METHODOLOGIE DE REFERENCE

RELATIVE AUX TRAITEMENTS DE DONNEES DU SNDS ET DES RESUMES DE PASSAGES AUX URGENCES (RPU) MIS EN ŒUVRE PAR LES RESPONSABLES DE TRAITEMENT AGISSANT DANS LE CADRE DE LEUR MISSION D'INTERET PUBLIC (MR-005)

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

1. Observations préalables

1.1 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 (ci-après « le RGPD ») et notamment son article 5, point 2, prévoit que le responsable de traitement doit être en mesure de démontrer que les principes du règlement sont respectés.

1.2 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.

1.3 Ainsi, en application de la loi du 6 janvier 1978 modifiée (ci-après « 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 (ci-après « la Commission »).

1.4 La Commission 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 (ci-après « PDS »), ainsi qu'avec les organismes publics et privés représentatifs des acteurs concernés.

1.5 Compte tenu de leurs missions d'intérêt public, un grand nombre d'acteurs, dont les fédérations et les établissements de santé, réalisent des études 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.).

1.6 Dès 2018, la Commission a adopté une méthodologie de référence 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 (ci-après « PMSI ») et des résumés de passages aux urgences (ci-après « RPU ») centralisées et mises à disposition sur la plateforme sécurisée de l'Agence technique de l'information sur l'hospitalisation (ci-après « ATIH »).

1.7 Compte tenu de l'évolution du cadre légal et réglementaire de la recherche dans le domaine de la santé et des propositions effectuées par les organismes acteurs de la recherche, il est apparu nécessaire de l'actualiser et d'élargir son périmètre.

1.8 Les responsables de traitement qui adressent une déclaration de conformité à cette méthodologie de référence sont autorisés à mettre en œuvre les traitements dès lors que ceux-ci répondent aux conditions prévues par ces dispositions.

2. Définitions

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

2.2 **Bulle sécurisée** : infrastructure technique servant à l'hébergement d'un ou plusieurs systèmes fils conformément au référentiel de sécurité applicable au SNDS et mettant en œuvre des mesures techniques et organisationnelles afin de cloisonner les différentes extractions du SNDS pouvant être stockées au sein de cette bulle afin d'empêcher toute fusion de ces données ;

2.3 **Comité éthique et scientifique pour les recherches, les études et les évaluations dans le domaine de la santé (CESREES)** : il s'agit du 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 et sur le caractère d'intérêt public que présente la recherche, l'étude ou l'évaluation ;

2.4 **Espace de travail** : environnement informatique configuré et mis à disposition des utilisateurs sur la solution sécurisée dédiée à une étude ;

2.5 **Etude :** recherche 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 (ci-après « CSP ») et présentant un caractère d'intérêt public au sens de l'article 66 de la loi « informatique et libertés ». Une étude peut nécessiter la réalisation de plusieurs requêtes à partir des données du SNDS ;

2.6 **Laboratoire de recherche/bureau d'études** : responsable de la mise en œuvre du traitement de données et chargé de leur analyse, ayant réalisé un engagement de conformité auprès de la Commission 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 ;

2.7 **Personnes chargées de la réalisation de l'étude** : la ou les personnes physiques qui travaillent sur les données individuelles du SNDS et les données des RPU mises à disposition sur une solution sécurisée ;

2.8 **PMSI** : système rassemblant les données de l'activité hospitalière pseudonymisées mises à disposition et centralisées par l'ATIH ou la Caisse nationale de l'assurance maladie (CNAM). Il peut s'agir des données annuelles définitives ou infra-annuelles ;

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

2.10 **Protocole** : document 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, ainsi que, lorsque les caractéristiques de l'étude l'exigent, la justification du nombre de personnes et la méthode d'observation retenue. Le protocole devra également comporter une expression de besoins s'agissant de l'accès aux données du SNDS historique comprenant notamment la population ciblée, la période de ciblage, la profondeur historique des données et la durée d'accès demandées ;

2.11 **RPU** : résumés des passages aux urgences centralisés et mises à disposition par l'ATIH ;

2.12 **Solution sécurisée** : portail de mise à disposition des données géré par l'ATIH, la CNAM, et le Centre d'accès sécurisé aux données (CASD), ainsi que l'ensemble des systèmes fils tels que définis par la présente MR ;

2.13 **Système fils** : système d'information hébergeant ou mettant à disposition des données relatives au SNDS à des fins de recherche, d'étude ou d'évaluation, transmises par le SNDS central ou un autre système fils. Sont uniquement concernées par la présente méthodologie de référence les bulles sécurisées prévues dans le cadre d'un traitement de données ayant fait l'objet d'une autorisation expresse de la CNIL datant de moins de trois ans, et dont l'homologation fait l'objet d'un suivi régulier par le responsable de traitement ;

2.14 **Système national des données de santé** : base de données couvrant l'ensemble de la population et réunissant les données mentionnées aux 1° à 4° du I de l'article L. 1461-1 du CSP (ci-après « SNDS » ou « SNDS historique »).

3. Responsables de traitements concernés

3.1 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 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.

3.2 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.

4. Traitements de données à caractère personnel inclus dans le champ d'application de la présente méthodologie

4.1 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 d'études 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 :

- les traitements visés par la présente méthodologie de référence doivent obtenir un avis expressément favorable [sans recommandation] du CESREES préalablement à leur mise en œuvre. En cas d'avis favorable avec recommandations, le responsable de traitement s'engage à prendre en compte les recommandations préalablement à la mise en œuvre du traitement ;

- les traitements de données ne peuvent être réalisés que par l'intermédiaire d'une solution sécurisée selon l'une ou l'autre des modalités suivantes :

    - les données sont mises à disposition du responsable de traitement ou du laboratoire de recherche ou bureau d'études auquel il a recours sur le portail de la CNAM, l'ATIH ou le CASD ;
    - les données sont mises à disposition du responsable de traitement ou du laboratoire de recherche ou bureau d'études dans une bulle sécurisée, telle que définie au point 1.1 (Définitions).

- 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 peut héberger les données au sein d'un système fils à condition de remplir les conditions cumulatives suivantes :

    - le système fils a fait l'objet d'une homologation par le responsable de traitement conformément au référentiel de sécurité applicable au SNDS. Cette homologation fait l'objet d'un suivi régulier et est régulièrement renouvelée dans les délais prévus par la décision d'homologation ;
    - le système fils a été expertisé par la CNIL dans le cadre d'un traitement de données ayant fait l'objet d'une autorisation expresse par la Commission ;
    - cette autorisation expresse doit dater de moins de trois ans ;

- le responsable de traitement devra signer une convention d'accès aux données avec le gestionnaire de la solution sécurisée mettant à disposition les données du SNDS et des RPU ainsi qu'un engagement individuel de chaque personne habilitée à respecter les conditions d'utilisation définies par la solution sécurisée. Le responsable de traitement devra lui transmettre la liste, actualisable, des laboratoires de recherche ou bureaux d'études auxquels il a recours ;

- un protocole comprenant une expression de besoins doit être élaboré par le responsable de traitement avant le début de la mise en œuvre du traitement des données. Ce protocole devra être soumis au CESREES.

4.2 La présente méthodologie de référence n'est pas applicable aux traitements :

- nécessitant un export des données à caractère personnel en dehors de la solution sécurisée utilisée ;

- nécessitant un appariement des données du SNDS et des RPU avec des données à caractère personnel issues d'autres sources (exemple : dossiers médicaux, *etc.*).

5. Intérêt public et finalités interdites

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

- répondre à un caractère d'intérêt public, justifié par le responsable de traitement dans le protocole et 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), et notamment l'interdiction d'utiliser ces données pour les finalités décrites à l'article L. 1461-1 V du code la santé publique.
  Deux finalités sont ainsi expressément interdites :
  - 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.

6. Finalité des traitements

6.1 Seules les finalités d'études dans le domaine de la santé ou encore de planification et de valorisation de l'offre de soins détaillées ci-dessous sont couvertes par 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 territoire (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 dans le cadre d'une recherche impliquant ou n'impliquant pas la personne humaine ;
- études épidémiologiques ;
- études médico-économiques.

7. Origine et nature des données

7.1 Origine des données à caractère personnel

7.1.1 Les données doivent provenir exclusivement des bases de données mises à disposition par :

- l'ATIH au titre du PMSI et des RPU ;
- la CNAM au titre des données du SNDS.

7.2 Nature des données à caractère personnel

7.2.1 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.

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

7.2.3 Pour les personnes concernées par les études :

7.2.4 Les données issues du SNDS et des RPU mises à disposition sur une solution sécurisée par l'ATIH ou la CNAM et en particulier :

- **Pour les données centralisées par l'ATIH** : les données des RPU, ainsi que l'ensemble des fichiers dans les champs :
  - médecine, chirurgie, obstétrique et odontologie (MCO) ;
  - soins de suite et de réadaptation (SSR) ;
  - recueil d'information médicalisée en psychiatrie (RIM-P) ;
  - hospitalisation à domicile (HAD) ;
  - avec la possibilité de relier toutes les données du PMSI concernant un même patient au moyen du fichier « ANO ».

- **Pour les données mises à disposition par la CNAM** :
  - 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).

7.2.5 Les traitements inclus dans le cadre de la présente méthodologie de référence portent sur les données dont la profondeur historique maximale est de [cinq ans].

7.2.6 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.

7.2.7 Pour les personnes chargées de la réalisation de l'étude

7.2.8 Les seules catégories de données à caractère personnel relatives aux personnes chargées de la réalisation de l'étude pouvant faire l'objet du traitement sont les suivantes :

- nom, prénom(s), 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.

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

7.2.10 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.

8. Destinataires des données à caractère personnel traitées

8.1 Les données sont mises à disposition du responsable de traitement ou de son sous-traitant, par l'intermédiaire d'une solution sécurisée.

8.2 Le responsable de 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.

8.3 Seul le personnel habilité par le responsable de traitement peut avoir accès aux données traitées au regard de leurs fonctions et dans des conditions conformes à la réglementation.

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

8.5 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.

9. Information et droits des personnes concernées par l'étude

9.1 S'agissant de données provenant exclusivement du SNDS et des RPU, 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.

9.2 Les dispositions de l'article 69 de la loi « informatique et libertés » sont applicables à tous les traitements réalisés à partir de données du SNDS. Conformément aux dispositions de l'article 14 du RGPD, dans l'hypothèse où la fourniture d'une information individuelle se révélerait impossible, exigerait des efforts disproportionnés ou compromettrait gravement la réalisation des objectifs du traitement, des mesures appropriées devront être mises en œuvre par le responsable de traitement afin de protéger les droits et libertés, ainsi que les intérêts légitimes de la personne concernée, y compris en rendant les informations publiquement disponibles.

9.3 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 du SNDS historique, s'il justifie précisément dans son registre d'activité de traitement et dans l'analyse d'impact relative à la protection des données que :

- la fourniture des informations exigerait des efforts disproportionnés, conformément à l'article 14.5.b du RGPD ;
- des garanties seront mises en œuvre afin de protéger les droits et libertés ainsi que les intérêts légitimes des personnes concernées.

9.4 A ce titre, le responsable de traitement doit prendre les mesures appropriées afin de rendre l'information publiquement disponible concernant la réalisation de chaque étude mise en œuvre dans le cadre de cette méthodologie de référence, notamment en utilisant plusieurs vecteurs pour diffuser cette information (communication sur les réseaux sociaux, dans les médias régionaux, auprès d'associations de patients, publication d'un communiqué de presse, envoi d'une newsletter, affichage dans les locaux, les salles d'attentes, *etc.*).

9.5 Cette information ne doit pas se limiter à l'inscription du traitement au sein du portail de transparence de la PDS. Une publication doit être systématiquement prévue sur le site internet du responsable de traitement ainsi que, le cas échéant, du laboratoire de recherche ou bureau d'études. Lorsqu'un responsable de traitement réalise plusieurs études à partir des données du SNDS, il devra mettre en place un portail de

transparence comportant une information générale sur le SNDS et pour chaque étude mise en œuvre, il devra également prévoir une note d'information spécifique à chaque étude.

9.6 L'information dispensée doit être conforme aux dispositions de l'article 14 du RGPD, et en particulier s'agissant de la source des données ainsi que des modalités d'exercice des droits.

9.7 Les droits d'accès, de rectification, d'effacement, de limitation du traitement, et d'opposition s'exercent par la personne concernée auprès du directeur de la PDS ou du directeur de l'organisme gestionnaire du régime d'assurance maladie obligatoire auquel la personne est rattachée, conformément aux dispositions de l'article R. 1461-9 du code de la santé publique.

9.8 L'information des personnes chargées de l'étude ainsi que les modalités d'exercice de leurs droits sont conformes au principe de transparence prévu au chapitre III du règlement général sur la protection des données.

10. Durée d'accès ou de conservation des données

10.1 La durée d'accès aux données dans la solution sécurisée ou la durée de conservation dans le système fils doit être limitée à la durée strictement nécessaire à la mise en œuvre du traitement. Celle-ci ne doit pas excéder la durée de l'étude. La durée d'accès ou de conservation ne peut excéder trois ans à compter de la mise à disposition effective des données. Aucun archivage des données ne peut être réalisé.

10.2 Les données à caractère personnel traitées dans le cadre de cette méthodologie ne peuvent faire l'objet d'une conservation en dehors de la solution sécurisée à laquelle le responsable de traitement ou son sous-traitant a recours.

10.3 Seuls des résultats anonymes peuvent être exportés.

10.4 Les données à caractère personnel des personnes concernées chargées de la réalisation de l'étude ne peuvent être conservées au-delà d'un délai de cinq ans après la fin de l'étude.

11. Publication des résultats

11.1 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.

12. Sécurité

12.1 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.

12.2 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.

12.3 Conformément au référentiel fixé par l'arrêté du 17 juillet 2017 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 attestant de la conformité à l'arrêté du 22 mars 2017 précité.

12.4 Enfin, le responsable de 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 et le gestionnaire de la solution sécurisée doit être formalisée par une convention, concernant notamment la sensibilisation des utilisateurs de l'étude, la surveillance des traces, la gestion des alertes et des incidents ainsi que la gestion des exports 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 utilisant des données stockées dans la solution sécurisée.
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 mot de passe (délibération n° 2017-012 du 19 janvier 2017 à la date de rédaction de cette méthodologie de référence).
Espace de travail	
SEC-ESP-1	Les données de l'étude doivent être manipulées par les utilisateurs habilités uniquement dans des espaces de travail spécifiques à chaque étude, étanches avec les données du SNDS central et étanches les uns des autres.
SEC-ESP-2	Les jeux de données importées dans un espace de travail spécifique à une étude doivent être minimisés et limités aux seules données nécessaires à l'étude. Un numéro pseudonyme unique spécifique à chaque espace de travail 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 la solution sécurisée ou les espaces de travail 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.
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 la solution sécurisée 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.
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 un espace cloisonné et dédié, puis doit être vérifié 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 la solution sécurisée 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 la solution sécurisée doit signer une charte de confidentialité précisant notamment ses obligations au regard de la protection des données personnelles de santé et au regard des mesures de sécurité mises en place dans la solution sécurisée, ainsi que les sanctions afférentes au non-respect de ces obligations.
SEC-SEN-3	Les postes de travail des personnes habilitées à accéder à la solution sécurisée, y compris les utilisateurs externes accédant uniquement aux espaces de travail, doivent faire l'objet de mesures de sécurité spécifique, par exemple en mettant en place des comptes nominatifs, une authentification adéquate, un verrouillage automatique des sessions, un chiffrement des 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 de travail de la solution sécurisée 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 à cette solution (identifiants, date et heure), les requêtes et opérations réalisées doivent être tracées.
SEC –JOU-3	Un contrôle des traces doit être réalisé régulièrement et *a minima* mensuellement, ainsi qu'à la fin de chaque période d'habilitation liée à 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 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 doivent être conservées pour une durée de six mois à un an à compter de leur collecte.
Gestion des incidents de sécurité et des violations de données à caractère personnel	
SEC-INC-1	Le responsable de traitement prévoit une procédure de gestion et de traitement des incidents de sécurité et des violations de données personnelles, précisant les rôles et responsabilités et les actions à mener en cas de survenue de tels incidents.
SEC-INC-2	Tout incident de sécurité, d'origine malveillante ou non et se produisant de manière intentionnelle ou non, ayant comme conséquence, même temporaire, de compromettre l'intégrité, la confidentialité ou la disponibilité de données personnelles, doit faire l'objet d'une documentation en interne dans un registre des violations.
SEC-INC-3	Toute violation de données doit être notifiée à la CNIL dans les conditions prévues à l'article 33 du RGPD.
SEC-INC-4	Dans l'hypothèse où la violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable de traitement est tenu de communiquer la violation des données aux personnes concernées dans les meilleurs délais, conformément à l'article 34 du RGPD.

12.5 Ces mesures ne sont pas exhaustives et devront être complétées au regard de la réévaluation régulière des risques pesants sur le traitement mis en œuvre.

12.6 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 celles-ci soient conformes à l'état de l'art.

13. Sous-traitants

13.1 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, de la loi « informatique et libertés » et garantisse la protection des droits de la personne concernée.

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

13.3 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.

13.4 Par ailleurs, le sous-traitant :

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

14. Transfert de données hors de l'Union européenne

14.1 Dans le cadre de la présente méthodologie de référence :

- aucun transfert de données en dehors de l'Union européenne ne peut être effectué, y compris vers un pays considéré comme adéquat, conformément à l'article R. 1461-1 du code de la santé publique. Est considéré comme transfert tout accès distant aux données depuis l'extérieur du territoire de l'Union européenne ;
- le sous-traitant doit être exclusivement soumis aux lois et aux juridictions de l'Union européenne.

15. Analyse d'impact sur la protection des données

15.1 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. Il met en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté aux risques identifiés. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques similaires.

16. Formalités

16.1 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.

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

16.3 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 à l'article 89 du décret n° 2019-536 du 29 mai 2019.

16.4 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.

17. Principe de transparence

17.1 La mise à disposition des données du SNDS et des RPU est conçue de façon à rendre compte de leur utilisation à la société civile. A cette fin, l'article L. 1461-3 du code de la santé publique 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 les études.

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

17.3 Cet enregistrement, à effectuer par le responsable de traitement ou la personne agissant pour son compte, avant le début des études, s'accompagne de la transmission à la PDS d'un dossier comportant :

- le protocole, comportant une expression des besoins et incluant la justification de l'intérêt public, ainsi qu'un résumé, selon le modèle mis à disposition par la PDS;
- en rapport avec l'objet de l'étude, la déclaration d'intérêts du responsable du traitement, et le cas échéant celle du sous-traitant.

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

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

18. Entrée en vigueur

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

18.2 La délibération n° 2018-256 du 7 juin 2018 portant homologation d'une méthodologie de référence relative aux traitements de données nécessitant l'accès par des établissements de santé et des fédérations aux données du PMSI et des RPU centralisées et mises à disposition sur la plateforme sécurisée de l'ATIH (MR005) est abrogée.

18.3 Les traitements de données mis en œuvre en application de la délibération précitée peuvent se poursuivre dans le respect des dispositions de la présente délibération.

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