches, études et évaluations dans le domaine de la santé, qui s'inscrivent dans un ensemble de finalités déterminées correspondant à leurs missions (par exemple : évaluation des parcours de santé ou de la qualité des soins, évaluations médico-économiques, réponses aux demandes des pouvoirs publics, actions auprès du grand public, conseil aux adhérents, etc.).

En complément de celle relative aux traitements de données nécessitant l'accès par des établissements de santé et des fédérations aux données du programme de médicalisation des systèmes d'information (PMSI), mises à disposition sur la plateforme sécurisée de l'Agence technique de l'information sur l'hospitalisation (ATIH), la Commission adopte une méthodologie de référence relative à certains traitements de données du Système national des données de santé (SNDS) mis en œuvre par les responsables de traitement agissant dans le cadre de leur mission d'intérêt public.

Les responsables de traitement qui adressent une déclaration de conformité à cette méthodologie de référence sont autorisés à mettre en œuvre leurs traitements, dès lors qu'ils répondent aux conditions prévues par la méthodologie et qu'ils ont obtenu un avis favorable du Comité éthique et scientifique pour les recherches, les études et les évaluations dans le domaine de la santé (CESREES).

TITRE Ier

DÉFINITIONS, RESPONSABLES DE TRAITEMENT CONCERNÉS, CHAMP D'APPLICATION ET INTÉRÊT PUBLIC

1.1. **Définitions**

Au sens de la présente méthodologie, les termes suivants sont ainsi définis :

Bilan : synthèse, transmise à la CNIL tous les trois ans par le responsable de traitement, faisant état des usages de la méthodologie de référence observés durant cette période.

Comité éthique et scientifique pour les recherches, les études et les évaluations dans le domaine de la santé (CESREES) : comité qui émet un avis motivé sur la méthodologie de la recherche, la nécessité du recours à des données de santé à caractère personnel, la pertinence de celles-ci par rapport à la finalité du traitement et, s'il y a lieu, sur la pertinence scientifique et éthique du projet ainsi que sur le caractère d'intérêt public que présente la recherche, l'étude ou l'évaluation ;

Donnée à caractère personnel : toute information se rapportant à une personne physique identifiée ou identifiable (« personne concernée ») ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale (v. art. 4 du RGPD). A ce titre, les données du SNDS, bien que pseudonymisées, constituent des données à caractère personnel ;

Environnement maîtrisé : ensemble de ressources (matériel, logiciels, personnel, données) sur lesquelles le gestionnaire d'un système du Système national des données de santé (SNDS) applique les exigences du référentiel de sécurité du SNDS ;

Espace projet : espace de travail dédié à une étude, sécurisé et maîtrisé par le gestionnaire du système mettant à disposition des données du SNDS ;

Etude : recherche ou étude dans le domaine de la santé ne répondant pas à la définition des recherches impliquant la personne humaine telles que définies à l'article L. 1121-1 du code de la santé publique (CSP). Il peut également s'agir d'une évaluation ou d'une analyse des pratiques ou des activités de soins ou de prévention, au sens de l'article 72 de la loi « informatique et libertés ». Ce traitement doit présenter un caractère d'intérêt public au sens de l'article 66 de cette même loi. Une étude peut nécessiter la réalisation de plusieurs requêtes à partir des données du SNDS ;

Expression de besoins : document indiquant les composantes de la base principale du SNDS concernées par la demande d'accès, la population ciblée, la période de ciblage, les données ou catégories de données nécessaires, la profondeur historique des données et la durée d'accès demandées, dont un modèle élaboré en collaboration avec la PDS et la Caisse nationale d'assurance maladie (CNAM) est mis à disposition ;

Laboratoire de recherche/bureau d'études : organisme responsable, le cas échéant, de la mise en œuvre du traitement de données et chargé de leur analyse, ayant réalisé un engagement de conformité auprès de la CNIL à l'arrêté du 17 juillet 2017 relatif au référentiel déterminant les critères de confidentialité, d'expertise et d'indépendance pour les laboratoires de recherche et bureaux d'études. Il s'agit d'un sous-traitant au sens du RGPD qui, dans le cadre de la présente méthodologie de référence, accède aux données du SNDS pour le compte du responsable de traitement ;

Plateforme des données de santé (PDS) : groupement d'intérêt public constitué entre l'Etat, des organismes assurant une représentation des malades et des usagers du système de santé, des producteurs de données de santé et des utilisateurs publics et privés de données de santé, y compris des organismes de recherche en santé, chargé de mettre en œuvre les grandes orientations stratégiques relatives au SNDS et ainsi de faciliter le partage des données de santé issues de sources variées afin de favoriser la recherche ;

Profondeur historique des données : années de production des données nécessaires à la réalisation de l'étude ;

Protocole : document rédigé par le responsable de traitement ou sous sa responsabilité, indiquant notamment :

- la méthodologie de l'étude ;
- l'objectif du traitement des données à caractère personnel ;
- les catégories de personnes concernées par le traitement ;
- l'origine, la nature et la liste des données à caractère personnel utilisées et la liste des justifications de recours à celles-ci ;
- la durée et les modalités d'organisation de l'étude ;
- la méthode d'analyse des données ;
- la justification du nombre de personnes et la méthode d'observation retenue ;

Responsable de la mise en œuvre du traitement : organisme, ayant accès aux données par convention, chargé d'effectuer les analyses pour le compte du responsable de traitement. Il peut s'agir d'un laboratoire de recherche ou d'un bureau d'études ;

Responsable de traitement : personne physique ou morale qui, seule ou conjointement avec d'autres, est responsable d'une recherche, étude ou évaluation n'impliquant pas la personne humaine, en assure la gestion, vérifie que son financement est prévu et détermine les finalités et les moyens des traitements nécessaires à celle-ci ;

Sous-traitant : personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ;

Système national des données de santé : base de données de santé comprenant une base principale, couvrant l'ensemble de la population, ainsi que d'autres bases de données intégrées dans un « catalogue » ;

Traitement : toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ;

Utilisateur : personne physique qui accède aux données individuelles du SNDS mises à disposition dans un espace projet.

1.2. **Responsables de traitement concernés**

1.2.1. Seuls peuvent réaliser une déclaration attestant de la conformité à la présente méthodologie de référence le ou les responsables de traitements pour lesquels la mise en œuvre de la recherche, étude ou évaluation dans le domaine de la santé est nécessaire à l'exécution d'une mission d'intérêt public ou relève de l'exercice de l'autorité publique dont il est investi au sens de l'article 6.1.e du RGPD et répondant aux finalités mentionnées ci-dessous. A ce titre, il s'agira le plus souvent d'organismes publics.

1.2.2. Dans le cas d'une responsabilité conjointe de traitement, les responsables doivent définir de manière transparente leurs obligations respectives conformément à l'article 26 du RGPD.

1.3. **Traitement de données à caractère personnel inclus dans le champ d'application de la présente méthodologie**

1.3.1. Seuls peuvent faire l'objet d'une déclaration de conformité à la présente méthodologie de référence les traitements de données à caractère personnel ayant pour finalité la réalisation de recherches, études ou évaluations dans le domaine de la santé, présentant un caractère d'intérêt public au sens de l'article 66 de la loi « informatique et libertés » et respectant les conditions de sécurité, d'organisation et de transparence suivantes :

- un protocole, ainsi qu'une expression de besoins, doivent être élaborés par le responsable de traitement avant le début de la mise en œuvre du traitement des données. Ces documents doivent être soumis au CESREES ;
- les traitements visés par la présente méthodologie de référence doivent obtenir un avis expressément favorable du CESREES préalablement à leur mise en œuvre. Lorsque cet avis est accompagné de recommandations, le responsable de traitement s'engage à les prendre en compte et à modifier son dossier en conséquence, préalablement à la mise en œuvre du traitement ;
- les données traitées doivent provenir exclusivement de la CNAM, seule compétente, dans le cadre de la présente méthodologie, pour extraire et transmettre les données du SNDS, dans le strict respect de l'expression de besoins ;
- les données traitées doivent également provenir directement de la CNAM. Aucune réutilisation des données n'est permise dans le cadre de cette méthodologie de référence ;
- les données sont mises à disposition du responsable de traitement ou du responsable de la mise en œuvre du traitement dans un environnement maîtrisé, tel que défini au point 1.1 (Définitions) et remplissant les conditions cumulatives suivantes :
  - a fait l'objet d'une homologation conformément au référentiel de sécurité applicable au SNDS. Cette homologation, qui ne doit pas avoir expiré, doit faire l'objet d'un suivi régulier et est régulièrement renouvelée dans les délais prévus par la décision d'homologation ;
  - a été expertisé par la CNIL dans le cadre d'un traitement de données ayant fait l'objet d'une autorisation expresse par la CNIL. Cette autorisation doit dater de moins de trois ans ;
  - est conforme au titre V de la présente délibération concernant les modalités d'hébergement des données et l'absence de transferts en dehors de l'Union européenne ;
- le responsable de traitement s'engage à ne pas poursuivre l'une des finalités interdites décrites à l'article L. 1461-1 V du code la santé publique ;
- le responsable de traitement et le cas échéant, le responsable de la mise en œuvre du traitement, doivent signer préalablement une convention d'accès aux données avec le gestionnaire de l'environnement maîtrisé mettant à disposition les données du SNDS. Ils doivent également faire signer à chaque utilisateur habilité un engagement individuel à respecter les conditions d'utilisation définies par l'environnement maîtrisé. Le responsable de traitement doit enfin transmettre au gestionnaire de l'environnement maîtrisé la liste, actualisable, des laboratoires de recherche ou bureaux d'études auxquels il a recours ;
- le responsable de traitement s'engage à transmettre tous les trois ans à la CNIL ainsi qu'au CESREES, un bilan synthétisant les usages de la méthodologie de référence, observés durant cette période. S'ils le jugent pertinent, la CNIL ou le CESREES peuvent partager ce bilan avec la CNAM et/ou la PDS ;
- le responsable de traitement doit enregistrer chaque étude réalisée dans le cadre de la méthodologie de référence auprès du répertoire public tenu par la PDS. La méthode et les résultats obtenus seront publiés par la PDS à la fin du traitement, selon les modalités prévues au paragraphe 6.3 « Principe de transparence ».

1.3.2. La présente méthodologie de référence n'est ainsi notamment pas applicable aux traitements :

– hébergés en dehors d'un environnement maîtrisé répondant aux conditions cumulatives mentionnées ci-dessus ;
– nécessitant un appariement des données du SNDS avec des données à caractère personnel issues d'autres sources (par exemple : dossiers médicaux) ;
– nécessitant une réutilisation de données mises à disposition dans le cadre d'une précédente étude ou provenant d'un entrepôt de données de santé comportant des données du SNDS.

1.3.3. Les traitements mentionnés au paragraphe 1.3.2 ne pourront être mis en œuvre qu'après autorisation de la CNIL.

1.4. **Intérêt public et finalités interdites**

1.2.1. Les traitements réalisés dans le cadre de cette méthodologie de référence doivent :

– présenter un caractère d'intérêt public, justifié par le responsable de traitement dans le protocole, qui sera transmis à la PDS lors de l'enregistrement dans le répertoire public ;
– respecter l'ensemble des dispositions législatives et réglementaires relatives au SNDS (articles L. 1461-1 à L. 1461-7 du code de la santé publique), notamment l'interdiction d'utiliser ces données pour poursuivre les finalités décrites à l'article L. 1461-1 V du code la santé publique :

1. la promotion des produits mentionnés au II de l'article L. 5311-1 en direction des professionnels de santé ou d'établissements de santé ;

2. l'exclusion de garanties des contrats d'assurance et la modification de cotisations ou de primes d'assurance d'un individu ou d'un groupe d'individus présentant un même risque.

TITRE II

TRAITEMENTS RELATIFS AUX DONNÉES DES PERSONNES CONCERNÉES PAR DES ÉTUDES

2.1. **Finalité des traitements**

2.1.1. Seuls les traitements de données portant sur les finalités de recherches, études ou évaluations dans le domaine de la santé, ainsi que de planification et de valorisation de l'offre de soins détaillées ci-dessous, peuvent être réalisés dans le cadre de la méthodologie de référence :

– évaluation comparative de l'offre de soins : analyses spatiales, analyses stratégiques ;
– évolution des pratiques de prises en charge, incidence de certains facteurs dans les hospitalisations, analyses temporelles ;
– analyses comparatives des activités de soins, études de trajectoire de patients, bassin de recrutement, devenir des patients ;
– description et analyse des pathologies et parcours de soins des patients dans les établissements de santé ;
– analyse du territoire de santé, des groupements hospitaliers de territoires (GHT), études de collaboration entre établissements d'un périmètre défini ;
– analyse continue d'évaluations comparatives, meilleure adaptation de l'offre de soins, optimisation, valorisation des séjours, réalisation d'indicateurs de pilotage, stratégie ;
– travaux de modélisation, simulation, planning, logistique hospitalière, recherche opérationnelle (analyse de données dans le but d'optimiser des organisations ou de produire des éléments d'aide à la décision pour de nouvelles organisations) ;
– ciblage des centres et/ou réalisation d'études de faisabilité pour la réalisation d'une recherche impliquant ou n'impliquant pas la personne humaine ;
– études épidémiologiques ;
– études médico-économiques.

2.2. **Origine et nature des données**

2.2.1. *Origine des données à caractère personnel*

2.2.1.1. Les données doivent provenir exclusivement et directement des bases de données mises à disposition par la CNAM.

2.2.2. *Nature des données à caractère personnel*

2.2.2.1. En application de l'article 5, paragraphe 1, point c, du RGPD, les données traitées doivent être pertinentes, adéquates et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (principe de minimisation des données). A cet égard, le responsable de traitement s'engage à ne traiter que les données strictement nécessaires et pertinentes au regard des objectifs de l'étude. Dès lors, chacune des catégories de données ne peut être traitée que si leur traitement est justifié dans le protocole.

2.2.2.2. Les catégories de données à caractère personnel suivantes peuvent faire l'objet d'un traitement dans le cadre de la présente méthodologie :

Pour les personnes concernées :

2.2.2.3. Seules les données issues de la base principale du SNDS, telle que définie à l'article R. 1461-2 du code de la santé publique, peuvent être traitées. Cette dernière comporte à ce jour :

- les données issues des systèmes d'information mentionnés à l'article L. 6113-7 du code de la santé publique (base PMSI) ;
- les données du système national d'information interrégimes de l'assurance maladie mentionné à l'article L. 161-28-1 du code de la sécurité sociale (base SNIIRAM) ;
- les données sur les causes de décès mentionnées à l'article L. 2223-42 du code général des collectivités territoriales (base du CépiDC de l'INSERM) ;
- les données médico-sociales du système d'information mentionné à l'article L. 247-2 du code de l'action sociale et des familles (données relatives au handicap) ;
- les données issues des bases de données « Vaccin-Covid » et « SI-DEP » (système d'information de dépistage).

2.2.2.4. Les traitements inclus dans le cadre de la présente méthodologie de référence portent sur les données dont la profondeur historique maximale est de neuf ans en plus de l'année en cours, sous réserve qu'elles soient diffusables par la CNAM.

2.2.2.5. Doivent notamment être justifiés dans le protocole au regard de la finalité du traitement : les catégories de données traitées, la période de ciblage des personnes concernées, les composantes du SNDS et la profondeur historique des données consultées demandées, la durée d'accès, la zone géographique et le nombre de personnes concernées.

Pour les utilisateurs :

2.2.2.6. Les catégories de données à caractère personnel relatives aux utilisateurs pouvant faire l'objet du traitement sont les suivantes :

- nom, prénoms, fonction, profils d'accès ;
- si pertinent :
  - coordonnées téléphoniques, postales et/ou électroniques professionnelles, organisme employeur ;
  - formation, diplômes ;
  - éléments nécessaires à l'évaluation des connaissances afin de réaliser l'étude.

2.2.2.7. Les traitements de données des utilisateurs doivent avoir pour seule finalité la mise en œuvre de l'étude et le respect des obligations légales du responsable de traitement.

2.2.2.8. En particulier, les données traitées ont pour finalité la gestion des déclarations d'intérêts, leur transmission à la PDS, le cas échéant et la gestion des procédures d'habilitation internes.

2.3. **Accédants et destinataires des données traitées (utilisateurs)**

2.3.1. Le responsable de traitement ou, le cas échéant, le responsable de la mise en œuvre du traitement, tient à jour des documents indiquant la ou les personnes compétentes en son sein pour délivrer l'habilitation à accéder aux données, la liste des personnes habilitées à accéder à ces données, leurs profils d'accès respectifs et les modalités d'attribution, de gestion et de contrôle des habilitations.

2.3.2. Seules les personnes habilitées par le responsable de traitement ou, le cas échéant, par le responsable de la mise en œuvre du traitement, peuvent avoir accès aux données traitées au regard de leurs fonctions et dans des conditions conformes à la réglementation.

2.3.3. Ces catégories de personnes sont soumises au secret professionnel dans les conditions définies par les articles 226-13 et 226-14 du code pénal.

2.3.4. La qualification des personnes habilitées et leurs droits d'accès doivent être régulièrement réévalués, conformément aux modalités décrites dans la procédure d'habilitation établie par le responsable de traitement ou par le responsable de la mise en œuvre du traitement.

2.4. **Information et droits des personnes concernées par l'étude**

2.4.1. *Information des personnes*

2.4.1.1. S'agissant de données provenant exclusivement du SNDS, les personnes concernées sont informées de la réutilisation possible de leurs données de santé à caractère personnel selon des modalités définies par l'article R. 1461-9 du code de la santé publique.

2.4.1.2. Les dispositions de l'article 69 de la loi « informatique et libertés », qui posent le principe d'une information individuelle des personnes dont les données sont traitées, sont applicables à tous les traitements réalisés à partir de données du SNDS.

2.4.1.3. Toutefois, en application des dispositions de l'article 14.5.b du RGPD, le responsable de traitement peut faire valoir une exception à l'obligation d'information individuelle pour la mise en œuvre d'un traitement comportant exclusivement des données issues de la base principale du SNDS.

2.4.1.4. Dans cette hypothèse, il devra prendre des mesures appropriées pour protéger les droits et libertés ainsi que les intérêts légitimes des personnes concernées, y compris en rendant les informations publiquement disponibles.

2.4.1.5. A cet égard, l'information des personnes concernées ne peut se limiter à l'inscription de l'étude au sein du répertoire public de la PDS.

2.4.1.6. Dans le cadre de cette méthodologie de référence, la réalisation de chaque recherche, étude ou évaluation dans le domaine de la santé doit être portée à la connaissance du public.

2.4.1.7. *A minima*, les mesures suivantes doivent être mises en œuvre pour garantir une information publiquement disponible :

– la diffusion de la note d'information sur le site web du responsable de traitement ainsi que, le cas échéant, du laboratoire de recherche ou bureau d'études ;
– la mise en place d'un portail de transparence lorsque le responsable de traitement réalise plusieurs études à partir des données du SNDS. Ce portail de transparence comporte une information générale sur le SNDS et une note d'information spécifique à chaque étude mise en œuvre.

2.4.1.8. D'autres modalités d'information collective peuvent également être prévues, en fonction des caractéristiques des études réalisées (réseaux sociaux, associations de patients, communiqué de presse, etc.).

2.4.1.9. Ces documents doivent comporter l'ensemble des mentions prévues à l'article 14 du RGPD.

2.4.2. *Exercice des droits des personnes*

2.4.2.1. La personne concernée exerce ses droits d'accès, de rectification, d'effacement, de limitation du traitement et d'opposition concernant le **traitement mis en œuvre dans le cadre de la présente méthodologie,** directement auprès du **délégué à la protection des données de l'organisme responsable du traitement.**

2.4.2.2. L'information des utilisateurs, ainsi que les modalités d'exercice de leurs droits, doivent être conformes au principe de transparence prévu au chapitre III du RGPD.

2.5. **Durée d'accès ou de conservation des données**

2.5.1. Cette durée doit être strictement nécessaire à la mise en œuvre du traitement et ne doit pas excéder la durée de l'étude. En tout état de cause, la durée d'accès ou de conservation ne peut excéder cinq ans à compter de la dernière mise à disposition effective des données. Cette durée peut exceptionnellement être prolongée pour une durée maximale de deux ans, sur demande motivée du responsable de traitement, adressée au CESREES, qui rend alors un nouvel avis. Aucun archivage des données ne peut être réalisé.

2.5.2. Les données à caractère personnel traitées dans le cadre de cette méthodologie ne peuvent faire l'objet d'une conservation en dehors de l'environnement maîtrisé auquel le responsable de traitement ou son sous-traitant a recours.

2.5.3. Seuls des résultats anonymes, au sens de l'avis du groupe de l'article 29 (G29) n° 05/2014 ou à tout avis ultérieur du CEPD relatif à l'anonymisation, peuvent être exportés.

2.5.4. Les données à caractère personnel des utilisateurs chargés de la réalisation de l'étude ne peuvent être conservées au-delà d'un délai de cinq ans après la fin de l'étude.

2.6. **Publication des résultats**

2.6.1. Conformément aux dispositions de la loi « informatique et libertés », la présentation des résultats du traitement de données ne peut en aucun cas permettre l'identification directe ou indirecte des personnes concernées.

TITRE III

SÉCURITÉ

3.1. Le traitement des données du Système national des données de santé et de ses composantes devra s'effectuer en conformité avec les dispositions des articles L. 1461- 1 à L. 1461-7 du code de la santé publique.

3.2. Les mesures de sécurité devront être conformes au référentiel de sécurité applicable au Système national des données de santé, prévu par l'arrêté du 22 mars 2017 et ses mises à jour ultérieures.

3.3. Conformément au référentiel précité, lorsque le responsable de traitement a recours à un laboratoire de recherche ou un bureau d'études, le responsable de traitement doit s'assurer que le contrat conclu avec le laboratoire de recherche ou bureau d'études précise les mesures et les conditions de sécurité relatives à la conformité au référentiel précité. En particulier, l'environnement maîtrisé devra avoir fait l'objet d'une homologation préalablement à la mise en œuvre du traitement de données nécessaire à l'étude.

3.4. Le responsable de traitement ou, le cas échéant, le responsable de la mise en œuvre du traitement, doit adopter les mesures techniques et organisationnelles suivantes :

Répartition des rôles et responsabilités	
SEC-REP-1	La répartition des rôles et responsabilités entre le ou les responsables de traitement, le responsable de la mise en œuvre du traitement et le gestionnaire de l'environnement maîtrisé doit être formalisée par une convention. Cette dernière doit porter notamment sur la sensibilisation des utilisateurs de l'étude, la surveillance des traces, la gestion des alertes et des incidents ainsi que la gestion des exportations de données anonymes. Cette convention devra être conforme à l'article 28 du RGPD.
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 de besoin et de façon exclusive.
SEC-HAB-2	Les personnes habilitées à accéder aux données à caractère personnel doivent être individuellement habilitées selon une procédure impliquant une validation par leur responsable hiérarchique.
SEC-HAB-3	Une revue des habilitations doit être réalisée régulièrement et *a minima* annuellement, ainsi qu'à la fin de chaque étude.
SEC-HAB-4	Les permissions d'accès doivent être retirées dès le retrait des habilitations, par exemple après le départ d'un utilisateur habilité ou une modification de ses missions.
Identification et authentification des utilisateurs	
SEC-IDE-1	L'accès aux données à caractère personnel doit être subordonné à une identification locale ou nationale pour toute personne physique ou morale, conformément aux exigences du palier 2 du Référentiel d'identification de la PGSSI-S.
SEC-IDE-2	L'accès aux données à caractère personnel doit être subordonné à une authentification forte faisant intervenir *a minima* deux facteurs d'authentification distincts, conformément aux exigences du palier 2 du Référentiel d'authentification de la PGSSI-S. Si un de ces facteurs est un mot de passe, celui-ci doit être conforme aux recommandations de la CNIL en matière de mots de passe à la date de rédaction de cette méthodologie de référence (délibération n° 2022-100 du 21 juillet 2022).
Espace projet	
SEC-ESP-1	Les données d'une étude doivent être manipulées par les utilisateurs habilités uniquement dans un espace projet spécifique à cette étude, étanche avec les données du SNDS central ainsi qu'avec les espaces projets d'autres études conduites dans le même environnement maîtrisé.
SEC-ESP-2	Les jeux de données importés dans un espace projet spécifique à une étude doivent être minimisés et limités aux seules données nécessaires à l'étude. Un numéro pseudonyme unique spécifique à chaque espace projet doit être généré dans les mêmes conditions de pseudonymisation que celles définies par le référentiel de sécurité applicable au SNDS précité. Par exemple, ce numéro pseudonyme unique pourra être généré par une fonction de hachage cryptographique résistante aux attaques par force brute ou un générateur de nombres pseudo-aléatoires cryptographiquement sûr.
Transmission de données	
SEC-TRA-1	Toutes les transmissions de données depuis ou vers l'environnement maîtrisé ou les espaces projets 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. Ces mesures de chiffrement s'appliquent aux données en transit et à leur stockage après réception dans l'environnement maîtrisé ou les espaces projets.
Exportation de données anonymes hors des espaces de travail	
SEC-EXP-1	Seuls des jeux de données anonymes peuvent faire l'objet d'une exportation hors de l'environnement maîtrisé ou d'un espace projet. 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. A défaut, si ces trois critères ne peuvent être réunis, une étude des risques de réidentification devra être menée et documentée, préalablement à chaque exportation.
SEC-EXP-2	Les exportations de données doivent être soumises 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 exportations 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, toute exportation identifiée 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 vérifiée manuellement par un responsable spécifiquement formé et habilité.
Sensibilisation des utilisateurs et sécurité des postes de travail	
SEC-SEN-1	Chaque personne habilitée à accéder à l'environnement maîtrisé doit être formée au respect du secret professionnel et sensibilisée régulièrement aux risques et obligations inhérents au traitement de données de santé.
SEC-SEN-2	Chaque personne habilitée à accéder à l'environnement maîtrisé doit signer une charte de confidentialité. Celle-ci doit préciser notamment les obligations au regard à la fois de la protection des données à caractère personnel de santé et des mesures de sécurité mises en place dans l'environnement maîtrisé, 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'environnement maîtrisé, y compris les utilisateurs externes accédant uniquement aux espaces projet, doivent faire l'objet de mesures de sécurité spécifiques, par exemple en mettant en place des comptes nominatifs, une authentification adéquate, un verrouillage automatique des sessions, un chiffrement des disques durs 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 projet et celles des utilisateurs de l'environnement maîtrisé doivent faire l'objet de mesures de journalisation, conformément aux exigences du palier 3 du Référentiel d'imputabilité de la PGSSI-S. En particulier, les connexions (identifiants, date et heure), les requêtes et les opérations réalisées doivent être tracées.
SEC-JOU-2	Un contrôle des traces doit être réalisé régulièrement et *a minima* mensuellement, ainsi qu'à la fin de chaque période d'habilitation liée à une étude. Ce contrôle doit être réalisé par : – une solution réalisant une surveillance automatique avec une remontée d'alertes traitées manuellement par un opérateur habilité ; ou – 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-3	Les traces de journalisation définies aux exigences SEC-JOU-1 doivent être conservées pour une durée de six mois à un an à compter de leur collecte, sauf exception justifiée par l'importance du risque pour les personnes en cas de détournement des finalités du traitement et de la fréquence d'occurrences de telles pratiques. Dans ce dernier cas, la durée de conservation maximale des traces de journalisation peut être étendue à trois ans.
Gestion des incidents de sécurité et des violations de données à caractère personnel	
SEC-INC-1	Les parties à la convention doivent prévoir 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	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.

3.5. Ces mesures ne sont pas exhaustives et devront être complétées au regard des risques pesants sur le traitement mis en œuvre.

3.6. De plus, 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 et que les mesures soient conformes à l'état de l'art.

TITRE IV

SOUS-TRAITANTS

4.1. Lorsque le responsable de traitement fait appel à un ou des sous-traitants, il s'assure que ceux-ci présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées, de manière à ce que le traitement réponde aux exigences du RGPD et de la loi « informatique et libertés » et garantisse la protection des droits de la personne concernée.

4.2. Un responsable de traitement peut notamment choisir comme sous-traitant un établissement de santé, une fédération hospitalière ou un laboratoire de recherche ou bureau d'études.

4.3. Le responsable de traitement établit avec le sous-traitant un contrat ou un autre acte juridique précisant les obligations de chaque partie et reprenant les exigences de l'article 28 du RGPD.

4.4. Par ailleurs, les sous-traitants :

– doivent désigner, le cas échéant, un délégué à la protection des données conformément à l'article 37 du RGPD ;
– doivent tenir un registre des catégories de traitements effectués pour le compte du responsable de traitement, conformément à l'article 30 du RGPD.

TITRE V

HÉBERGEMENT DES DONNÉES DU SNDS ET ABSENCE DE TRANSFERT DE DONNÉES HORS DE L'UNION EUROPÉENNE

5.1. Dans le cadre de la présente méthodologie de référence, le ou les responsables de traitement de l'étude s'assurent :

– que les données issues de la base principale du SNDS hébergées dans l'environnement maîtrisé le sont exclusivement au sein des pays membres de l'espace économique européen et sans transfert possible en dehors de l'Union européenne ;
– de l'absence d'accès distant aux données depuis l'extérieur du territoire de l'Union européenne.

5.2. Par ailleurs, les organismes et le cas échéant, leurs sous-traitants, accédant aux données du SNDS dans le cadre de la réalisation des opérations d'hébergement de l'infrastructure technique de l'environnement maîtrisé, ainsi que l'administration et l'exploitation associées à ce stockage, doivent être exclusivement soumis aux lois de l'Union européenne.

TITRE VI

MISE EN ŒUVRE DU PRINCIPE DE RESPONSABILITÉ

6.1. **Analyse d'impact sur la protection des données**

6.1.1. Le responsable de traitement effectue une analyse d'impact relative à la protection des données menée conformément aux dispositions de l'article 35 du RGPD, qui doit couvrir en particulier les risques sur les droits et libertés des personnes concernées.

6.1.2. Cette analyse d'impact doit être réexaminée et mise à jour régulièrement, notamment si des changements importants sont prévus dans le traitement mis en œuvre dans le cadre de la présente méthodologie ou si les risques pour les personnes concernées ont évolué.

6.1.3. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques semblables.

6.2. **Formalités**

6.2.1. Chaque responsable de traitement désigne un délégué à la protection des données, en application de l'article 37 du RGPD. Ce délégué à la protection des données aura notamment pour mission de vérifier le respect de la conformité des traitements mis en œuvre selon la présente méthodologie.

6.2.2. Le responsable de traitement adresse à la CNIL une seule déclaration de conformité à la présente méthodologie pour l'ensemble des traitements qu'il met en œuvre dès lors qu'ils sont et seront réalisés en conformité avec l'ensemble des dispositions de la méthodologie.

6.2.3. Dans le cadre d'une responsabilité conjointe, chaque responsable de traitement procède à une déclaration de conformité à la méthodologie de référence pour son propre compte.

6.2.4. Les traitements visés par la présente méthodologie de référence doivent obtenir un avis expressément favorable du CESREES préalablement à leur mise en œuvre. Pour obtenir cet avis, un dossier doit être déposé auprès du secrétariat unique de la PDS et doit comporter les éléments listés dans la présente méthodologie.

6.2.5. Conformément à l'article 30 du RGPD, le responsable de traitement tient à jour, au sein du registre des activités de traitement, la liste des traitements mis en œuvre dans le cadre de la présente méthodologie. Il vérifie régulièrement la conformité des traitements en cours au regard des exigences de la méthodologie de référence et documente cette analyse.

6.3. **Principe de transparence**

6.3.1. Le cadre juridique permettant la mise à disposition des données du SNDS est conçu de façon à rendre compte de leur utilisation à la population. A cette fin, l'article L. 1461-3 II du CSP subordonne l'accès aux données du SNDS et de ses composantes à la communication à la PDS de plusieurs éléments par le responsable de traitement, avant et après la réalisation des études.

6.3.2. Ainsi, le responsable du traitement s'engage à enregistrer dans le répertoire public tenu par la PDS chaque étude réalisée dans le cadre de cette méthodologie.

6.3.3. Cet enregistrement doit être effectué, avant le début de chaque étude, par le responsable de traitement ou la personne agissant pour son compte. Il s'accompagne de la transmission à la PDS d'un dossier comportant :

- le protocole, incluant la justification de l'intérêt public, ainsi qu'un résumé, selon le modèle mis à disposition par la PDS. En cas d'avis favorable avec recommandations du CESREES, le protocole et le résumé tenant compte de manière apparente des recommandations, doivent être enregistrés ;
- la déclaration d'intérêts, en rapport avec l'objet de l'étude, du responsable du traitement et le cas échéant du sous-traitant.

6.3.4. A la fin de l'étude, la méthode et les résultats obtenus devront être communiqués à la PDS en vue de leur publication.

6.3.5. L'enregistrement du traitement et la transmission des résultats sont effectués conformément aux modalités définies par la PDS.

6.4. **Bilan**

6.4.1. Le responsable de traitement, le cas échéant après avoir consulté le ou les sous-traitants, transmet tous les trois ans à la CNIL un bilan synthétisant les usages observés de la présente méthodologie de référence, en indiquant notamment :

- le nombre d'études mises en œuvre sur la période analysée ;
- les types de finalités poursuivies ;
- les modalités de financement des projets et partenaires (notamment financements publics, etc.) ;
- concernant les données traitées :
  - les composantes du SNDS majoritairement sollicitées ;
  - la conformité globale de l'expression des besoins aux objectifs de l'étude ;

  - la profondeur historique moyenne sollicitée et son caractère suffisant ou non ;
  - le nombre moyen de personnes concernées par les études ;
  - la moyenne de la durée d'accès ou de conservation des données sollicitée et leur caractère suffisant ou non ;
- les supports d'information collective mis en œuvre ;
- la qualité des personnes habilitées à accéder aux données du SNDS ;
- concernant la sécurité des données :
  - les incidents de sécurité, susceptibles d'impacter les droits des personnes, éventuellement révélés ou évités ;
  - toute modification substantielle de l'architecture de l'environnement maîtrisé ;
- le nombre de publications scientifiques découlant des recherche, études et évaluations réalisées dans le cadre de la méthodologie ;
- les bénéfices, apports scientifiques observés et/ou mesurés.

TITRE VII

ENTRÉE EN VIGUEUR

7.1. La présente méthodologie de référence entre en vigueur à compter de sa publication au *Journal officiel*.

7.2. Lorsqu'une recherche, étude ou évaluation dans le domaine de la santé, autorisée antérieurement par la CNIL, fait l'objet d'une modification substantielle et est conforme à la présente méthodologie, il n'est pas nécessaire d'obtenir une nouvelle autorisation de la CNIL.

7.3. La présente délibération sera publiée au *Journal officiel* de la République française.