Décrets, arrêtés, circulaires

TEXTES GÉNÉRAUX

MINISTÈRE DES AFFAIRES SOCIALES ET DE LA SANTÉ

Arrêté du 22 mars 2017 relatif au référentiel de sécurité applicable au Système national des données de santé

NOR : *AFSE1705146A*

Le ministre de l'économie et des finances et la ministre des affaires sociales et de la santé,

Vu le code de la santé publique, notamment son article L. 1461-1 ;

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

Vu l'avis de la Commission nationale de l'informatique et des libertés en date du 26 janvier 2017,

Arrêtent :

Art. 1er. – Le référentiel mentionné au 3° du IV de l'article L. 1461-1 du code de la santé publique est fixé conformément à l'annexe du présent arrêté.

Art. 2. – La mise en application du référentiel de sécurité s'effectue selon les règles suivantes :

– le Système national des données de santé (SNDS) et tous les systèmes d'information traitant des données de santé issues du SNDS existants à la date d'entrée en vigueur du présent arrêté devront être en conformité totale avec le référentiel mentionné à l'article 1 dans un délai maximum de deux ans à compter de cette même date ;

– dès la création du SNDS, le responsable du traitement et les gestionnaires de systèmes d'information existants traitant des données de santé issues du SNDS doivent définir un plan d'action de mise en conformité indiquant les mesures à prendre dans l'immédiat puis à court et moyen terme. Ils doivent, dans les mêmes délais, mener une analyse de risques et mettre en place des actions garantissant la protection des données et le respect de la vie privée des personnes afin d'assurer la confidentialité et l'intégrité des données et la traçabilité des accès ;

– les nouveaux systèmes d'information, créés après l'entrée en vigueur du présent arrêté, traitant des données de santé issues du SNDS doivent être en conformité avec le référentiel dès leur création.

Art. 3. – Le présent arrêté sera publié au *Journal officiel* de la République française.

Fait le 22 mars 2017.

La ministre des affaires sociales et de la santé,
MARISOL TOURAINE

Le ministre de l'économie et des finances,
MICHEL SAPIN

ANNEXE

RÉFÉRENTIEL DE SÉCURITÉ APPLICABLE AU SYSTÈME NATIONAL DES DONNÉES DE SANTÉ

1. **Introduction**

1.1. *Contexte*

L'article 193 de la loi de modernisation de notre système de santé du 26 janvier 2016 instaure le Système national des données de santé (SNDS).

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

☐ Les données issues des systèmes d'information des établissements de santé, publics ou privés ;

☐ Les données du Système national d'information inter-régimes de l'assurance maladie (SNIIRAM) ;

☐ Les données sur les causes de décès ;

☐ Les données médico-sociales du système d'information des maisons départementales des personnes handicapées ;

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

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

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

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

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

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

☐ A la surveillance, à la veille et à la sécurité sanitaire ;

☐ 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.

1.2. *Objet du document*

Le présent document, intitulé « Référentiel de sécurité applicable au système national des données de santé » découle d'une disposition du titre VI du code de la santé publique instauré par la loi :

« 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 ».

1.3 *Périmètre d'application*

Le présent référentiel s'applique au SNDS central ainsi qu'à tous les systèmes mettant à disposition des données du SNDS.

Les exigences s'appliquent aux systèmes mettant à disposition des jeux de données ré-identifiants du SNDS. Pour les jeux de données anonymes, une fois exportés, les exigences du référentiel ne s'appliquent plus.

Ce référentiel n'a pas vocation à définir les méthodes d'anonymisation et de qualification du caractère anonyme d'un jeu de données.

2. **Définitions**

Les concepts suivants sont utilisés dans le référentiel :

☐ 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.).

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

☐ Anonymisation : Processus empêchant la ré-identification des individus.

☐ Appariement : Action de joindre des données complémentaires à des systèmes fils ou des jeux de données du SNDS.

☐ Chaînage des données : Procédé permettant de relier entre elles les données du SNDS correspondant à un même individu, 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 fort risque : Données dont la divulgation à une personne non autorisée a un impact élevé sur la vie privée.

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

☐ Environnement maîtrisé : Ensemble de ressources (matériel, logiciels, personnel, données) sur lesquelles le gestionnaire de système mettant à disposition des données du SNDS applique les exigences de sécurité du référentiel.

☐ Exportation de données : Alimentation d'un système fils à partir de données d'un système du SNDS élargi (SNDS central, système source ou un système fils).

☐ Gestionnaire du système : Responsable de l'ensemble des composants matériels et logiciels du système, ainsi que du choix et de l'exploitation des services de télécommunications mis en œuvre.

☐ Jeu de données : Tout ou partie du SNDS mis à disposition des utilisateurs du SNDS, dans le cadre d'une autorisation pour sa mise à disposition.

☐ 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, numéro de sécurité sociale NIR). Le procédé de pseudonymisation ne doit pas permettre l'identification individuelle directe de la personne associée à ce pseudonyme (l'identification indirecte reste toutefois possible). Ce processus est utilisé pour contribuer à l'anonymat et 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 : Personne, l'autorité publique, le service ou l'organisme qui détermine les finalités et moyens du traitement (définition Cnil).

☐ SNDS : Ensemble des données qui constituent le Système National des Données de Santé mentionné à l'Art.1461-1-I de la loi de modernisation du système de santé du 26 janvier 2016.

☐ SNDS élargi : Ensemble des systèmes réunissant, organisant et mettant à disposition tout ou partie des données du SNDS à des fins de recherche, d'étude ou d'évaluation. Le SNDS élargi comporte le SNDS central, des systèmes fils et des systèmes sources.

☐ SNDS central : Système réunissant, organisant et mettant à disposition le SNDS. Le gestionnaire du SNDS central est la CNAMTS.

☐ Sortie de données : Ensemble de données anonymes sorties par un utilisateur de l'environnement maîtrisé.

☐ Système fils : Système du SNDS élargi hébergeant ou mettant à disposition des données relatives au SNDS cédées par le SNDS central ou un système source ou un autre système fils.

☐ Système source : Système alimentant le SNDS central en données du SNDS.

☐ Tiers de confiance national : Dans le cadre du présent référentiel, organisme, distinct des gestionnaires des systèmes du SNDS élargi et des responsables de traitement, en mesure de faire le lien entre les identités des bénéficiaires et un ensemble de pseudonymes du SNDS élargi. Il assure la sécurité de ce dispositif.

☐ Utilisateur : Personne accédant à un ou plusieurs jeux de données du SNDS à des fins de recherche, d'étude ou d'évaluation. Un utilisateur ne peut pas réaliser d'exportations de données du SNDS.

3. **Exigences générales**

3.1. *Prérequis avant la mise à disposition de données du SNDS*

Chaque gestionnaire de systèmes du SNDS élargi doit apporter la preuve du respect des règles du présent référentiel, du règlement européen sur la protection des données personnelles, de la Politique générale de sécurité des systèmes d'information en santé (PGSSI-S), de la Politique de sécurité des systèmes d'information pour les ministères chargés des affaires sociales (PSSI MCAS), des règles applicables dans le cadre du Référentiel Général de Sécurité (RGS) et de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

En particulier, chaque système du SNDS élargi doit être homologué. A ce titre, le gestionnaire du système doit adopter la démarche suivante avant la mise en œuvre du système :

☐ Réalisation d'une analyse de risques ;

☐ Réalisation d'une étude d'impacts sur la vie privée (Privacy Impact Assessment) ;

☐ 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 considéré ;

☐ Suivi opérationnel de la sécurité du système d'information.

Le gestionnaire d'un système du SNDS élargi doit s'assurer que les utilisateurs sont autorisés par la CNIL ou par les autres conditions prévues par la loi à accéder aux données non anonymes du SNDS.

Les données non anonymes du SNDS ne peuvent être hébergées que sur des systèmes homologués vis-à-vis du présent référentiel.

Tout projet ayant un impact sur la sécurité d'un système du SNDS élargi (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 structurante 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*

L'hébergement des données du SNDS doit être réalisé sur le territoire européen. Il peut y avoir des exceptions pour un hébergement :

☐ Dans des pays n'appartenant pas à la communauté européenne mais reconnus par la Commission européenne comme « offrant un niveau de protection des données suffisant » ;

☐ Dans un autre pays, sous réserve d'un accord spécifique de la CNIL.

3.3. *Externalisation*

Dans le cas d'une externalisation de tout ou partie d'un système du SNDS élargi, les exigences suivantes sont applicables :

☐ Réalisation d'une analyse de risques préalable ;

☐ Encadrement contractuel de l'externalisation avec le tiers. En particulier, le tiers doit s'engager sur le respect des règles du présent Référentiel et des Référentiels associés (PGSSI-S, PSSI MCAS, etc.) sur le périmètre externalisé ;

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

3.4. *Classification des données*

La classification d'un jeu de données comme étant à faible risque doit être basée sur une analyse de risques. A défaut, le jeu de données doit être considéré comme étant à fort risque.

3.5. *Sensibilisation*

L'ensemble des gestionnaires des systèmes SNDS doit régulièrement mettre en place des actions de sensibilisation et de formation à destination des utilisateurs et des administrateurs (utilisation des données, conséquence en cas de mauvaise utilisation, bonnes pratiques, responsabilité, trace…).

3.6. *Archivage des données*

Les données archivées et les données sauvegardées sont soumises au présent référentiel.

Le gestionnaire du SNDS central doit s'assurer que les données archivées et sauvegardées de son 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.

3.7. *Environnements hors production*

Les données de production ne peuvent pas être utilisées sur des environnements hors production (recette, qualification, intégration, test, développement, pré-production…) sauf si le présent référentiel est appliqué sur lesdits environnements.

4. **Transfert des données**

4.1. *Constitution d'un système fils*

L'exportation de jeux de données non anonymes d'un système du SNDS élargi vers un autre système doit se faire uniquement si le destinataire respecte, avant la mise à disposition, le présent référentiel.

Cette exportation doit se faire dans le cadre d'une convention. Cette convention doit permettre au gestionnaire de système cédant les données de conserver des moyens de contrôle sur la bonne application du Référentiel de sécurité sur le système fils.

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

☐ Une procédure d'exportation des données précisant quelles sont les données autorisées à être cédées, 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 de transfert sécurisé de ces données ;

☐ Un engagement sur le respect des règles du présent référentiel et des référentiels associés (PGSSI-S, PSSI MCAS, etc.) par le gestionnaire de système recevant les données ;

☐ Une description des modalités d'audits et de contrôle de la sécurité du système recevant les données par le gestionnaire de système cédant les données.

Chaque gestionnaire de système du SNDS élargi doit construire et maintenir à jour un inventaire des jeux de données cédés et des systèmes associés.

4.2. *Gestion des exportations*

Seuls les jeux de données anonymes peuvent être exportés vers un système ne faisant pas partie du SNDS élargi.

Dès lors que des données non anonymes du SNDS élargi doivent transiter sur un réseau non maîtrisé, il convient de les protéger spécifiquement par un chiffrement adapté aux conclusions de l'analyse de risques.

Les administrateurs ayant des droits d'exportation de jeux de données doivent être en nombre limité, dûment identifiés et voir leurs habilitations contrôlées régulièrement.

5. **Accès aux données**

5.1. *Autorisation d'accès au SNDS*

Tout accès d'une personne à un jeu de données du SNDS ne doit être ouvert que pour une durée déterminée (cf § 9.2), 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 non anonymes 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 accès est réalisée par le gestionnaire du système concerné, après validation par l'autorité hiérarchique.

Les utilisateurs et les gestionnaires de systèmes doivent s'être engagés de manière opposable à respecter les conditions générales d'utilisation du SNDS élargi, à savoir :

- ☐ Engagement de confidentialité, notamment sur la non-diffusion des données non anonymes ;
- ☐ Absence d'actions visant la réidentification ;
- ☐ 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.

Des sanctions adéquates doivent être prévues dans le cas du non-respect de ces engagements, notamment la fermeture de l'accès aux données. Les utilisateurs et les gestionnaires de systèmes doivent être informés de ces sanctions.

5.2. *Modalités d'accès au SNDS*

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

Les données non anonymes du SNDS sont stockées dans un environnement maîtrisé. L'accès à cet environnement doit se faire à partir d'un poste respectant les exigences de la PSSI-MCAS. Cette exigence peut être imposée par convention si nécessaire.

Un utilisateur ne doit pas sortir de données non anonymes de l'environnement maîtrisé.

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

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

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

L'accès à des données à fort risque doit nécessiter 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, et une authentification forte, conformément aux exigences du palier 2 du Référentiel d'authentification de la PGSSI-S.

Les procédures d'accès à des données à faible risque doivent être adaptées au niveau de risque en termes d'impact sur la vie privée.

6. **Pseudonymisation**

6.1. *Pseudonymisation des données des systèmes du SNDS*

Les identifiants individuels des bénéficiaires stockés dans un des systèmes du SNDS élargi 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 le bénéficiaire concerné. 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 élargi, sauf autorisation de la CNIL.

Seul le tiers de confiance national peut posséder le dispositif de correspondance entre l'information sur l'identité des bénéficiaires et leurs pseudonymes dans le SNDS élargi. La possession de ce double niveau d'information doit être réalisée dans le cadre des attributions du tiers de confiance et celui-ci ne doit gérer aucune donnée du SNDS. Le tiers de confiance ne doit pas posséder les fonctions de pseudonymisation.

Seul le tiers de confiance national doit être en mesure de reconstituer les identités des bénéficiaires à partir d'un ensemble de pseudonymes. Cette reconstitution ne peut être effectuée que dans des cas particuliers autorisés par la loi (par exemple, dans le cas de l'urgence sanitaire) et doit être tracée.

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

6.2. *Alimentation du SNDS central*

Pour l'alimentation du SNDS central, un procédé sécurisé doit être utilisé pour pseudonymiser les données venant des bases sources. Ce procédé doit être basé 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 (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).

Dans le cadre de l'alimentation, la génération des pseudonymes du SNDS central s'opère sur deux niveaux minimum.

Les pseudonymes générés par le gestionnaire du système source cédant les données sont appelés pseudonymes de niveau 1. Ils sont générés au moyen d'une fonction respectant les principes énoncés ci-dessus et alimentent le SNDS central. A la réception de ces jeux de données, le gestionnaire du SNDS central génère de nouveaux pseudonymes (de niveau 2) au moyen d'une fonction respectant les principes énoncés ci-dessus.

Les fonctions de pseudonymisation utilisées successivement ne doivent pas avoir les mêmes secrets. Elles ne doivent pas non plus être dérivées les unes des autres, ni être dérivées de fonctions de pseudonymisation déjà existantes.

Tous les gestionnaires de systèmes sources alimentent le SNDS central avec un même pseudonyme de niveau 1.

6.3. *Exportation vers des systèmes fils*

Pour l'exportation de données provenant du système SNDS central, s'il n'y a pas de besoin de chaînage entre deux exportations, un numéro d'ordre éventuellement volatile peut être utilisé à la place d'une fonction de pseudonymisation.

6.4. *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. Les accès à ce secret doivent être basés 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 cédant les données est autorisé à le détenir.

Pour la pseudonymisation des bases alimentant le SNDS central, la génération de chaque secret doit être réalisée par deux organismes distincts.

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

6.5. *Renouvellement des pseudonymes*

En cas de soupçon ou de divulgation avérée du secret de pseudonymisation, l'ensemble des données potentiellement impactées doit faire l'objet d'une nouvelle pseudonymisation. Une nouvelle pseudonymisation de l'ensemble du système a également lieu régulièrement 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.

7. **Traçabilité**

7.1. *Paliers d'imputabilité*

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.

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 élargi doit disposer de dispositifs de journalisation permettant de conserver une trace des événements de sécurité sur leur périmètre, notamment sur :

- ☐ Les accès ;
- ☐ Les sorties ;
- ☐ Les exportations de données ;
- ☐ Les appariements ;
- ☐ Les opérations d'administration ;
- ☐ Les requêtes.

Le besoin en trace des requêtes pour les jeux de données à faible risque peut être arbitré au regard de l'analyse de risque. Cette trace doit permettre une imputation individuelle.

Cette journalisation doit s'inscrire dans le cadre d'une convention de preuve entre le gestionnaire de système et le gestionnaire du SNDS central ou le gestionnaire de système lui ayant cédé des données, indiquant en particulier les conditions dans lesquelles les traces sont collectées, traitées, conservées et restituées.

Les traces doivent être conservées 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 élargi est responsable de la surveillance des comportements anormaux pour le périmètre dont il a la responsabilité, notamment :

- ☐ Temps de réponse du système ;
- ☐ Elévation de privilèges ;
- ☐ Sortie de données non autorisées ;
- ☐ Accès non autorisé à une ressource du SNDS ;
- ☐ Modification anormale de données sources du SNDS ;
- ☐ Volume sorti trop important.

La fréquence d'analyse est définie au travers de l'analyse de risque. D'autres comportements peuvent être contrôlés au regard de l'analyse de risque.

7.4. *Horodatage des journaux*

Chaque gestionnaire de système du SNDS élargi 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 élargi doivent être cohérentes entre elles, c'est-à-dire que les décalages entre ces références doivent être connus et que toutes les informations temporelles indiquées au niveau des traces doivent pouvoir être traduites dans un référentiel de temps commun à l'ensemble du SNDS. Cela permet notamment d'être en mesure de faciliter la réconciliation de traces.

7.5. *Traitement des incidents*

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

8. **Contrôle**

8.1. *Audits*

Tous les systèmes du SNDS élargi doivent être périodiquement contrôlés (fonctionnellement et techniquement) dans le cadre d'audits internes (éventuellement délégués à des prestataires PASSI) et d'audits externes.

8.2. *Revue des habilitations*

Chaque gestionnaire de système donnant accès à des données du SNDS doit mettre en place une revue annuelle des habilitations.

9 Droits des personnes

9.1. *Droit d'accès*

Le gestionnaire du SNDS central doit définir et appliquer un processus d'exercice du droit d'accès (au sens de la LIL). Celui-ci doit notamment viser à s'assurer de l'identité de la personne exerçant le droit d'accès, de l'intégrité des informations communiquées et des modalités de communication permettant de garantir leur confidentialité.

9.2. *Droit d'opposition*

Le gestionnaire du SNDS central doit s'assurer qu'aucune donnée d'une personne ayant fait jouer son droit d'opposition n'est exportée vers un système fils généré à des fins de recherche, d'étude ou d'évaluation.

10. *Homologation*

Avant la mise en œuvre du système, celui-ci doit faire l'objet d'une homologation formelle par le responsable de traitement (*i.e* : acceptation des risques résiduels).