Décrets, arrêtés, circulaires

TEXTES GÉNÉRAUX

MINISTÈRE DU TRAVAIL, DE LA SANTÉ ET DES SOLIDARITÉS

Arrêté du 6 mai 2024 relatif au référentiel de sécurité applicable au Système national des données de santé

NOR : *TSSE2407926A*

Le ministre délégué auprès de la ministre du travail, de la santé et des solidarités, chargé de la santé et de la prévention, et la secrétaire d'État auprès du ministre de l'économie, des finances et de la souveraineté industrielle et numérique, chargée du numérique,

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 le code de la santé publique, notamment ses articles L. 1461-1 et R. 1461-7 ;

Vu le code de la recherche, notamment son article L. 225-1 ;

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

Vu l'avis de la Commission nationale de l'informatique et des libertés en date du 20 juillet 2023,

Arrêtent :

Art. 1er. – Le référentiel mentionné au 3° du IV de l'article L. 1461-1 et au II de l'article R. 1461-7 du code de la santé publique figure en annexe au présent arrêté.

Art. 2. – L'arrêté du 22 mars 2017 relatif au référentiel de sécurité applicable au Système national des données de santé est abrogé.

Art. 3. – I. – Les systèmes d'information existants soumis au référentiel fixé par l'arrêté du 22 mars 2017 relatif au référentiel de sécurité applicable au Système national des données de santé sont mis en conformité avec le référentiel fixé par le présent arrêté pour leur prochaine homologation de sécurité, et au plus tard dans un délai de deux ans à compter de la publication du présent arrêté. Durant ces délais, ces systèmes d'information restent conformes au référentiel fixé par l'arrêté du 22 mars 2017 précité.

II. – Les systèmes d'information existants non soumis au référentiel fixé par l'arrêté du 22 mars 2017 précité sont mis en conformité avec le référentiel fixé par le présent arrêté dans un délai maximal de deux ans à compter de sa publication.

III. – Les gestionnaires des systèmes d'information mentionnés aux I et II définissent, dans un délai maximal de six mois, un plan d'action de mise en conformité avec le référentiel fixé par le présent arrêté, indiquant les mesures à prendre dans l'immédiat puis à court et moyen terme. Dans le même délai, ils mènent une analyse de risques et mettent en place des actions garantissant la confidentialité et l'intégrité des données, ainsi que la traçabilité des accès et traitements de ces données, afin d'assurer la protection des données et le respect de la vie privée des personnes concernées.

IV. – Les systèmes d'information créés après l'entrée en vigueur du présent arrêté sont en conformité avec le référentiel fixé par ce dernier dès leur création.

Art. 4. – Le présent arrêté sera publié au *Journal officiel* de la République française.

Fait le 6 mai 2024.

Le ministre délégué auprès de la ministre du travail, de la santé et des solidarités, chargé de la santé et de la prévention,
FRÉDÉRIC VALLETOUX

La secrétaire d'État auprès du ministre de l'économie, des finances et de la souveraineté industrielle et numérique, chargée du numérique,
MARINA FERRARI

ANNEXE

RÉFÉRENTIEL DE SÉCURITÉ DU SYSTÈME NATIONAL DES DONNÉES DE SANTÉ

1. **Définitions**

Les concepts suivants sont utilisés dans le référentiel :

☐ Administrateur fonctionnel : personnel en charge de l'administration fonctionnelle du système et des transmissions de données du système.

☐ Administrateur technique : personnel au sein des équipes du gestionnaire du système considéré en charge de l'administration technique du système (la gestion des infrastructures, des systèmes, des bases de données, la mise en place de nouveaux environnements de travail, etc.).

☐ Anonymisation : processus empêchant toute ré-identification directe ou indirecte de personnes physiques.

☐ Base principale : elle réunit les données mentionnées aux 1° à 4° du I de l'article L. 1461-1 du code de la santé publique (CSP), complétées progressivement de données mentionnées aux 5° à 11° au I de ce même article.

☐ Bases du catalogue : les bases de données du catalogue comprennent des données mentionnées aux 1° à 11° du I de l'article L. 1461-1 du code de la santé publique. Ces bases sont inscrites dans l'arrêté pris en application de l'article R. 1461-2 du même code.

☐ Chaînage des données du SNDS : procédé permettant de relier entre elles les données correspondant à un même individu au sein du SNDS, quelle que soit la source de données. Le chaînage des données rend possible la mise en relation de différentes données se rattachant à un même individu et la réalisation de traitement sur ces dernières.

☐ Données à faible risque : données dont la divulgation à une personne non autorisée a un impact limité sur la vie privée.

☐ Données à fort risque : données dont la divulgation à une personne non autorisée a un impact élevé sur la vie privée.

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

☐ Espace projet : espace de travail sécurisé et maîtrisé par le gestionnaire du système mettant à disposition des données du SNDS.

☐ Gestionnaire du système : responsable de l'ensemble des composants matériels et logiciels du système, du choix et de l'exploitation des services de télécommunication mis en œuvre, de la mise en œuvre de la conformité et du suivi opérationnel du système.

☐ Mise à disposition : rendre accessible aux utilisateurs les données d'un système du SNDS pour la réalisation de leurs traitements au titre du L. 1461-3 du code de la santé publique.

L'accès aux données est réalisé via :

– l'ouverture de l'accès à un espace projet [ou d'un accès permanent] ;

– le transfert de données d'un système à un autre système qui correspond à une transmission de données.

Une mise à disposition est considérée comme étant à un tiers à partir du moment où la personne physique ou morale, l'autorité publique, le service ou un autre organisme accédant aux données n'est pas responsable de traitement du système mettant à disposition les données, notamment dans le cas des co-responsabilités de traitements.

☐ Pseudonymisation : procédé visant à la génération d'un identifiant pseudonymisé, appelé ici pseudonyme, à partir d'un identifiant initial signifiant lié à une personne (par exemple : nom, prénom, le numéro d'inscription des personnes (NIR) au répertoire national d'identification des personnes physiques). Le procédé de pseudonymisation doit empêcher l'identification directe (par exemple à partir du prénom, nom, NIR) de la personne associée à ce pseudonyme (l'identification indirecte reste toutefois possible) et contribue à ce titre au respect de la vie privée des individus.

☐ Ré-identification : capacité à découvrir l'identité réelle d'une ou plusieurs personnes dont on ne connaît pas directement l'identité (par exemple par déduction ou inférence sur un ou plusieurs jeux de données).

☐ Responsable de traitement : le responsable de traitement est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens d'un traitement, c'est à dire l'objectif et la façon de le réaliser.

☐ Système du SNDS : système rassemblant des données mentionnées au I du L. 1461-1 du code de la santé publique et assurant leur mise à disposition pour les finalités prévues au III du même article, qui couvre trois catégories :

- ☐ SNDS central : système du SNDS réunissant, organisant et mettant à disposition l'ensemble des données qui constituent la base principale et les bases du catalogue. La responsabilité de traitement est conjointe entre la CNAM et la Plateforme des données de santé (en application de l'article R. 1461-3 du CSP).
- ☐ Système fils : système du SNDS rassemblant des données mentionnées au I du L. 1461-1 du code de la santé publique provenant d'un système du SNDS (SNDS central, système fils du SNDS ou autre système du SNDS) et assurant leur mise à disposition pour les finalités prévues au III du même article.
- ☐ Autre système du SNDS : système du SNDS, rassemblant des données mentionnées au I du L. 1461-1 du code de la santé publique, ne répondant ni à la définition de SNDS central, ni à celle de système fils.

☐ Sortie de données : opération réalisée par un utilisateur qui consiste à exporter des données en dehors de l'environnement maitrisé. Seules des données anonymes peuvent faire l'objet d'une sortie par un utilisateur de l'environnement maîtrisé.

☐ 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. Les sous-traitants ont des obligations concernant les données personnelles, qui doivent être formalisées dans un contrat ou tout acte juridique conforme aux exigences de l'article 28 du règlement (UE) 2016/679 du 27 avril 2016 (RGPD).

☐ Tiers : une personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel.

☐ Transmission de données : envoi de données d'un système à un autre système.

☐ Utilisateur : personne physique accédant à des données d'un système du SNDS dans un espace projet pour la réalisation d'un traitement au titre du L. 1461-3 du code de la santé publique sous la responsabilité d'un responsable de traitement.

2. **Introduction**

2.1. *Contexte*

La loi OTSS de 2019 a modifié l'organisation du Système national des données de santé afin de donner un cadre pour faciliter le recueil, le rassemblement, et la mise à disposition des données de santé dans des conditions de sécurité indispensables. Elle élargit le champ des données du SNDS et les finalités d'usages et ajoute à l'acteur historique (la CNAM) un acteur de mise à disposition des données le groupement d'intérêt public « Plateforme des données de santé » qui reprend également les missions de l'Institut national des données de santé.

L'article L. 1461-1 du code de la santé publique instaure ainsi le Système national des données de santé (SNDS).

Le Système national des données de santé rassemble et met à disposition :

1° Les données issues des systèmes d'information mentionnés à l'article L. 6113-7 du code de la santé publique ;

2° 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 ;

3° Les données sur les causes de décès mentionnées à l'article L. 2223-42 du code général des collectivités territoriales ;

4° Les données médico-sociales du système d'information mentionné à l'article L. 247-2 du code de l'action sociale et des familles ;

5° Un échantillon représentatif des données de remboursement par bénéficiaire transmises par des organismes d'assurance maladie complémentaire et défini en concertation avec leurs représentants ;

6° Les données destinées aux professionnels et organismes de santé recueillies à l'occasion des activités mentionnées au I de l'article L. 1111-8 du présent code donnant lieu à la prise en charge des frais de santé en matière de maladie ou de maternité mentionnée à l'article L. 160-1 du code de la sécurité sociale et à la prise en charge des prestations mentionnées à l'article L. 431-1 du même code en matière d'accidents du travail et de maladies professionnelles ;

7° Les données relatives à la perte d'autonomie, évaluée à l'aide de la grille mentionnée à l'article L. 232-2 du code de l'action sociale et des familles, lorsque ces données sont appariées avec les données mentionnées aux 1° à 6° du présent I ;

8° Les données à caractère personnel des enquêtes dans le domaine de la santé, lorsque ces données sont appariées avec des données mentionnées aux 1° à 6° ;

9° Les données recueillies lors des visites médicales et de dépistage obligatoire prévues à l'article L. 541-1 du code de l'éducation ;

10° Les données recueillies par les services de protection maternelle et infantile dans le cadre de leurs missions définies à l'article L. 2111-1 du présent code ;

11° Les données de santé recueillies lors des visites d'information et de prévention, telles que définies à l'article L. 4624-1 du code du travail.

Le SNDS a pour finalité la mise à disposition des données pour contribuer :

1° A l'information sur la santé ainsi que sur l'offre de soins, la prise en charge médico-sociale et leur qualité ;

2° A la définition, à la mise en œuvre et à l'évaluation des politiques de santé et de protection sociale ;

3° A la connaissance des dépenses de santé, des dépenses d'assurance maladie et des dépenses médico-sociales ;

4° A l'information des professionnels, des structures et des établissements de santé ou médico-sociaux sur leur activité ;

5° A la surveillance, à la veille et à la sécurité sanitaires ;

6° A la recherche, aux études, à l'évaluation et à l'innovation dans les domaines de la santé et de la prise en charge médico-sociale.

2.2. *Objet du document*

Compte tenu de la nature des données et des finalités de leurs usages, et notamment du fait que ce sont des données personnelles de santé pseudonymisées, le dispositif législatif et réglementaire du SNDS a prévu un référentiel de sécurité propre au SNDS pour les responsables de traitement et les gestionnaires des différents systèmes concernés. Le référentiel précise ainsi les exigences en regard de ces traitements qui comprennent des exigences générales mais aussi des exigences particulières au SNDS.

Le présent document, intitulé « Référentiel de sécurité applicable au Système national des données de santé », est ainsi pris en application des dispositions du 3° du IV de l'article L. 1461-1 du code de la santé publique qui prévoient que : « L'accès aux données s'effectue dans des conditions assurant la confidentialité et l'intégrité des données et la traçabilité des accès et des autres traitements, conformément à un référentiel défini par arrêté des ministres chargés de la santé, de la sécurité sociale et du numérique, pris après avis de la Commission nationale de l'informatique et des libertés ».

2.3. *Périmètre d'application*

Les exigences du présent référentiel s'appliquent au périmètre suivant :

- au SNDS central pour l'alimentation, l'hébergement, la transmission, y compris entre les gestionnaires de système du SNDS central, et la mise à disposition des données ;
- à l'ensemble des systèmes fils pour l'hébergement, la transmission et la mise à disposition des données ;
- pour les autres systèmes du SNDS :
  - s'il y a mise disposition de données du SNDS, à cette mise à disposition dès lors qu'elle est faite à un tiers pour des finalités du SNDS ainsi qu'à l'hébergement des données mises à disposition ;
  - s'il y a transmission de données SNDS, à cette transmission pour des finalités SNDS.

Ainsi, les exigences du référentiel de sécurité ne s'appliquent pas :

- aux autres systèmes contenant des données du SNDS, utilisées pour leurs propres finalités et non mises à disposition à des tiers.

Pour les données anonymes, les exigences du référentiel ne s'appliquent plus. Ce référentiel n'a pas vocation à définir les méthodes d'anonymisation ou de qualification du caractère anonyme de ces données.

3. **Exigences générales**

3.1. *Exigences générales en termes de sécurité des systèmes d'information*

Chaque gestionnaire de système soumis à l'application du présent référentiel doit respecter les règles de ce dernier, de la politique de sécurité des systèmes d'information pour les ministères chargés des affaires sociales (PSSI MCAS) ainsi que, le cas échéant, du décret n° 2022-513 du 8 avril 2022 relatif à la sécurité numérique du système d'information et de communication de l'Etat et de ses établissements publics. Le gestionnaire du système constitue et regroupe la documentation nécessaire à la conformité de son projet au regard des dispositions du règlement général sur la protection des données (RGPD), ainsi qu'aux dispositions de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés (LIL).

Le gestionnaire du système doit adopter la démarche suivante avant sa mise en production :

- ☐ Réalisation d'une analyse de risques « sécurité des systèmes d'information » ;
- ☐ Réalisation d'une analyse d'impact relative à la protection des données (AIPD) ;
- ☐ Mise en œuvre des mesures de couverture des risques associées ;
- ☐ Réalisation d'étapes de recette et de tests pour s'assurer de la bonne couverture des risques ;
- ☐ Réalisation d'une homologation de sécurité sur le périmètre sous sa responsabilité ;
- ☐ Suivi opérationnel de la sécurité du système d'information.

Le gestionnaire du système doit s'assurer que les conditions légales précitées sont réunies avant de permettre aux utilisateurs et aux administrateurs l'accès aux données d'un système du SNDS. Dans le cadre d'un accès via des espaces projets ouverts par le gestionnaire du système, la mise en sécurité et l'homologation du dispositif de mise à disposition des données est à la charge du gestionnaire du système.

Tout projet ayant un impact significatif sur la sécurité d'un système du SNDS soumis au présent référentiel (modification de l'architecture, inclusion de nouveaux types de données, inclusion d'un nouveau logiciel, revue des accès, etc.) doit donner lieu à une revue de l'analyse de risques du système concerné.

En cas de modification des caractéristiques essentielles de cette analyse de risques (par exemple l'apparition de nouveaux risques majeurs), une revue de l'homologation du système concerné doit être réalisée.

3.2. *Territorialité*

Conformément à l'article R. 1461-1 du code de la santé publique : « Les données du SNDS sont hébergées au sein de l'Union européenne. Aucun transfert de données de santé à caractère personnel ne peut être réalisé en dehors du territoire de l'Union européenne, sauf dans le cas d'accès ponctuels aux données par des personnes situées en dehors de l'Union européenne, pour une finalité relevant du 1° du I de l'article L. 1461-3. »

Les gestionnaires ou les sous-traitants susceptibles d'être soumis à la législation d'un pays tiers n'assurant pas un niveau de protection adéquat au sens de l'article 45 du RGPD, ont pour obligation d'identifier les législations susceptibles de permettre un accès non autorisé par le droit de l'Union aux données, au sens de l'article 48 du RGPD, de mettre en œuvre des mesures pour atténuer les risques d'accès non autorisé induits par ces réglementations et d'identifier les risques résiduels qui demeureraient malgré ces mesures.

3.3. *Sous-traitance des systèmes d'informations*

Dans le cas d'une sous-traitance ou d'une sous-traitance en cascade de tout ou partie d'un système soumis à l'application du présent référentiel, les exigences suivantes sont applicables à cette externalisation :

☐ Réalisation d'une analyse de risques préalable par le sous-traitant sur le périmètre externalisé ;

☐ Encadrement contractuel de l'externalisation avec le sous-traitant. En particulier, le sous-traitant doit s'engager à respecter les règles du présent référentiel sur le périmètre externalisé, y compris les exigences relatives à la territorialité ;

☐ Définition des modalités d'audits et de contrôle de sécurité pour s'assurer du respect des engagements du sous-traitant.

Dans le cas d'une mise à disposition de données du SNDS par un des responsables de traitement mentionnés au II de l'article L. 1461-1 du code de la santé publique, ces derniers ne sont pas considérés comme des sous-traitants.

3.4. *Sous-traitance des traitements*

La mise à disposition de données du SNDS par l'un des gestionnaires du SNDS central relève du périmètre de leur responsabilité de traitement. Ces derniers ne sont donc pas considérés comme des sous-traitants agissant pour le compte de tiers habilités à traiter les données.

Néanmoins, si la Plateforme des données de santé procède à des opérations pour le compte de tiers dans les conditions prévues par le 6° de l'article L. 1462-1 du code de la santé publique, elle sera considérée comme sous-traitant pour cette partie des traitements de données. A ce titre, elle devra garantir aux responsables de traitement, par voie de convention, le respect des exigences du présent référentiel qui leur incombent.

Dans le cas d'une sous-traitance des traitements ou d'une sous-traitance en cascade, le sous-traitant doit se conformer par convention aux exigences du présent référentiel qui s'appliquent au responsable de traitement.

3.5. *Classification des données*

La classification de données comme étant à faible risque doit se fonder sur une analyse de risques. A défaut, les données doivent être considérées comme étant à fort risque.

3.6. *Sensibilisation*

Chaque gestionnaire des systèmes soumis à l'application du présent référentiel doit régulièrement mettre en place des actions de sensibilisation et de formation à destination des utilisateurs auxquels il met à disposition des données du SNDS pour les finalités SNDS et à destination des administrateurs (utilisation des données, conséquence en cas de mauvaise utilisation, bonnes pratiques, responsabilité, trace…).

3.7. *Archivage des données*

Le traitement des données archivées et des données sauvegardées est soumis au présent référentiel. Les gestionnaires du SNDS central doivent s'assurer que les données archivées et sauvegardées de leur périmètre restent lisibles pendant la durée légale de conservation. Il convient, en particulier, de prévoir à chaque migration de technologie une récupération des données sur les technologies précédentes.

3.8. *Environnements hors production*

Les données de production ne peuvent pas être utilisées sur des environnements hors production sauf si le présent référentiel est appliqué sur lesdits environnements.

4. **Transmission des données**

4.1. *Alimentation du SNDS central*

L'alimentation du SNDS central doit se faire uniquement si le système l'alimentant respecte les mesures adéquates pour sécuriser les données de bout en bout lors de la transmission. Cette alimentation doit se faire dans le cadre d'une convention entre le ou les responsables de traitements des données qui constituent le SNDS central et les producteurs de données et qui doit comprendre :

☐ Une procédure d'alimentation des données précisant quelles sont les données transmises, identifiées dans le cadre de la loi (article L. 1461-1 du CSP) précisant les responsabilités et rôles de chacun des gestionnaires de système ;

☐ Un engagement sur les modalités sécurisant les données de bout en bout lors de la transmission ;

☐ Un engagement par le responsable de traitement du système alimentant le SNDS central de fournir les preuves mises à jour de la conformité de la transmission au présent référentiel.

Les gestionnaires de système du SNDS central doivent construire et maintenir à jour un inventaire des jeux de données l'alimentant et des conventions associées.

4.2. *Transmission de données entre les responsables de traitement du SNDS central*

Les transmissions entre les responsables de traitements des données qui constituent le SNDS central font l'objet de conventions entre la CNAM et la PDS qui en précisent les modalités et les conditions de sécurité.

4.3. *Transmission de données vers un système fils*

La transmission de données vers un système fils depuis le SNDS central ou depuis un autre système fils ou depuis un autre système du SNDS, doit se faire uniquement si le destinataire respecte, avant la transmission, le présent référentiel.

Cette transmission doit se faire dans le cadre d'une convention.

La convention entre le gestionnaire de système transmettant les données et le gestionnaire de système recevant les données doit comprendre :

☐ Une procédure de transmission des données précisant quelles sont les données autorisées à être transmises, identifiées dans le cadre d'une autorisation accordée par la CNIL ou par les autres conditions prévues par la loi ;

☐ Un engagement sur les modalités sécurisant les données de bout en bout lors de la transmission ;

☐ Un engagement sur le respect des règles du présent référentiel ;

☐ Un engagement du système recevant les données de fournir les preuves mises à jour de sa conformité au présent référentiel.

Chaque gestionnaire de système soumis au présent référentiel pour la transmission de données doit tenir à jour un inventaire des données transmises et des systèmes les recevant.

4.4. *Mise à disposition des données*

La mise à disposition de données dans le cadre des finalités du SNDS, à un tiers depuis le SNDS central ou depuis un système fils ou depuis un autre système du SNDS, doit se faire dans le cadre d'une convention entre le gestionnaire du système mettant à disposition des données et le responsable du traitement accédant à ces données comprenant :

☐ Une procédure de mise à disposition des données précisant quelles sont les données autorisées à être mises à disposition, identifiées dans le cadre d'une autorisation accordée par la CNIL ou par les autres conditions prévues par la loi ;

☐ Un engagement sur le respect des règles du présent référentiel notamment sur les modalités d'accès.

Les données des systèmes soumis au présent référentiel peuvent être mises à disposition dans un espace projet.

Chaque gestionnaire de système soumis au présent référentiel pour la mise à disposition de données doit tenir à jour un inventaire des données mises à disposition et d'un registre des utilisateurs y accédant.

4.5. *Sorties des données*

Seules des données anonymes peuvent faire l'objet d'une sortie par un utilisateur en dehors de l'environnement maitrisé

5. **Accès aux données**

5.1. *Autorisation d'accès aux données du SNDS*

Tout accès d'une personne à un jeu de données du SNDS ne doit être ouvert que pour une durée déterminée, conforme à celle précisée dans l'autorisation accordée par la CNIL ou par les autres conditions prévues par la loi

Pour les traitements utilisant des données du SNDS, les personnes responsables de ces traitements, ainsi que celles les mettant en œuvre ou autorisées à accéder aux données non anonymes qui en sont issues, sont soumises au secret professionnel dans les conditions et sous les peines prévues à l'article 226-13 du code pénal.

La mise à disposition des données du SNDS est réalisée par un administrateur technique du système concerné, après validation par le responsable de traitement.

Les utilisateurs et les administrateurs de systèmes doivent s'être engagés par contrat ou un autre acte juridique à respecter les conditions générales d'utilisation du SNDS, à savoir :

☐ Engagement de confidentialité, notamment sur la non-diffusion des données non anonymes ;

☐ Absence d'actions visant la réidentification d'individu ;

☐ Engagement de respect des règles du référentiel de sécurité mises en œuvre pour le SNDS ;

☐ Engagement à ne pas poursuivre une des finalités interdites du SNDS mentionnées au V de l'article L. 1461-1 du code de la santé publique.

Conformément à l'article 77 de la LIL, en cas d'urgence qui serait motivée par exemple par le non-respect des exigences du présent référentiel ou en cas d'incident grave, les gestionnaires de systèmes SNDS peuvent suspendre temporairement l'accès au système SNDS dont ils ont la responsabilité. Ils doivent en informer immédiatement le ou les responsables de traitement, ainsi que le président du comité d'audit et le président de la Commission nationale de l'informatique et des libertés. Le rétablissement de l'accès est décidé par le gestionnaire de système, après accord du président de cette commission, au regard des mesures correctives prises par le ou les responsables de traitement.

Toute violation de données susceptible d'engendrer un risque pour les droits et libertés des personnes physiques impliquée par l'incident grave ou l'urgence ayant motivé la suspension temporaire de l'accès au système SDNS doit faire l'objet d'une notification à l'autorité compétente, dans les conditions prévues par le RGPD.

Les utilisateurs et les administrateurs de systèmes doivent être informés de l'existence de ces mesures.

5.2. *Modalités d'accès aux données du SNDS*

Chaque gestionnaire de système doit définir ses exigences de disponibilité en concertation avec ses utilisateurs.

L'accès à l'environnement doit se faire à partir d'un poste respectant les exigences de la PSSI-MCAS et cette exigence peut être imposée par convention si nécessaire.

Les administrateurs ne doivent pas avoir accès à internet depuis les environnements d'administration du SNDS.

Un utilisateur ne doit pas pouvoir modifier les données du SNDS central.

5.3. *Paliers d'identification et d'authentification*

L'accès à des données du SNDS nécessite une identification et une authentification pour toute personne physique ou morale, conformément aux exigences du règlement 910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE (règlement EIDAS). Le niveau de garantie doit être le niveau substantiel précisé dans le règlement d'exécution 2015/1502 du 8 septembre 2015 fixant les spécifications techniques et procédures minimales relatives aux niveaux de garantie des moyens d'identification électronique visés à l'article 8, paragraphe 3, du règlement 910/2014.

6. **Pseudonymisation**

6.1. *Pseudonymisation des données des systèmes du SNDS*

Les identifiants individuels des personnes concernées stockés dans un des systèmes soumis au référentiel de sécurité ne peuvent être que des pseudonymes. Un pseudonyme est obtenu par une opération cryptographique irréversible sur un identifiant ; il est non signifiant et ne permet pas d'identifier directement la personne concernée. Aucun gestionnaire de système ne doit posséder à la fois l'ensemble des données à caractère personnel ayant servi à générer le pseudonyme et le pseudonyme généré dans un des systèmes du SNDS soumis au référentiel de sécurité, sauf autorisation de la CNIL.

Les pseudonymes des bénéficiaires doivent être différents d'un système du SNDS soumis au référentiel de sécurité à l'autre et différents de ceux du SNDS central.

Toute pseudonymisation mise en œuvre dans le cadre du SNDS doit être fondée sur des fonctions cryptographiques robustes répondant aux besoins suivants :

☐ Etre irréversible (impossibilité de disposer d'une transformation inverse permettant de passer d'un pseudonyme à un identifiant initial) ;

☐ Ne pas générer de collision ou à un niveau négligeable non impactant (deux identifiants initiaux différents donneront deux pseudonymes différents) ;

☐ Avoir un bon effet d'avalanche (deux identifiants initiaux de valeurs proches donneront deux pseudonymes de valeurs éloignées) ;

☐ Etre une fonction d'agrégation (pour une même transformation, association à un identifiant initial d'un seul et même pseudonyme et association à un seul pseudonyme d'un unique identifiant initial) ;

☐ Etre paramétrable (utilisation possible de différents secrets) ;

☐ Etre identifiable (la fonction utilisée doit être identifiable dans son résultat) ;

☐ Pour l'alimentation du SNDS central s'opérer sur plusieurs niveaux (2 minimum) avec des secrets différents, non dérivés les uns des autres et s'exécutant dans des organismes distincts.

En cas de compromission avérée du secret de pseudonymisation ou de fuite avérée et significative de données avec pseudonymes, l'ensemble des données potentiellement impactées doit faire l'objet d'une nouvelle pseudonymisation.

6.2. *Conservation et gouvernance de la valeur secrète*

Le secret utilisé par une fonction de pseudonymisation doit être supprimé (si cette fonction n'est plus utile à la suite des traitements) ou conservé de manière sécurisée. A ce titre, seules les personnes dûment habilitées doivent pouvoir accéder à ce secret et cet accès doit se faire dans le cadre d'une procédure définie et formalisée.

Les accès à ce secret doivent être fondés sur des mécanismes robustes et tracés de manière à assurer l'imputabilité individuelle de l'accédant. La connaissance et l'utilisation de ce secret sont encadrées par un processus de divulgation maitrisé.

En aucun cas le receveur d'un jeu de données ne doit détenir le secret ayant permis la pseudonymisation du jeu de données considéré. Seul le gestionnaire du système transmettant les données est autorisé à le détenir.

Après leur mise en place, les accès aux secrets de pseudonymisation et à leurs sauvegardes doivent être tracés.

6.3. *Renouvellement des pseudonymes*

Une nouvelle pseudonymisation de l'ensemble du système a également lieu au plus tard toutes les six années pour assurer le niveau de sécurité des secrets et des fonctions de pseudonymisation. Des procédures permettant de modifier les secrets doivent être mises en place à cet effet.

Le gestionnaire d'un système qui reçoit des données doit accepter les changements découlant d'un changement de secret décidé par le gestionnaire du système transmettant les données.

6.4. *Usages de la pseudonymisation dans le SNDS*

6.4.1. Pseudonymisation

La CNAM a à sa charge la pseudonymisation du SNDS sur le périmètre de responsabilité décrit au 3° du II de l'article R. 1461-3 du CSP. Elle s'engage à la mettre en œuvre avec des techniques à l'état de l'art de la sécurité applicable et nécessaire à son contexte et dans le respect du présent référentiel.

6.4.2. Pseudonymisation des données transmises vers la Plateforme de données de santé

Lors du transfert des données du SNDS de la CNAM vers la PDS, la CNAM applique un niveau de pseudonymisation avant transmission de ces données à la PDS, laquelle y applique à son tour au moins un niveau de pseudonymisation dès réception.

6.4.3. Pseudonymisation pour les mises à disposition de données du SNDS à des utilisateurs

Les pseudonymes pour mises à disposition de données du SNDS aux utilisateurs, et ce pour chaque traitement, doivent faire l'objet d'un niveau de pseudonymisation supplémentaire ou bien faire l'objet d'une substitution par un numéro aléatoire qui doit être volatile s'il n'y a pas de besoin de chaînage entre deux mises à disposition.

6.4.4. Pseudonymisation pour l'appariement de données avec celles du SNDS

Les jeux de données devant être appariés au SNDS doivent être pseudonymisés par les chaînes de pseudonymisation propres au SNDS central administré par la CNAM ou à celles du SNDS central administré par la PDS selon les cas.

6.4.5. Pseudonymisation pour la transmission vers des systèmes fils

Avant la transmission vers un système fils, les pseudonymes des données SNDS doivent faire l'objet pour chaque système fils d'un niveau de pseudonymisation supplémentaire ou bien faire l'objet d'une substitution par un numéro aléatoire qui doit être volatile s'il n'y a pas de besoin de chaînage entre deux mises à disposition.

6.4.6. Pseudonymisation pour la transmission de données depuis un système du SNDS vers un autre système du SNDS

La pseudonymisation est de la responsabilité du gestionnaire du système transmettant les données. Elle doit respecter le présent référentiel de sécurité.

6.4.7. Pseudonymisation des demandes d'exercice de droit

Pour les demandes d'exercice des droits, les identifiants communiqués doivent être pseudonymisés par les chaînes de pseudonymisation propres au SNDS central administré par la CNAM et au SNDS central administré par la PDS.

7. **Traçabilité**

La traçabilité doit permettre de contrôler l'utilisation de données et de disposer de preuves pouvant être instruites en justice avec éventuellement un caractère probant.

7.1. *Paliers d'imputabilité*

Les paliers d'imputabilité suivants du référentiel d'imputabilité de la PGSSI-S doivent être mis en place pour le SNDS :

☐ Le palier minimum d'imputabilité des accès des utilisateurs du SNDS est le palier 3 ;

☐ Le palier minimum d'imputabilité des administrateurs techniques et fonctionnels du SNDS pour les opérations d'exportation de données à partir de données à fort risque est le palier 3.

7.2. *Journaux de traces*

Chaque gestionnaire de système du SNDS soumis au référentiel de sécurité doit disposer de dispositifs de journalisation permettant de conserver une trace des événements de sécurité sur leur périmètre.

Cette journalisation doit s'inscrire dans le cadre des conventions prévues dans les chapitres 4.1, 4.2, 4.3 et 4.4 du présent référentiel, indiquant en particulier les conditions dans lesquelles les traces sont collectées, traitées, conservées et restituées.

Les traces doivent être conservées pour une durée de 6 mois dans le respect des textes encadrant le traitement de données à caractère personnel.

7.3. *Règles de surveillance et de détection*

Chaque gestionnaire de système du SNDS soumis au référentiel de sécurité est responsable de la surveillance des comportements anormaux, en lien avec l'analyse de risque conduite par le gestionnaire, pour le périmètre dont il a la responsabilité.

7.4. *Horodatage des journaux*

Chaque gestionnaire de système du SNDS soumis au référentiel de sécurité doit s'assurer, au sein de son système, qu'une référence de temps commune est employée.

Les références de temps utilisées pour les systèmes du SNDS soumis au référentiel de sécurité doivent être cohérentes entre elles, c'est-à-dire que les décalages entre ces références doivent être connus.

7.5. *Traitement des incidents*

En fonction de l'impact des incidents détectés sur les systèmes du SNDS, les conventions de transmission de données et les procédures de gestion des incidents de sécurité, formalisées par chacun des gestionnaires de système du SNDS, doivent prévoir la notification voire la mobilisation d'autres gestionnaires de systèmes du SNDS.

8. **Contrôle**

8.1. *Audits*

Tous les systèmes du SNDS soumis au référentiel de sécurité doivent être contrôlés *a minima* tous les trois ans pour le périmètre soumis au présent référentiel (fonctionnellement et techniquement) dans le cadre d'audits internes. Ces systèmes peuvent aussi faire l'objet d'audits externes commandités par le comité d'audit prévu à l'article 77 de la LIL ou par d'autres organismes qui en ont l'autorité.

8.2. *Revue des habilitations*

Chaque responsable de traitement doit tenir à jour une liste des personnes compétentes en son sein pour délivrer l'habilitation à accéder aux données du SNDS et une 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.

Chaque responsable de traitement doit mettre en place une revue annuelle des habilitations et chaque gestionnaire de système SNDS doit également mettre en place une revue des habilitations pour les administrateurs du système dont il est gestionnaire.

9. **Droits des personnes**

Le II de l'article R. 1461-9 du code de la santé publique cite les droits des personnes qui s'appliquent lorsque les données relèvent de la base principale ou des bases inscrites au catalogue et décrit leur modalité d'exercice.

Conformément au IV de l'article R. 1461-9 du code de la santé publique, les responsables conjoints de traitement s'assurent de donner suite aux demandes d'exercice de droits des personnes concernées. Une convention entre les responsables conjoints de traitement décrit le circuit et la procédure spécifique garantissant l'exercice des droits.

Conformément à l'article 4 de l'arrêté du 12 mai 2022 relatif aux données alimentant la base principale et aux bases de données du catalogue du Système national des données de santé une convention entre l'organisme responsable de la base de données alimentant le catalogue et la Plateforme des données de santé définit les droits et obligations des parties, notamment concernant l'exercice des droits des personnes.