

Systeme national des donnees de sante

Référentiel de sécurité Guide d'accompagnement



SNDS
Système national des données de santé

1. Préambule

Qu'est-ce que le Système national des données de santé ?

L'article 193 de la loi de modernisation de notre système de santé prévoit l'ouverture de l'accès aux données de santé en mettant en place le Système national des données de santé : le SNDS.

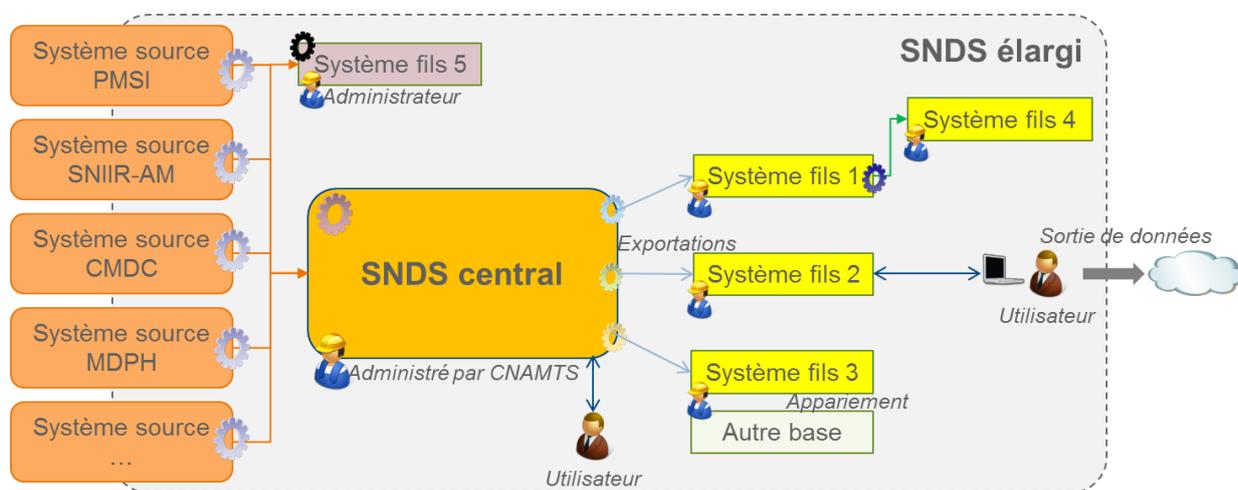
Le SNDS a pour vocation de centraliser l'ensemble des données suivantes :

- 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 médicales de décès ;
- les données médico-sociales du système d'information des Maisons départementales des personnes handicapées (MDPH) ;
- un échantillon représentatif des données de remboursement par bénéficiaire transmises par des organismes d'assurance maladie complémentaire.

La loi de modernisation de notre système de santé indique que le SNDS a pour finalités principales de contribuer :

- à l'information sur la santé ;
- à la mise en œuvre des politiques de santé ;
- à la connaissance des dépenses de santé ;
- à l'information des professionnels et des établissements sur leurs activités ;
- la recherche, aux études, à l'évaluation et à l'innovation dans les domaines de la santé
- à la surveillance, à la veille et à la sécurité sanitaire.

Le schéma ci-dessous illustre le fonctionnement du SNDS :



 Fonction de pseudonymisation

 Les fonctions de pseudonymisation sont réalisées avec des fonctions et des secrets différents pour chaque système fils

Légende :

- PMSI : Programme de médicalisation des systèmes d'information = données en provenance des hôpitaux.
- SNIIRAM : Système national d'information inter-régimes de l'Assurance maladie = données en provenance des Caisses primaires d'assurance maladie (CPAM), des caisses du Régime social des indépendants (RSI) et de la Mutualité sociale agricole (MSA).
- MDPH : Maisons départementales des personnes handicapées (système d'information en construction).
- CMDC : Causes Médicales de Décès = données de décès en provenance des médecins certificateurs.

Pourquoi un référentiel de sécurité est-il mis en œuvre ?

Le référentiel de sécurité du SNDS 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 ».

En effet, les données mises à disposition dans le SNDS sont sensibles. Bien qu'entreposées sur la base de pseudonymes, la combinaison de plusieurs variables peut déboucher sur l'identification des citoyens concernés, ce qui constitue un risque d'atteinte à la vie privée. Le référentiel a été élaboré sur la base d'une analyse de risques rigoureuse de façon à mettre en place les mesures de sécurité adéquates.

Pourquoi ce guide pédagogique est-il diffusé ?

Le présent guide pédagogique a pour but d'accompagner les responsables de la sécurité des systèmes d'information (RSSI) dans leurs démarches de conformité au référentiel de sécurité. Ce guide propose une vision pratique et des références à des documents/méthodes déjà existants afin de guider les utilisateurs au plus proche du terrain. Ce guide pédagogique a notamment vocation à apporter des éclairages sur les points les plus complexes.

Quels sont les fondamentaux juridiques ?

1. La loi Informatique et Libertés n°78-17 du 6 janvier 1978 relative à la protection des données personnelles (ci-après, la « loi Informatique et Libertés »), notamment son article 1er affirmant que « l'informatique (...) ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ».

Les données de santé étant considérées comme « sensibles », le SNDS est également soumis aux dispositions spécifiques de la loi informatique et libertés (chapitre IX).

2. Le règlement européen sur la protection des données à caractère personnel du 8 avril 2016 s'appliquera pleinement à compter de mai 2018.
3. Les dispositions régissant le SNDS ont été intégrées au Code de la santé publique (articles L. 1460-1 et suivants).

Comment utiliser le guide pédagogique ?

Chaque section du référentiel est détaillée sous la forme d'une fiche contenant :

- L'exigence du référentiel de sécurité
- L'objectif principal de l'exigence
- Une rubrique « À savoir » qui rappelle les notions clés à maîtriser pour appliquer l'exigence
- Une rubrique « À faire » qui indique les actions à mener dans le temps et qui est découpée selon trois items : *Qui ? Quoi ?* et *Quand ?*

1. Titre

Exigence 4.1 : Titre de l'exigence

Section du référentiel :

Détail de l'exigence

OBJECTIF

Détail de l'objectif

À SAVOIR

- Détail des notions clés et des documentations auxquelles l'utilisateur peut se référer

À FAIRE

 **Qui ?** L'acteur correspondant

 **Quand ?** La phase correspondante

 **Que faire ?**

- ▶ Les différentes actions à mener pour être en conformité avec l'exigence

 **Point de vigilance**

 **Bonne pratique**

Portée du document : l'objectif de ce document est d'illustrer le référentiel de sécurité et d'accompagner les RSSI du SNDS pour faciliter la mise en œuvre des exigences. La conformité avec le référentiel reste de la responsabilité de chaque gestionnaire.

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 au I de l'Art.1461-1 du code de la santé publique.
- **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 - Prérequis

Exigence 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 à caractère personnel, 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. À 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.

OBJECTIF

Le référentiel de sécurité est un socle minimum et générique. Chaque gestionnaire doit **réaliser une analyse de risques afin d'identifier les risques qui lui sont propres**, de mettre en place les mesures complémentaires nécessaires et de piloter sa sécurité dans le temps.

À SAVOIR

- Le gestionnaire de système doit s'assurer d'être en mesure de justifier de la conformité du système à travers le temps. Il devra donc pouvoir présenter les preuves de sa conformité à tout instant.
- Selon la CNIL, le terme « vie privée » est employé comme raccourci pour évoquer l'ensemble des droits et libertés fondamentaux : « vie privée, identité humaine, droits de l'homme et libertés individuelles ou publiques ». L'acronyme « PIA » est utilisé pour désigner indifféremment Privacy Impact Assessment, étude d'impact sur la vie privée (EIVP), Data Protection Impact Assessment (DPIA) et étude d'impact sur la protection des données. »
- La CNIL propose un tableau générique des grands types d'impacts sur la vie privée de défaillances de la sécurité de traitements informatiques sensibles. Ce tableau peut servir de base de réflexion pour réaliser un PIA :

Niveaux	Descriptions génériques des impacts (directs et indirects)
Négligeable	Les personnes concernées ne seront pas impactées ou pourraient connaître quelques désagréments, qu'elles surmonteront sans difficulté
Limitée	Les personnes concernées pourraient connaître des désagréments significatifs, qu'elles pourront surmonter malgré quelques difficultés
Importante	Les personnes concernées pourraient connaître des conséquences significatives, qu'elles devraient pouvoir surmonter, mais avec des difficultés réelles et significatives
Maximale	Les personnes concernées pourraient connaître des conséquences significatives, voire irrémédiables, qu'elles pourraient ne pas surmonter

La CNIL met également à disposition un outillage détaillé sur le sujet :

<https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-2-Outillage.pdf>

À FAIRE



Qui ?

Chaque gestionnaire de système



Quand ?

Avant la mise en œuvre du système



Quoi ?

Les principes de base sont les suivants

- faire une analyse de risques
- mettre en œuvre les mesures correspondantes
- revoir l'analyse de risques en cas de changement majeur



La bonne pratique :

La méthode d'amélioration continue (Roue de Deming) qui présente les quatre phases à enchaîner successivement : planifier, réaliser, vérifier/contrôler, agir/améliorer, constitue une bonne approche.

PLANIFIER :

Les méthodes suivantes sont données à titre d'exemple, et peuvent faire l'objet d'une adaptation/simplification au vu du contexte opérationnel des différents organismes.

- ▶ Réaliser une analyse de risques. L'Agence nationale de la sécurité des systèmes d'information (ANSSI) propose la méthode d'analyse de risques EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) : <http://www.ssi.gouv.fr/uploads/2011/10/EBIOS-1-GuideMethodologique-2010-01-25.pdf>. Il existe également d'autres méthodes : par exemple la méthode CRAMM, la méthode OCTAVE, le processus proposé dans l'ISO 27005, etc.
- ▶ Réaliser un PIA : soit directement intégré dans l'analyse de risques, soit via l'application d'une méthodologie spécifique (cf. CNIL).

REALISER :

- ▶ Mettre en œuvre le plan d'action de couverture des risques.

VERIFIER / CONTROLER :

- ▶ Réaliser les tests et recettes ;
- ▶ Réaliser l'homologation (cf. Chapitre 20 qui réfère à l'exigence sur l'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)* » ;
- ▶ Demander la transmission du dossier de demande d'autorisation et la délibération de la CNIL pour donner l'accès aux données.

AGIR / AMELIORER :

- ▶ Définir les mesures d'amélioration continue ;
- ▶ Mettre en œuvre un suivi opérationnel et mettre à jour l'analyse de risques et le plan d'actions associé en cas de modification du contexte.

Exigence générales - Territorialité

Exigence 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 :

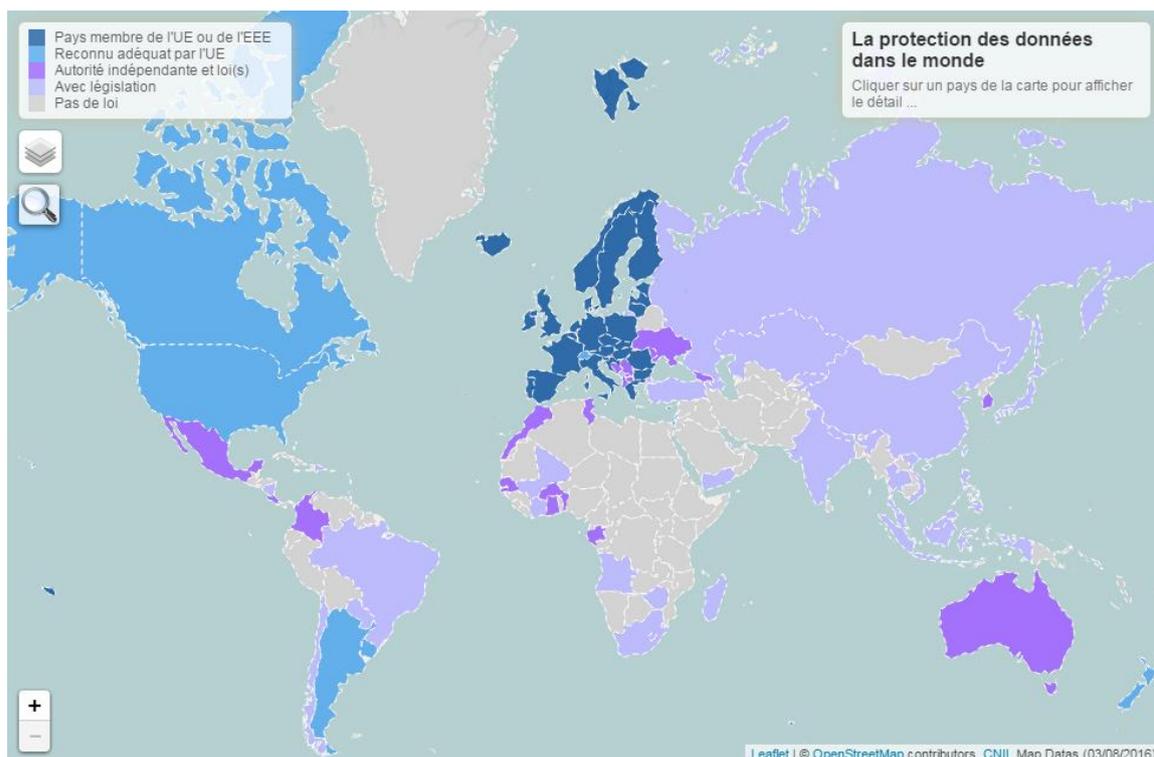
- Dans des pays n'appartenant pas à la communauté européenne mais reconnus par la Commission européenne comme « offrant un niveau de protection des données suffisant ».
- Dans un autre pays, sous réserve d'un accord spécifique de la CNIL.

OBJECTIF

Le niveau de protection des données est variable selon le pays destinataire. En premier lieu, il convient de s'assurer que le niveau de protection des données du pays hôte est considéré comme suffisant au regard des exigences de la CNIL en matière de protection des données à caractère personnel. De plus, ce niveau doit également être conforme avec les exigences du règlement européen sur la protection des données à caractère personnel.

À SAVOIR

- Cette exigence est applicable à tout système contenant des données du SNDS, à savoir l'ensemble des systèmes du SNDS élargi.
- Tous les pays ne disposent pas d'une législation spécifique ou d'une autorité de protection des données personnelles conforme aux exigences du règlement européen sur la protection des données à caractère personnel. Le lieu d'hébergement des données doit proposer un niveau de sécurité suffisamment élevé afin qu'il soit conforme au niveau de sécurité requis par l'Union Européenne. La CNIL fournit la carte du monde des niveaux de sécurité des différents pays dans le monde : <https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde>



Carte à la date du 03/08/2016

Les pays reconnus adéquats par l'Union-Européenne, à la date du 03 août 2016, sont les suivants :

- La Suisse
 - Le Canada
 - Andorre
 - L'Argentine
 - Guernesey
 - L'île de Man
 - Les îles Féroé
 - Jersey
 - Israël
 - L'Uruguay
 - Les Etats-Unis
-
- Néanmoins, la CNIL peut émettre un avis divergent de celui de l'Union européenne, Le G29 a notamment exprimé diverses réserves sur l'adéquation du Privacy Shield : <https://www.cnil.fr/fr/declaration-du-g29-relative-la-decision-de-la-commission-europeenne-concernant-le-privacy-shield>

 - **À noter** : le stockage de données ainsi que leur restitution sur un territoire étranger sont concernés (*ex : des données stockées en France mais affichées au Chili nécessitent des modalités de transfert*). Tout pays reconnu comme « *non adéquat* » requiert une autorisation de transfert de la CNIL et la mise en place de mesures de sécurité spécifiques au regard de l'analyse de risques.

 - **La CNIL détaille sur son site les formalités nécessaires au transfert des données hors Union-Européenne** : <https://www.cnil.fr/fr/transferts-hors-ue-quelles-formalites>

 - **La CNIL propose également un Guide des transferts de données à caractère personnel hors Union européenne** : <https://www.cnil.fr/sites/default/files/typo/document/GUIDE-transferts-integral.pdf>

À FAIRE



Qui ? Le responsable du traitement.



Quand ? Avant le transfert des données (valable uniquement pour les pays non adéquats).



Quoi ?

- Vérifier la localisation des données et la localisation de leur restitution.

- Obtenir une autorisation de transfert de la CNIL si le pays hôte n'est pas reconnu comme étant « *adéquat* » et mettre en place le niveau de sécurité attendu.

Exigences générales - Externalisation

Exigence 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.

OBJECTIF

L'**externalisation** correspond au transfert d'activités d'un organisme vers un prestataire externe. L'externalisation des données (parfois chez plusieurs prestataires en chaîne) peut provoquer des failles dans la protection de la confidentialité des données. Il est nécessaire de s'assurer du maintien de la sécurité des données et d'être en mesure de le contrôler.

À SAVOIR

- La CNIL fournit des modèles de clauses à intégrer dans les contrats avec les sous-traitants : <https://www.cnil.fr/fr/sous-traitance-modeles-de-clauses-de-confidentialite>



Point de vigilance : plus il y a de niveaux de sous-traitance, plus la vigilance doit être renforcée sur :

- le contrôle de l'application du référentiel ;
- la création d'un inventaire ;
- la notification en cas d'appel à un autre sous-traitant ;
- le renforcement du contrat en conséquence / convention en annexe au contrat.



La bonne pratique : mettre en place une convention d'hébergement.

À FAIRE



Qui ?

Chaque gestionnaire de système et chaque tiers



Quand ? Avant l'externalisation



Quoi ?

- **Analyse de risques préalable** : le gestionnaire du système doit *réaliser* ou *mettre à jour* une analyse de risques mettant en exergue les risques liés à l'externalisation.
- **Encadrement contractuel de l'externalisation d'un tiers** : le tiers doit s'engager à respecter les règles du référentiel de sécurité et des référentiels associés sur le périmètre externalisé.
- **Définir des modalités d'audits et de contrôle de sécurité par chaque gestionnaire** : chaque gestionnaire du système doit s'assurer du respect des engagements du tiers.

Exigences générales - Classification des données

Exigence 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.

OBJECTIF

Les exigences de traçabilité et d'authentification du référentiel peuvent être modérées pour des données identifiées comme ayant un impact limité sur la vie privée en cas de divulgation à une personne non autorisée.

À SAVOIR

- La classification des données doit résulter de l'analyse d'impact sur la vie privée. Les jeux de données les plus susceptibles de nuire aux individus, s'ils étaient divulgués, doivent faire l'objet d'une protection accrue. Un groupe de travail a été mobilisé sur l'analyse des niveaux de risque : un rapport issu de ces travaux sera prochainement diffusé. Il contiendra des exemples d'analyse sur quelques jeux de données du SNDS et proposera quelques pistes de réflexion. Une synthèse des axes les plus saillants est proposée ci-dessous.
- Les bases brutes du SNDS sont considérées, par défaut, comme étant à fort risque.



La bonne pratique

Les travaux menés par le groupe de travail précité identifient plusieurs axes à analyser pour aider à la classification des risques :

- **Quelles informations le jeu de données permet-il de connaître**, notamment **dispose-t-on d'informations directes ou indirectes** (via les médicaments consommés par exemple) **sur les pathologies des individus ?**

Peut-on dévoiler une pathologie discriminante (du fait de sa gravité ou de considérations morales) ?

Un jeu de données ne contenant par exemple que des informations sur les dépenses de santé (et donc ne permettant pas de dévoiler une pathologie précise) sera a priori moins sensible qu'un jeu de données contenant des diagnostics ou des codes ALD¹ car, en cas de divulgation, l'impact sur la vie privée est considéré comme moindre.

- **Le jeu de données est-il échantillonné et si oui à quel taux ?** L'échantillonnage affaiblit les risques d'impact sur la vie privée pour plusieurs raisons :
 - il réduit la probabilité de réussite d'attaques visant un individu en particulier (car il est fortement probable qu'il ne soit pas dans le jeu de données),
 - il limite les risques d'inférence car les estimations qui en seront issues seront moins précises.
- **Le risque d'une réidentification publique est-il élevé ?**

¹ Affection de Longue Durée : il s'agit d'affections dont la gravité et/ou le caractère chronique nécessitent un traitement prolongé et une thérapeutique particulièrement coûteuse, et pour lesquelles le ticket modérateur est supprimé.

Le risque de réidentification doit normalement se calculer à partir de l'ensemble des informations susceptibles d'être connues des potentiels « attaquants » (personnes malveillantes). Cet ensemble est potentiellement illimité si l'« attaquant » est un proche de la « victime » et dans ce cas, dès que le jeu de données contient un nombre important d'informations sur un même individu, le risque de réidentification est maximal, il n'est donc pas possible de couvrir ce risque autrement qu'en limitant et sensibilisant les utilisateurs.

En revanche, il paraît pertinent de calculer un risque de réidentification publique c'est-à-dire le nombre de personnes que l'on peut réidentifier avec une probabilité forte à partir d'informations relativement facilement accessibles, à savoir l'âge, le sexe, le lieu de résidence et le fait d'avoir été hospitalisé. En particulier, les trois premières informations sont disponibles dans les listes électorales, communicables à tout électeur. Le croisement de ces données avec celles contenues dans le SNDS pourrait, dans certains cas, déboucher sur la réidentification d'un groupe d'individus. A minima, il convient donc de considérer que ce risque de réidentification par croisement de ces trois informations doit être pratiquement nul pour considérer que le risque est faible.

À FAIRE



Qui ? Le responsable de traitement et le gestionnaire de système



Quand ? Avant toute sortie de données de l'environnement maîtrisé



Quoi ? Analyse des risques par un questionnaire systématique

Exigences générales - Sensibilisation

Exigence 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...).

OBJECTIF

Les fuites de données sont souvent dues à une action humaine (erreur ou acte intentionnel). Il faut ainsi mettre en place une sensibilisation pour limiter les incidents de sécurité. Par ailleurs, les utilisateurs doivent être informés de la traçabilité de toutes leurs actions ainsi que des sanctions mises en place en cas de non-respect des consignes.

À SAVOIR

- La garantie de traçabilité est un enjeu clé pour la sécurité des données : en effet, la capacité à identifier les auteurs de l'ensemble des actions pourra limiter les velléités malveillantes.
- Il est important de souligner auprès des utilisateurs et des administrateurs l'existence d'une traçabilité fine.
- Les sanctions et échelles de sanctions doivent être établies préalablement et communiquées.
- Les actions de sensibilisation doivent être l'occasion de rappeler les grands principes juridiques s'appliquant aux traitements de données de santé (données sensibles, sanctions pénales, mobilisation des données strictement nécessaires, etc...)

À FAIRE



Qui ? Chaque gestionnaire de système



Quand ? Avant l'ouverture du système, puis périodiquement (au minimum une fois par an).



Quoi ?

- Mettre en place des **actions de sensibilisation**.
- Mettre en place des **formations à destination des utilisateurs et des administrateurs**.
- **Communiquer** sur le niveau de traçabilité et les sanctions encourues dès l'ouverture de tout système.
- Sanctionner tout dérapage **dès sa constatation**.

Exigences générales - Archivage et sauvegarde des données

Exigence 3.6 : archivage et sauvegarde 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.

OBJECTIF

Afin d'assurer une conformité à la durée de conservation des données (selon la loi informatique et libertés, article 6.5 : « elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées. »), les gestionnaires de système doivent être en mesure de restituer l'ensemble des données sauvegardées et archivées. Par ailleurs, de nombreuses actions malveillantes sont réalisées sur les données hors ligne, il convient donc de s'assurer qu'elles bénéficient d'un niveau de sécurité optimal.

À SAVOIR

- D'après l'article Art. L. 1461-1.-I du code de la santé publique, « Les données individuelles du système national des données de santé sont conservées pour une durée maximale de vingt ans, sans préjudice de l'application du [deuxième alinéa de l'article 36 de la loi n° 78-17 du 6 janvier 1978](#) relative à l'informatique, aux fichiers et aux libertés. »
- Afin de s'assurer de la sécurité des données, les gestionnaires doivent appliquer le référentiel sur leurs sauvegardes et archives : traçabilité, authentification, intégrité des données...
- Une sauvegarde permet de récupérer les données en cas de perte ou d'endommagement. La sauvegarde peut s'appliquer sur des données activées (modifiées quotidiennement) ou inactives (données figées). Elle n'a pas vocation à être conservée dans le temps
- Une archive a pour finalité de préserver des données anciennes - ou dites dormantes – sur une longue durée.
- Le gestionnaire du SNDS central doit s'assurer que les données archivées et sauvegardées de son périmètre restent lisibles pendant une durée légale de conservation.
- Dans le cas d'une externalisation des sauvegardes et des archives, consulter la partie *Externalisation* (3.3) du Référentiel de sécurité du SNDS ainsi que la partie *Externalisation* du présent Guide pédagogique p.11.

À FAIRE

Quatre actions distinctes sont nécessaires. Quatre niveaux d'action sont donc présentés :

Niveau 1 : protection des sauvegardes :



Qui ? Chaque gestionnaire de système



Quand ? Avant la mise en œuvre du système



Quoi ? Mettre en œuvre le référentiel sur les sauvegardes.

Niveau 2 : protection des archives :



Qui ? Chaque gestionnaire de système



Quand ? Avant la mise en œuvre du système



Quoi ? Mettre en œuvre le référentiel sur les archives.

Niveau 3 et 4 : lisibilité des sauvegardes et des archives



Qui ? Le gestionnaire du SNDS central



Quand ? Périodiquement (au changement de technologie notamment).



Quoi ?

- Prévoir, à chaque migration de technologie, une récupération des données sur les technologies précédentes.
- Prévoir une montée de version à chaque évolution logicielle. Par exemple, si la mise à jour d'un logiciel n'est pas réalisée à chaque nouvelle version, le gestionnaire du système ne sera pas en mesure de récupérer les données de manière exploitable entre la version 1.1 et la version 1.5.



La bonne pratique : chaque gestionnaire de système fils devrait s'assurer de la lisibilité des données archivées et sauvegardées afin de garantir une meilleure protection des sauvegardes et des archives.

Exigences générales - Environnements hors production

Exigence 3.7 : Environnement de 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.

OBJECTIF

Les environnements hors production sont des zones à risques concernant le vol de données sensibles. La sécurisation des environnements hors production est donc primordiale.

À SAVOIR

S'il est possible de flouter des données de production ou d'utiliser des données similaires non-identifiantes, sans impacter la qualité des tests, ces solutions doivent être privilégiées. L'utilisation de données de production ne doit se faire qu'en dernier recours. Dans ce cas, des données de production ne peuvent être utilisées sur des environnements hors production que si le référentiel de sécurité est appliqué sur lesdits environnements.

À FAIRE



Qui ? Chaque Gestionnaire de système



Quand ? Avant l'exploitation des environnements hors production.



Quoi ?

- Chaque gestionnaire de système doit s'assurer que les environnements hors production soient conformes aux exigences du référentiel de sécurité (développement, qualification, intégration, test, recette, pré-production...).



Bonne pratique impérative : supprimer obligatoirement les données une fois la mise en place du système assurée.

4. Transfert des données - Constitution d'un système fils

Exigence 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

OBJECTIF

La création d'un système fils peut engendrer certaines failles de sécurité sur les données. Le gestionnaire de système doit s'assurer que le système fils respecte bien les exigences du référentiel de sécurité et de la sécurité des données lors de leur communication.

À SAVOIR

- L'exportation de jeux de données non anonymes d'un système du SNDS élargi vers un autre système ne doit se faire que si le destinataire **respecte le référentiel de sécurité**.
- L'exportation doit se faire dans le cadre d'une **convention**.
- Elle doit permettre au gestionnaire de système de **conserver des moyens de contrôle** sur la bonne application du référentiel de sécurité.
- La demande d'autorisation d'exportation est faite auprès d'une entité unique d'enregistrement hébergée par l'Institut national des données de santé -INDS- (pour plus de précisions, consulter le dossier relatif aux circuits des demandes qui transitent via l'INDS).



Bonne pratique : toute nouvelle cession de données nécessite l'information systématique du gestionnaire du système source. Ceci doit être convenu par écrit dans la convention de cession initiale pour **accord entre les différentes parties**.

À FAIRE



Qui ? Chaque responsable de traitement de système fils, le gestionnaire de système cédant les données, le gestionnaire de système fils.



Quand ? Avant la mise en œuvre du système.



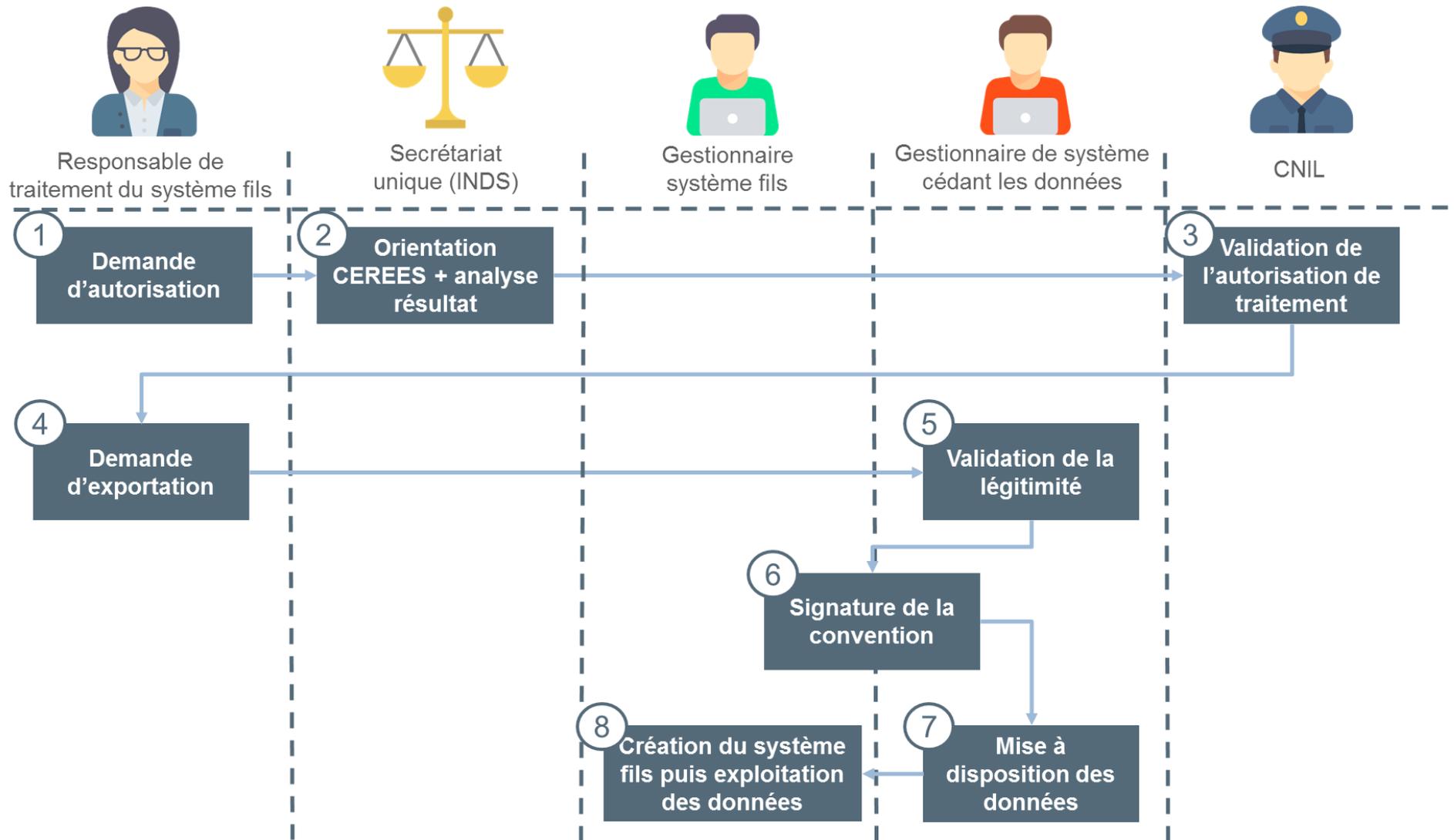
Quoi ?

Pour disposer d'un accès aux données du SNDS, il est nécessaire de disposer d'une autorisation délivrée par la CNIL.

Le processus de constitution d'un système fils composé exclusivement de données du SNDS est le suivant² :

1. Le responsable de traitement du système fils envoie sa demande d'autorisation d'accès aux données (ou à une partie) du SNDS directement à l'INDS.
2. L'INDS traite la demande puis l'envoie au Comité d'expertise pour les recherches, les études et les évaluations dans le domaine de la santé (CEREES) Le secrétariat recueille le résultat de l'examen du CEREES et informe le demandeur.
3. Si le résultat est positif, la demande d'autorisation de traitement est ensuite envoyée par l'INDS à la CNIL pour validation.
4. Lorsque l'autorisation est validée par la CNIL, le responsable de traitement du système fils reçoit une validation pour sa demande d'exportation.
5. Le responsable de traitement du système fils - s'appuyant sur la bonne application du Référentiel de sécurité du SNDS - soumet sa requête au gestionnaire de système cédant les données pour une dernière validation de légitimité.
6. Une convention, incluant les modalités de contrôle du système fils, est signée entre le gestionnaire de système cédant les données et le gestionnaire de système-fils.
7. Le gestionnaire de données de système cédant les données met alors les données à disposition du gestionnaire du système fils selon les modalités convenues dans la convention.
8. Le gestionnaire du système fils peut créer le système fils et exploiter les données.

² En cas de constitution d'un système fils appariant des données du SNDS avec des données impliquant la personne humaine, le dossier doit être examiné par un Comité de protection des personnes.



Transfert des données - Gestion des exportations

Exigence 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.

OBJECTIF

La ré-identification des personnes au travers des données du SNDS constitue l'un des principaux risques.

- ➔ Le référentiel de sécurité doit ainsi être appliqué tant que l'on n'a pas la certitude que les données sont anonymes (et donc qu'une personne ne peut pas être ré-identifiée).
- ➔ Afin de réduire le risque de malveillance humaine, il convient de limiter le nombre d'administrateurs de ces données.
- ➔ L'interception de données sur les réseaux étant fréquente, il convient de protéger les données afin que celles-ci ne soient pas exploitables le cas échéant.

À SAVOIR

- Les utilisateurs ne doivent pas pouvoir exporter des données, seuls des administrateurs habilités doivent y être autorisés.
- Les administrateurs qui exportent les données doivent être identifiés au préalable et contrôlés de manière régulière.
- Les administrateurs doivent impérativement être informés du fait que toutes leurs actions, en particulier les exportations de données, sont suivies et tracées. Tout non-respect aux exigences de sécurité de données sera immédiatement sanctionné.
- Il y a quatre points clés :
 - ▶ Il est nécessaire **d'identifier les flux de données et de les protéger** (par exemple par un chiffrement adapté à l'analyse de risques) dès la mise en œuvre du système.
 - ▶ Les administrateurs doivent donner aux utilisateurs les **moyens de protéger les données non anonymes**.
 - ▶ Il existe de nombreuses **méthodes de chiffrement** : celles-ci évoluent en permanence au cours du temps et sont régulièrement cassées. Chaque gestionnaire doit donc s'assurer d'utiliser une méthodologie de chiffrement robuste et adaptée aux risques encourus.

À FAIRE



Qui ? L'utilisateur et chaque gestionnaire de système



Quand ? Dès la mise en œuvre du système.



Quoi ?

- Protéger spécifiquement les données non anonymes du SNDS élargi qui doivent transiter sur un réseau non maîtrisé par un chiffrement adapté aux conclusions de l'analyse de risques.
- Communiquer sur les conséquences du non-respect des exigences de sécurité pour l'exportation des données et des sanctions prévues dans ces cas de figure.

5. Accès aux données - Autorisation d'accès au SNDS

Exigence 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 § 8.2), 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.

OBJECTIF

L'objectif est triple :

- Engager formellement les utilisateurs.
- Les informer de la traçabilité de leurs actions.
- Souligner les sanctions encourues.

À SAVOIR

- Tout accès d'une personne à un jeu de données du SNDS ne doit être ouvert que pour une durée déterminée par la CNIL ou toute autre condition prévue par la loi.
- La rupture du secret professionnel et/ou la divulgation d'information non anonymes expose l'utilisateur à des sanctions (cf. article 226.13 du code pénal : 1 an d'emprisonnement et 15000€ d'amende).
- Les Conditions générales d'utilisation (CGU) permettent de fournir aux utilisateurs certaines informations. Sur le plan juridique, des CGU acceptées formellement par les utilisateurs permettent d'éviter un grand nombre d'actions contentieuses. Les CGU permettent notamment de limiter la responsabilité, prévoir quelle juridiction sera compétente en cas de litiges ou encore informer des sanctions mise en place selon le type de délit.
 - ▶ En particulier, les CGU pourront être utilisées pour rappeler :
 - ▶ les **finalités d'utilisation** du SNDS,
 - ▶ la nécessité de ne **sortir que des données anonymes**,
 - ▶ l'**enjeu de traçabilité** de l'ensemble des actions réalisées,
 - ▶ les **sanctions** en cas de non-respect de ces conditions d'utilisation.

À FAIRE



Qui ? L'utilisateur et chaque gestionnaire de système



Quand ? Avant l'accès aux données.



Quoi ?

- Vérifier que les conditions d'accès sont remplies.
- Mettre en place une procédure formelle d'acceptation des CGU par les utilisateurs.
- Communiquer sur les conséquences du non-respect de ces CGU et des sanctions prévues dans ces cas de figure.

Accès aux données - Modalités d'accès au SNDS

Exigence 5.2 : Modalité 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 Politique de sécurité des systèmes d'information des ministères chargés des affaires sociales (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.

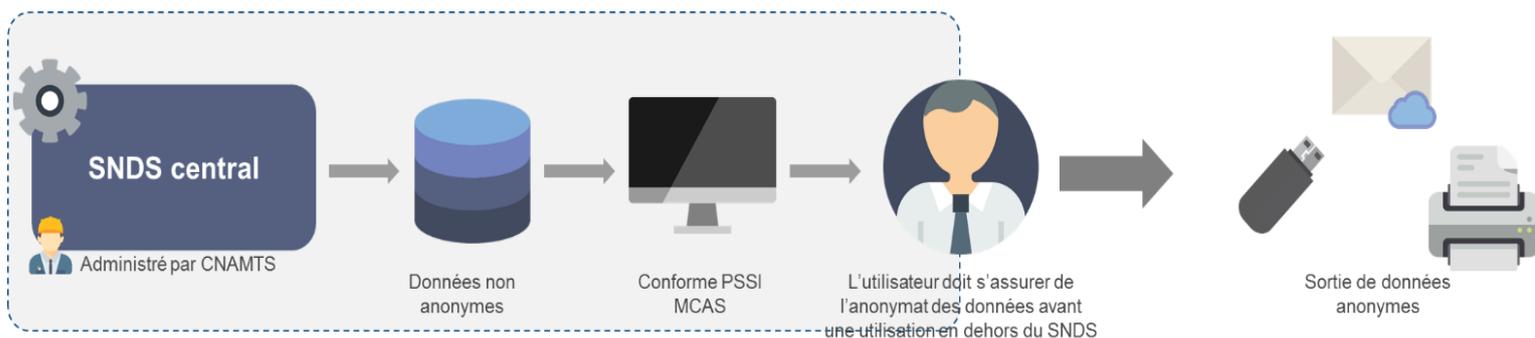
OBJECTIF

Il s'agit de garantir que les données du SNDS demeurent dans un environnement maîtrisé (i.e. environnement sur lequel on applique le présent référentiel et pour lequel on maîtrise les sorties). Cette maîtrise passe notamment par l'application de la PSSI MCAS sur les postes de travail accédant aux données du SNDS.

Seules des données anonymes, ne représentant ainsi pas de risque d'atteinte à la vie privée, peuvent être sorties du système

À SAVOIR

- La sortie de données anonymes par un utilisateur implique la mise en place de mesure de sensibilisation (pour que l'utilisateur ait les moyens de juger de la nature anonyme des données) et de contrôle.
- Les besoins de disponibilité sont propres à chaque système. Il conviendra à chaque gestionnaire de système de définir formellement ces besoins et de mettre en œuvre les mesures associées.
- Afin de garantir l'intégrité des données, les utilisateurs ne sont pas autorisés à modifier les données sur le SNDS central. Cette mesure est obligatoire pour le SNDS Central. Les gestionnaires de systèmes fils, quant à eux, peuvent déterminer si ladite mesure est pertinente au regard de l'analyse des risques sur leur système.
- Les données non anonymes du SNDS doivent être stockées dans un environnement maîtrisé et soumis au référentiel de sécurité.



■ Les exigences de la PSSI MCAS sont les suivantes :

- ▶ Gestion des mots de passe
- ▶ Sécurisation des flux d'administration
- ▶ Protection contre les codes malveillants
- ▶ Mise à jour de la base de signature
- ▶ Configuration du navigateur internet
- ▶ Maîtrise des matériels
- ▶ Rappel des mesures de protection contre le vol
- ▶ Déclarer les pertes et vols
- ▶ Réaffectation de matériels informatiques
- ▶ Déclaration des équipements nomades aptes à traiter les informations sensibles
- ▶ Accès à distance au système d'informations de l'organisme
- ▶ Système d'exploitation
- ▶ Fourniture et gestion des postes des travail
- ▶ Formalisation de la configuration des postes de travail
- ▶ Verrouillage de l'unité centrale des postes fixes
- ▶ Verrouillage des postes portables
- ▶ Réaffectation du poste de travail
- ▶ Privilèges des utilisateurs sur les postes de travail
- ▶ Utilisation des privilèges d'accès administrateurs
- ▶ Gestion du compte administrateur local
- ▶ Stockage des informations
- ▶ Sauvegarde : synchronisation des données locales
- ▶ Partage de fichiers
- ▶ Suppression des données sur les postes partagés
- ▶ Chiffrement des données sensibles
- ▶ Fourniture de supports de stockage amovible
- ▶ Accès à distance aux SI de l'entité
- ▶ Pare-feu local
- ▶ Stockage local d'information sur les postes nomades
- ▶ Filtre de confidentialité
- ▶ Configuration des interfaces de connexion sans fil
- ▶ Désactivation des interfaces de connexion sans fil
- ▶ Durcissement des imprimantes et copieurs multifonctions
- ▶ Sécurisation de la fonction de numérisation
- ▶ Sécuriser la configuration des autocommutateurs
- ▶ Codes d'accès téléphoniques
- ▶ Limiter l'utilisation du DECT³
- ▶ Utiliser les outils de vérification automatique de la conformité

Source : PSSI MCAS.

→ Le détail des ces exigences est fourni en annexe du présent document.

À FAIRE



Qui ?

Chaque gestionnaire système et les utilisateurs



Quand ?

Avant la mise en œuvre du système.



Quoi ?

- L'accès aux données non anonymes doit se faire depuis un poste qui respecte les exigences de la PSSI-MCAS, condition qui peut être imposée par convention entre le gestionnaire de système cédant les données et le gestionnaire de système-fils.
- Le gestionnaire de système et le gestionnaire du poste sont parfois différents. Le gestionnaire du système doit donc imposer des règles de sécurité au poste à travers une convention signée par les deux parties (ex : Dans le cas d'un organisme accédant (ex : une agence sanitaire) qui délègue la gestion de ses postes à un autre organisme (ex : un CHU), ce dernier ne signera pas de convention avec le gestionnaire du SNDS central. Le service accédant (agence sanitaire) doit alors signer une convention avec l'entité prestataire (CHU), afin de s'assurer que ses postes respectent également la PSSI-MCAS.).

³ DECT (Digital Enhanced Cordless Telecommunications) : norme de téléphonie sans-fil numérique.

Accès aux données - Paliers d'identification et d'authentification

Exigence 5.3 : paliers d'identification et d'authentification

Section du référentiel : Accès aux données

L'accès à des données à fort risque nécessite 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.

OBJECTIF

Il s'agit de mettre en place les moyens nécessaires permettant de s'assurer de l'identité des personnes qui se connectent au système.

À SAVOIR

- Des **paliers d'identification et d'authentification** doivent être mis en place pour les données à fort risque.
- La PGSSI-S indique que « deux types d'identifiants peuvent être distingués selon les périmètres d'action des autorités d'enregistrement » :
 - **un identifiant de portée nationale (ou identifiant « public »)** : c'est un identifiant attribué à la suite de l'enregistrement dans un référentiel d'identité national par une autorité d'enregistrement dûment habilitée (par exemple le numéro du répertoire partagé des professionnels de santé –RPPS-).
 - **un identifiant de portée locale (ou identifiant « privé »)** : c'est un identifiant attribué à la suite de l'enregistrement par une autorité d'enregistrement pour un référentiel autre qu'un référentiel d'identité national tel que défini au 4.1 du référentiel d'identification de la PGSSI-S. Son utilisation est limitée aux finalités du référentiel (par exemple pour la mise en place au sein d'un établissement de santé d'un registre permettant d'attribuer un numéro de matricule à chaque salarié, avec pour finalité d'assurer la gestion des ressources humaines). Un identifiant « privé » doit être unique au sein d'une base locale mais peut être utilisé dans plusieurs bases locales différentes.

Le développement rapide de l'usage des technologies de l'information dans le domaine de la santé s'accompagne d'un accroissement des menaces et des risques d'atteinte aux informations conservées sous forme électronique, et plus généralement aux processus de santé s'appuyant sur les systèmes d'information de santé. L'État a élaboré une Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S), en concertation avec l'ensemble des acteurs partie prenante, afin de fixer le cadre de la sécurisation des SI de Santé. Le PGSSI-S propose une synthèse des exigences des paliers 1 et 2 pour l'identification et l'authentification :

		Palier 1	Palier 2
IDENTIFICATION			
Personne physique	Enregistrée dans un référentiel d'identité national en lien avec le domaine sanitaire et médico-social	<p>Identification locale :</p> <p>--> identifiant « privé » avec possibilité de plusieurs identifiants « privés » par personne</p> <p>Identification nationale :</p> <p>--> identification indirecte (identifiant « public » de la personne morale + identifiant « privé » de la personne physique)</p>	<p>Identification locale ou nationale :</p> <p>--> identifiant « public » (RPPS ou ADELI)</p>
	Non enregistrée dans un référentiel d'identité national en lien avec le domaine sanitaire et médico-social	<p>Identification locale :</p> <p>--> identifiant « privé » avec possibilité de plusieurs identifiants « privés » par personne</p> <p>Identification nationale :</p> <p>--> identification indirecte (identifiant « public » de la personne morale + identifiant « privé » de la personne physique)</p>	<p>Identification locale :</p> <p>--> identifiant « privé » unique</p> <p>Identification nationale :</p> <p>--> identification indirecte (identifiant « public » de la personne morale + identifiant « privé » de la personne physique)</p>
Personne morale		Non applicable	<p>Identification locale ou nationale :</p> <p>--> identifiant « public » (FINESS EJ, FINESS ET, SIREN ou SIRET) y compris identifiant opérationnel de portée nationale (RPPS-rang ou ADELI-rang)</p>

AUTHENTIFICATION			
Authentification « publique » des personnes physiques	Directe	-	Certificat logiciel de personne physique
	Architecture d'authentification	-	Authentification indirecte : --> Authentification « publique » de la personne morale --> Identification de portée nationale ou locale de la personne physique --> Authentification « privée » de la personne physique
Authentification « privée » des personnes physiques	Directe	Authentification basée sur un couple [identifiant individuel / mot de passe] Identification de l'acteur de santé de portée nationale ou locale Contraintes pour la construction des mots de passe	Tout dispositif d'authentification forte, au choix et sous la responsabilité du directeur d'Établissement Identification de l'acteur de santé de portée nationale ou locale
Authentification « publique » des personnes morales		-	Certificat serveur Référence à la personne morale responsable du serveur et identifiée dans le certificat. L'identifiant de la personne morale utilisé est national (FINESS, SIRET / SIREN).

À FAIRE



Qui ? Chaque gestionnaire du système



Quand ? Avant la mise en œuvre du système



Quoi ?

- Mettre en œuvre, pour les données à risque fort, les 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.

6. Pseudonymisation

Exigence 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.

Exigence 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 :

- être 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) ;
- être 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) ;
- être paramétrable (utilisation possible de différents secrets) ;
- être 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 pas 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. À 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.

Exigence 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.

Exigence 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. À 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 maîtrisé.

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.

Exigence 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.

OBJECTIF

Un processus de pseudonymisation doit être assuré au niveau de chaque système afin de protéger la confidentialité des données à caractère personnel.

À SAVOIR

- Les pseudonymes doivent être différents d'un système à l'autre afin d'éviter qu'une entité ayant des accès sur différents systèmes puisse reconstituer une base complète lui permettant d'identifier indirectement une personne.
- La confidentialité de la valeur secrète doit être assurée et ses processus de gestion finement décrits.
- Le renouvellement de pseudonyme doit être assuré en cas de mise à mal du secret de pseudonymisation.
- A ce jour, le tiers de confiance national et les processus associés ne sont pas encore définis.

La pseudonymisation, comment ça marche ?

Le processus de pseudonymisation et d'anonymisation sont deux processus bien distincts. Le concept de pseudonymisation requiert pour sa compréhension, le rappel de certaines définitions :

- **Une donnée à caractère personnel** (selon la *Loi Informatique et libertés*) « désigne toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. »
- **Une donnée anonyme** désigne une information à laquelle il est impossible de relier une personne, de manière directe ou indirecte.
- **L'anonymisation** désigne un processus qui rend impossible le lien entre une donnée et une personne, de manière directe ou indirecte. Ce processus permet de rendre une donnée anonyme. Il peut parfois utiliser un mécanisme de pseudonymisation, mais ce n'est pas une obligation.

Le législateur européen a donné une définition unique de la **pseudonymisation** pour tous les États membres de l'Union Européenne : « traitement de données à caractère personnel de telle façon qu'elles ne puissent plus être attribuées à une personne concernée sans avoir recours à des informations supplémentaires, pour autant que celles-ci soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir cette non-attribution à une personne identifiée ou identifiable. ».

Pour garantir la traçabilité et la mise à jour des informations dans la base et éviter d'associer à un individu les données relatives à un autre, faute de disposer d'un identifiant pérenne, il est nécessaire que, pour chaque personne, ce pseudonyme soit unique.

À cette fin, il peut être établi de trois manières différentes.

Une **table de correspondance secrète** peut être générée, qui associe une fois pour toutes, l'ensemble des identifiants avec les pseudonymes qui leur ont été attribués. Le niveau de sécurité de cette technique d'anonymisation est faible. L'opération est en effet réversible, puisqu'on peut retrouver l'identifiant à partir du pseudonyme et que celui qui détient la table lit à livre ouvert dans la base donnée : l'anonymisation n'est garantie qu'autant que cette table reste secrète.

La seconde façon de procéder à la « pseudonymisation » est d'utiliser un **algorithme de chiffrement** : l'ensemble des identifiants initiaux sont transformés en des pseudonymes uniques. L'opération est, là encore, réversible, puisque l'on peut retrouver l'identifiant à partir du pseudonyme, pour peu que l'on sache quel algorithme de chiffrement et quel secret ont été utilisés.

La dernière façon de procéder à la substitution d'un pseudonyme à l'identifiant initial est de recourir à une fonction dite de « **hachage** », qui présente la particularité, par rapport aux algorithmes de chiffrement standards, de ne pas être réversible : il n'est pas possible de retrouver l'identifiant initial à partir du seul pseudonyme, même si l'on connaît la fonction de hachage utilisée.

Toutefois, en dépit de cette irréversibilité de principe, cette technique peut être mise en échec en reconstituant, par itération, une table de correspondance. Cette méthode pour casser l'anonymisation suppose d'importants moyens informatiques : elle consiste à appliquer la fonction de hachage à l'ensemble des identifiants possibles (par exemple, l'ensemble des noms et prénoms des individus susceptibles d'appartenir à la base de données). Ainsi, on retrouve, pour chacun, le pseudonyme unique qui lui est attribué par la fonction de hachage initialement utilisées.

Il est possible de renforcer la sécurité de l'anonymisation en ajoutant préalablement aux identifiants initiaux une clé secrète arbitraire : par exemple au nom « Jean Dupont », on associe la clé « azerty », pour donner un second identifiant « Jean Dupontazerty », qu'on soumet alors à la fonction de hachage. Celui qui souhaitera reconstituer la table de correspondance devra donc non plus seulement tester l'ensemble des noms et prénoms possibles, ce qui est relativement facile, mais aussi l'ensemble des modifications que ces identifiants sont susceptibles de connaître à partir de clés inconnues.

La sécurité du dispositif repose cependant encore une fois sur la confidentialité des outils utilisés : la clé secrète d'une part, la fonction de hachage utilisée d'autre part.

Il est encore possible de durcir l'anonymisation, en procédant à un double hachage avec clé secrète, qui consiste à réaliser une première fois l'opération, et à soumettre le pseudonyme obtenu à une seconde fonction de hachage avec clé secrète. Pour assurer une pleine confidentialité, les clés

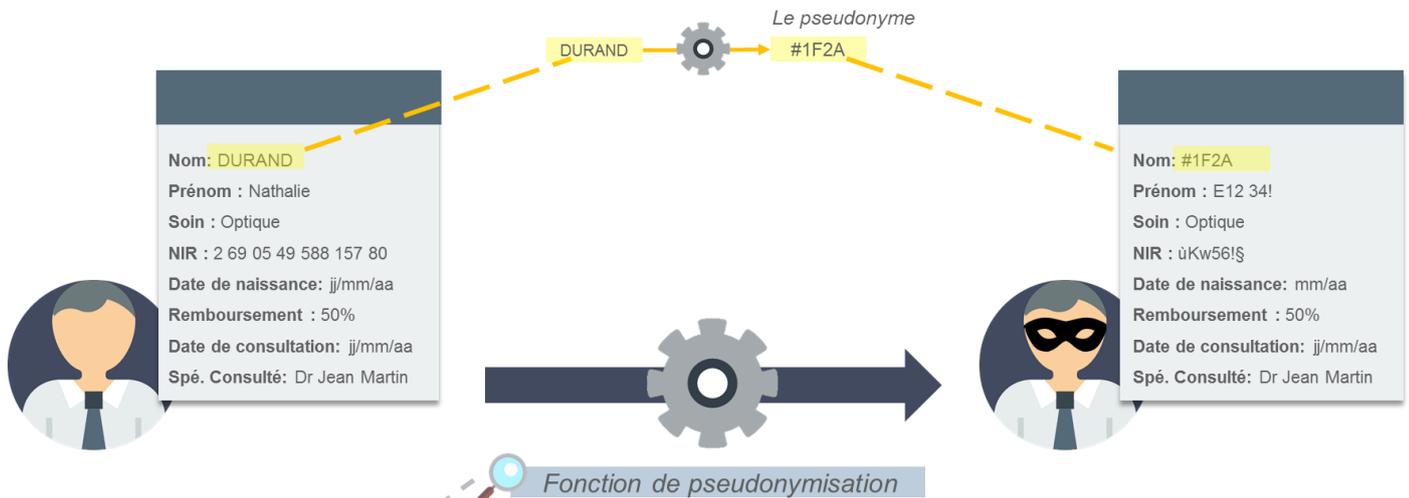
peuvent être renouvelées régulièrement. Toutefois, dans ce cas, il n'est plus possible de suivre dans le temps l'évolution des données relatives à un individu, puisqu'il n'y aura plus de moyen de mettre en relation son pseudonyme à un moment donné, avec un second pseudonyme généré plus tard.

Le processus de pseudonymisation :

1

Supprimer les champs directement identifiants des enregistrements et ajouter un nouveau champ qui doit rendre impossible tout lien entre cette nouvelle valeur et la personne réelle.

NB: Dans l'exemple, en jaune, #1F2A est le pseudonyme de DURAND



2

Une fonction de hachage est appliquée à un champ identifiant afin de rendre impossible le lien avec la valeur initiale



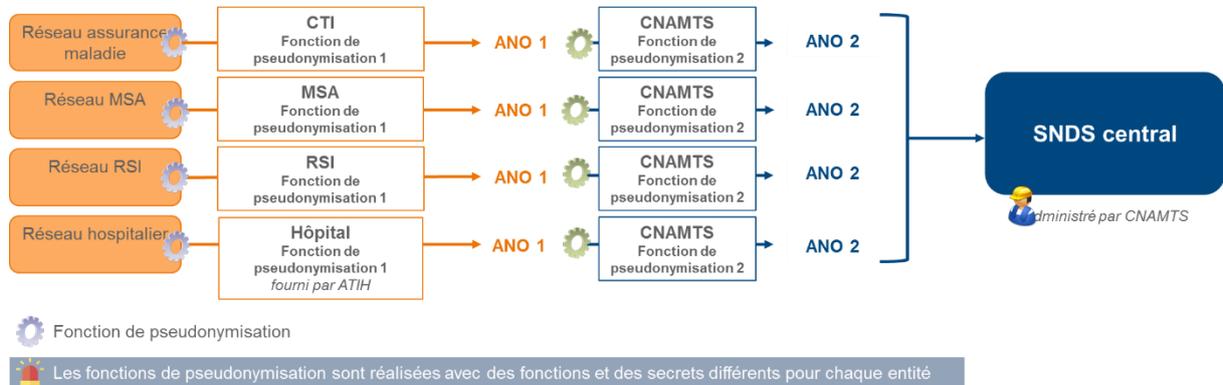
La pseudonymisation permet ainsi :

- **L'individualisation** : il est possible d'isoler les enregistrements d'une personne grâce à son identification par un attribut unique obtenu suite à la pseudonymisation.
- **La corrélation** : la corrélation est possible entre les différents enregistrements qui utilisent un attribut pseudonymisé commun faisant référence à une même personne. En particulier, cela permet le chaînage de deux exportations.

Dans le contexte du SNDS, la pseudonymisation est donc réalisée comme illustrée sur le schéma ci-dessous. Plusieurs systèmes sources alimentent le SNDS central. Une fonction de pseudonymisation doit être utilisée pour pseudonymiser les données venant de ces bases sources.

La fonction de pseudonymisation dans ce cas est à deux niveaux. Des pseudonymes dits de niveau 1 sont générés par le gestionnaire du système source cédant les données et alimentent le SNDS central. À la réception de ces jeux de données, le gestionnaire du SNDS central génère de nouveaux pseudonymes dits de niveau 2. Les fonctions de pseudonymisation utilisées successivement ne doivent pas avoir les mêmes secrets. Les fonctions de pseudonymisation de niveau 1 et de niveau 2 sont ainsi réalisées par des entités différentes et avec des secrets différents.

Le schéma de la cible du processus de pseudonymisation du SNDS central est donc le suivant :

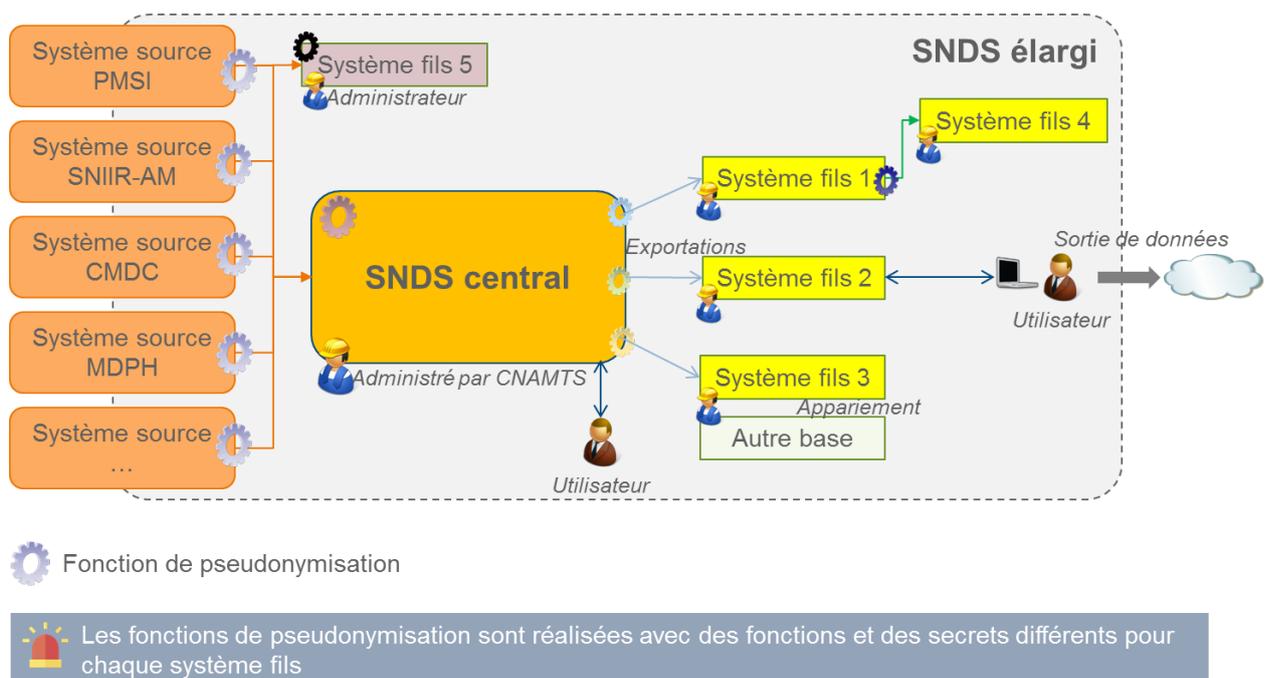


Les mentions **ANO 1** et **ANO 2** sont les résultats de la fonction de pseudonymisation.

Au niveau de chacun des systèmes fils, une nouvelle fonction de pseudonymisation doit être appliquée, au moment de l'exportation, afin que les pseudonymes soient différents d'un système à l'autre.

La fonction de pseudonymisation intervient également dans le cadre d'exportation des données du SNDS central vers des systèmes fils. 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.

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



À FAIRE



Qui ?

Le gestionnaire de système cédant les données et le gestionnaire de système recevant.



Quand ?

Avant la mise en œuvre du système.



Quoi ?

- Il est de la responsabilité de la CNAMTS de coordonner les fonctions de pseudonymisation utilisées par les systèmes sources afin d'assurer une alimentation cohérente du SNDS central.
- Pour les systèmes fils, il convient de mettre en place un système de pseudonymisation conforme au présent référentiel. La pseudonymisation avant chaque exportation est de la responsabilité du gestionnaire cédant les données.

7. Traçabilité

Exigence 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 [...].

Exigence 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.

Exigence 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 ; élévation 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.

Exigence 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.

Exigence 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.

OBJECTIF

Chaque gestionnaire de système doit s'assurer de disposer des éléments nécessaires afin de détecter les incidents de sécurité et être en capacité d'investiguer si besoin.

À SAVOIR

- Les gestionnaires doivent mettre en place des mesures relatives à la traçabilité des actions des utilisateurs et des administrateurs.
- Les mesures de traçabilité peuvent s'inscrire dans le cadre de la **convention** de preuve entre le gestionnaire de système et le gestionnaire du SNDS central ou le gestionnaire de système lui ayant cédé des données.
- Il s'agit pour le gestionnaire de système de conserver des **moyens de contrôle** sur l'application du Référentiel de sécurité afin d'assurer la détection des incidents de sécurité.
- La traçabilité doit permettre de **contrôler l'utilisation de données et de détecter les incidents de sécurité**.
- La traçabilité doit permettre de **disposer de preuves** pouvant être instruites en justice.
- Le palier d'imputabilité minimum pour la traçabilité du SNDS est le palier 3. Voici la synthèse des exigences présentées dans la PGSSI-S à ce sujet :

Paliers	Prérequis	Génération de la piste d'audit	Conservation des traces	Restitution de la piste d'audit	Documentation spécifique
1		Traces fonctionnelles	Possibilité d'extraction des traces pour conservation dans des endroits multiples pour réduire le risque de modifications systémiques	Outil de gestion de la preuve permettant la restitution ergonomique des traces fonctionnelles	Documentation des dispositifs d'authentification, de gestion des identités, des rôles, des habilitations et des traces
2	Palier 1 du référentiel d'identification et d'authentification Gestion dans le temps des identités, des rôles et des habilitations		Archives journalières regroupant l'ensemble des traces	utilisable par des non spécialistes de la sécurité	Idem palier 1 + Description des sources des traces et des processus mis en œuvre de la génération à la constitution de l'archive journalière
3	Heure partagée par l'ensemble des composants du SIS	Traces fonctionnelles Traces techniques provenant d'au moins un type de composant du SIS	Scellement quotidien des traces	Idem palier 1 + L'outil de gestion de la preuve permet de réconcilier les traces autant que de besoin L'outil de gestion de la preuve gère un format pivot ou gère de nombreux formats de traces Guide didactique d'utilisation de	Idem palier 2 + Description des processus mis en œuvre de la génération à la réconciliation

- Les grands items de la convention de preuve sont les suivants :
 - ▶ périmètre,
 - ▶ moyen d'exploitation,
 - ▶ processus d'escalade.
- L'ASIP met à disposition un référentiel sur l'imputabilité et la gestion des traces : http://esante.gouv.fr/sites/default/files/pgssi_referentiel_imputabilite_v1.0_0.pdf
- Les conventions établies entre les différentes parties devront indiquer les conditions portant :
 - ▶ sur la durée de conservation à respecter selon la sensibilité des jeux de données,
 - ▶ sur le besoin d'intégrité dans la collecte et la conservation des traces.

Les analyses de risques révèlent souvent un risque résiduel portant sur l'altération des journaux par un utilisateur ayant des privilèges d'administration et pouvant effacer toute trace d'action malveillante.



Bonnes pratiques :

- ➔ Les incidents de sécurité relatifs aux jeux de données mis à disposition doivent être remontés aux autres gestionnaires si l'incident de sécurité les concerne.
- ➔ Les traces d'échecs sur les opérations listées peuvent également être demandées explicitement. Elles sont souvent révélatrices d'incidents de sécurité potentiels.

À FAIRE



Qui ? Chaque gestionnaire de système



Quand ? Avant la mise en œuvre du système.



Quoi ?

- Mettre en place la collection des traces, les stocker et les protéger correctement.
- Exploiter les traces, à minima selon les scénarios préidentifiés.
- Savoir identifier les écarts temporels (ex. système d'horodatage).
- Informer les utilisateurs sur l'existence des traces.
- Sensibiliser sur les conséquences d'une utilisation inadéquate.

8. Contrôle

Exigence 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.

Exigence 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.

OBJECTIF

Chaque gestionnaire doit mettre en place les contrôles afin d'assurer l'amélioration continue du niveau de sécurité. Ces contrôles seront enrichis de contrôles externes.

À SAVOIR

- **Audit interne** : audit à l'initiative du gestionnaire de système (corps interne ou appel à un prestataire).
- **Audit externe** : audit mandaté par une entité tierce (par exemple le comité d'audit « données de santé »).
- Un prestataire qualifié PASSI (*Prestataires d'audit de la sécurité des systèmes d'information*) peut mener de audits d'architecture, de configuration, de code source, des tests d'intrusion, des audits organisationnels et physiques. Il doit subir une évaluation « exigence » qui s'appuie sur des références normalisés (ISO 27001, ISO 17065) ainsi que des exigences spécifiques (CERT CPS REF 63) : cela est donc un gage de qualité des audits de sécurité des systèmes d'information.
- L'ANSSI met à disposition un référentiel des prestataires PASSI :
<http://www.ssi.gouv.fr/entreprise/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-daudit-de-la-securite-des-systemes-dinformation-passi-qualifies/>
- Les acteurs qui accèdent aux données du SNDS peuvent être contrôlés par la Commission nationale de l'informatique et des libertés (CNIL).
En effet la CNIL a, parmi ses missions principales, une mission de contrôle et de sanction

Rappel des attributions de la CNIL en matière de contrôle et de sanction

Le contrôle sur place, sur pièces, sur audition ou en ligne permet à la CNIL de vérifier la mise en œuvre concrète de la loi et des autorisations qu'elle délivre.

Un programme des contrôles est élaboré annuellement, en fonction des thèmes d'actualité, des grandes problématiques identifiées et des plaintes dont la CNIL est saisie.

.../...

Lors d'un contrôle sur place, la CNIL peut :

- accéder à tous les locaux professionnels,
- demander communication de tout document nécessaire et en prendre copie,

- recueillir tout renseignement utile et entendre toute personne,

- accéder aux programmes informatiques et aux données.

Seul un médecin peut requérir un accès aux données médicales individuelles.

A l'issue des contrôles, le Président de la CNIL peut clôturer la procédure ou, en cas de manquement, décider d'adresser une mise en demeure à l'organisme contrôlé. La formation restreinte de la CNIL, composée de 5 membres, peut prononcer diverses sanctions à l'issue d'une procédure contradictoire, notamment un avertissement ou une sanction pécuniaire (sauf pour les traitements de l'État) d'un montant maximal de 3 millions d'euros. Cette sanction peut être rendue publique ; la formation contentieuse peut également ordonner l'insertion de sa décision dans la presse, ou ordonner que les organismes sanctionnés informent individuellement les personnes concernées aux frais de l'organisme sanctionné.

Le montant des amendes est perçu par le Trésor Public et non par la CNIL.

La formation restreinte de la CNIL peut également prononcer :

- Une injonction de cesser le traitement.

- Un retrait de l'autorisation accordée par la CNIL.

En cas d'atteinte grave et immédiate aux droits et libertés, le président de la CNIL peut demander, par référé, à la juridiction compétente, d'ordonner toute mesure nécessaire. Il peut également dénoncer au Procureur de la République les infractions à la législation dont il a connaissance.

- L'entrée en vigueur du règlement européen renforce les missions de contrôle et de sanction de la CNIL.

Les responsables de traitement et les sous-traitants peuvent faire l'objet de sanctions administratives importantes en cas de méconnaissance des dispositions du règlement. La CNIL et ses homologues européennes peuvent notamment :

- prononcer un avertissement,
- mettre en demeure l'entreprise,
- limiter temporairement ou définitivement un traitement,
- suspendre les flux de données,
- ordonner de satisfaire aux demandes d'exercice des droits des personnes,
- ordonner la rectification, la limitation ou l'effacement des données.

Les amendes administratives peuvent s'élever, selon la catégorie de l'infraction, de 10 ou 20 millions d'euros, ou, dans le cas d'une entreprise, **de 2% jusqu'à 4% du chiffre d'affaires annuel mondial**, le montant le plus élevé étant retenu.

À FAIRE

Cette exigence souligne deux obligations : la mise en place de contrôles réguliers d'une part et une revue des habilitations régulière d'autre part.

Contrôles périodiques



Qui ? Chaque gestionnaire de système et le comité d'audit « données de santé »



Quand ? Périodiquement à partir de la mise en œuvre du système.



Quoi ?

- Mettre en place des audits internes et externes périodiquement pour contrôler l'application du référentiel de sécurité.

Revue des habilitations



Qui ? Chaque gestionnaire de système



Quand ? Périodiquement à partir de la mise en œuvre du système.



Quoi ?

- Mettre en place une revue annuelle des habilitations.

9. Droits des personnes

Exigence 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.

Exigence 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.

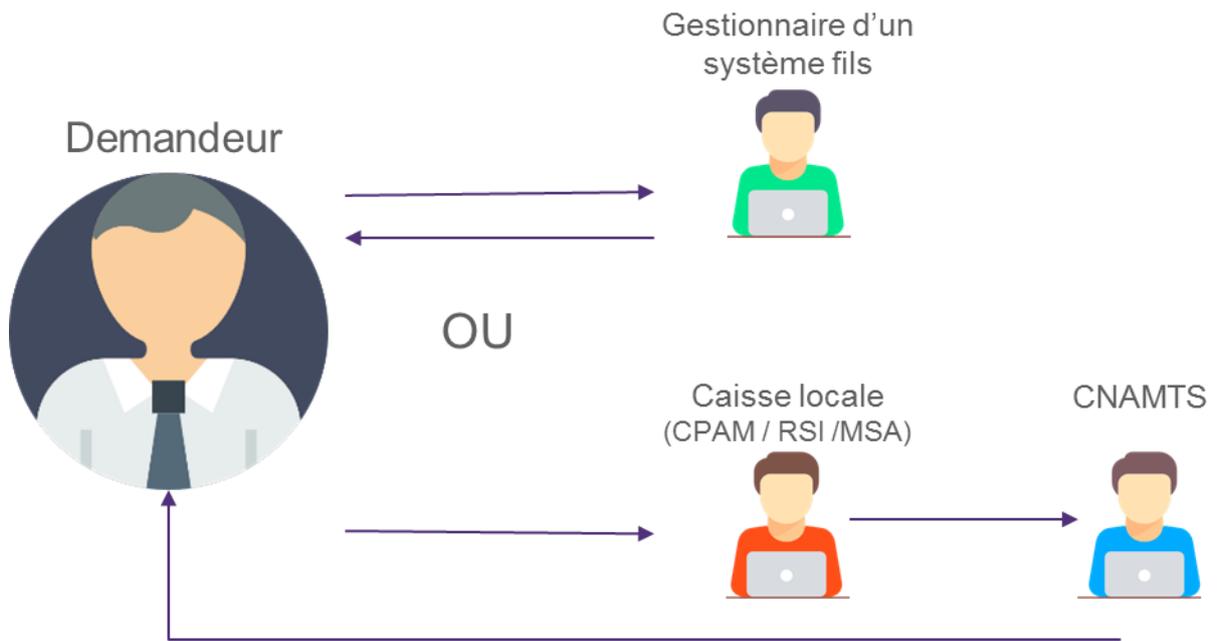
OBJECTIF

Le gestionnaire du SNDS central doit s'assurer de la conformité du système avec les exigences du règlement européen sur la protection des données à caractère personnel.

À SAVOIR

- **Droit d'accès** : demande, formulée par le citoyen, de communication des informations le concernant détenues dans une base de données débouchant sur l'obligation pour le responsable de traitement de transmettre l'intégralité des données concernées.
- **Droit d'opposition** : pour une personne ayant fait jouer son droit d'opposition, « ses données de santé à caractère personnel ne seront pas mises à disposition dans le cadre du 1° du I de l'article L. 1461-3 de la LOI n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé. »
- Le droit d'accès et d'opposition peuvent s'exercer auprès du SNDS central ainsi qu'unitairement, auprès des systèmes fils.

Exemple de démarche :



- Tout organisme doit répondre dans un délai maximal de 2 mois à compter de la réception de la demande. La Cnil met à disposition un guide du droit d'accès et d'opposition : https://www.cnil.fr/sites/default/files/atoms/files/cnil_droit_d_acces.pdf_0_0.pdf
- Les informations communiquées par le responsable de traitement doivent être lisibles (cf. indicateur n°60 du règlement européen sur la protection des données à caractère personnel (« Ces informations peuvent être fournies accompagnées d'icônes normalisées afin d'offrir une bonne vue d'ensemble, facilement visible, compréhensible et clairement lisible, du traitement prévu ») et article 95 de la loi informatique et libertés).

À FAIRE



Qui ? Le gestionnaire du SNDS central



Quand ? Avant la mise en œuvre du système.



Quoi ?

- Sensibiliser les personnels de caisses locales sur les possibilités de demandes relatives à ces droits sur les plateformes de service (flux entrants : guichets, téléphone, mail, courrier, internet, ...). *Mettre en place les processus de gestion de ces droits d'accès et d'opposition.*
- S'assurer de l'identité de la personne exerçant ses droits et de la validité des informations communiquées.

10. Homologation

Exigence 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).

OBJECTIF

Les risques résiduels doivent être validés par le responsable de traitement.

À SAVOIR

- Les risques résiduels, issus de l'analyse de risques, doivent être précisément décrits et faire l'objet d'une acceptation formelle.
- Selon l'ANSSI, « En informatique, comme dans les autres domaines, le risque zéro n'existe pas. La démarche d'homologation de sécurité est destinée à faire connaître et faire comprendre aux responsables les risques liés à l'exploitation d'un système d'information. Il s'agit d'un processus d'information et de responsabilisation qui aboutit à une décision, prise par le responsable de l'organisation. Cette décision constitue un acte formel par lequel il :
 - atteste de sa connaissance du système d'information et des mesures de sécurité (techniques, organisationnelles ou juridiques) mises en œuvre
 - accepte les risques qui demeurent, qu'on appelle risques résiduels. »
- Pour faciliter la mise en œuvre de la démarche d'homologation, l'ANSSI a édité le guide de l'homologation de sécurité en neuf étapes simples :

http://www.ssi.gouv.fr/uploads/2014/06/guide_homologation_de_securite_en_9_etapes.pdf

À FAIRE



Qui ? Le responsable de traitement et chaque gestionnaire de système



Quand ? Avant la mise en œuvre du système et à chaque modification significative de l'analyse de risques.



Quoi ?

- Le responsable de traitement doit homologuer formellement le système avant sa mise en œuvre.
- Le gestionnaire du système doit formaliser les risques résiduels

Annexe 1. Détail des exigences MCAS

Titre de l'exigence	Réf. Exigence	Détail exigence
Gestion des mots de passe	EXP-GEST-AUTH	Les utilisateurs ne doivent pas stocker leurs mots de passe en clair (par exemple dans un fichier) sur leur poste de travail. Les mots de passe ne doivent pas transiter en clair sur les réseaux.
Sécurisation des flux d'administration	EXP-SEC-FLUXADMIN	Les opérations d'administration sur les ressources locales d'une entité doivent s'appuyer sur des protocoles sécurisés. Un réseau dédié à l'administration des équipements, ou au moins un réseau logiquement séparé de celui des utilisateurs, doit être utilisé. Les postes d'administrateurs doivent être dédiés et ne doivent pas pouvoir accéder à Internet.
Protection contre les codes malveillants	EXP-PROT-MALV	Des logiciels de protection contre les codes malveillants, appelés communément antivirus, doivent être installés sur l'ensemble des serveurs d'interconnexion, serveurs applicatifs et postes de travail de l'entité. Ces logiciels de protection doivent être distincts pour ces trois catégories au moins, et le dépouillement de leurs journaux doit être corrélié.
Mise à jour de la base de signature	EXP-MAJ-ANTIVIR	Les mises à jour des bases antivirales et des moteurs d'antivirus doivent être déployées automatiquement sur les serveurs et les postes de travail par un dispositif prescrit par les directions, bureaux ou services informatiques, validé par le RSSI.
Configuration du navigateur internet	EXP-NAVIG	Le navigateur déployé par l'équipe locale chargée des SI sur l'ensemble des serveurs et des postes de travail nécessitant un accès Internet ou Intranet doit être configuré de manière sécurisée (désactivation des services inutiles, nettoyage du magasin de certificats, etc.).
Maîtrise des matériels	EXP-MAIT-MAT	Les postes de travail - y compris dans le cas d'une location - sont fournis à l'utilisateur par l'entité, gérés et configurés sous la responsabilité de l'entité. La connexion d'équipements non maîtrisés, non administrés ou non mis à jour par l'entité (qu'il s'agisse d'ordiphones, d'équipements informatiques nomades et fixes ou de supports de stockage amovibles) sur des équipements et des réseaux professionnels est interdite.
Rappel des mesures de protection contre le vol	EXP-PROT-VOL	Les postes fixes bénéficient des mesures de protection physique offertes au titre de la directive de sécurité physique de la présente PSSI-MCAS. Chaque utilisateur doit veiller à la sécurité des supports amovibles (clés USB et disques amovibles), notamment en les conservant dans un endroit sûr. Il est recommandé de chiffrer les données contenues sur ces supports. Les supports contenant des données sensibles doivent être stockés dans des meubles fermant à clef.
Déclarer les pertes et vols	EXP-DECLAR-VOL	Toute perte ou vol d'une ressource d'un système d'information doit être déclarée au RSSI.
Réaffectation de matériels informatiques	EXP-REAFLECT	Une procédure de gestion des postes et supports dans le cadre de départs de personnel ou de réaffectations à de nouveaux utilisateurs doit être mise en place et validée par le RSSI. Elle doit définir les conditions de recours à un effacement des données.
Déclaration des équipements nomades aptes à traiter les informations sensibles	EXP-NOMAD-SENS	L'autorité d'homologation du SI valide les usages possibles des équipements nomades vis-à-vis du traitement des informations sensibles ; les usages non explicitement autorisés sont interdits.
Accès à distance au système d'informations de l'organisme	EXP-ACC-DIST	Les utilisateurs distants doivent s'authentifier sur le réseau de l'entité en utilisant une authentification forte.
Système d'exploitation	EXP-CI-OS	Les systèmes d'exploitation déployés doivent faire l'objet d'un support valide de la part d'un éditeur ou d'un prestataire de service. Seuls les services et applications nécessaires sont installés, de façon à réduire la surface d'attaque. Une attention particulière doit être apportée aux comptes administrateurs.
Fourniture et gestion des postes de travail	PDT-GEST	Les postes de travail utilisés dans le cadre professionnel sont fournis et gérés par l'équipe locale chargée des SI. Si un poste est mis à disposition par une autre voie, sa connexion au réseau est soumise à l'autorisation du RSSI.
Formalisation de la configuration des postes de travail	PDT-CONFIG	Une procédure formalisée de configuration des postes de travail est établie par chaque entité.
Verrouillage de l'unité centrale des postes fixes	PDT-VEROUIL-FIXE	Lorsque l'unité centrale d'un poste fixe est peu volumineuse, donc susceptible d'être facilement emportée, elle doit être protégée contre le vol par un système d'attache (par exemple un câble antivol).
Verrouillage des postes portables	PDT-VEROUIL-PORT	Un câble physique de sécurité doit être fourni avec chaque poste portable. Les utilisateurs doivent être sensibilisés à son utilisation.
Réaffectation du poste de travail	PDT-REAFLECT	Une procédure SSI définit les règles concernant le traitement à appliquer aux informations ayant été stockées ou manipulées sur les postes réaffectés.
Privileges des	PDT-PRIVIL	La gestion des privilèges des utilisateurs sur leurs postes de travail doit suivre le principe

utilisateurs sur les postes de travail		du « moindre privilège » : chaque utilisateur ne doit disposer que des privilèges nécessaires à la conduite des actions relevant de sa mission.
Utilisation des privilèges d'accès administrateurs	PDT- PRIV	Les privilèges d'accès « administrateur » doivent être utilisés uniquement pour les actions d'administration le nécessitant.
Gestion du compte administrateur local	PDT-ADM-LOCAL	L'accès au compte « administrateur local » sur les postes de travail doit être strictement limité aux équipes en charge de l'exploitation et du support sur ces postes de travail.
Stockage des information	PDT-STOCK	Dans la mesure du possible, les données traitées par les utilisateurs doivent être stockées sur des espaces réseau, eux-mêmes sauvegardés selon les exigences des entités.
Sauvegarde : synchronisation des données locales	PDT-SAUV-LOC	Dans le cas où des données doivent être stockées en local sur le poste de travail, des moyens de synchronisation ou de sauvegarde doivent être fournis aux utilisateurs.
Partage de fichiers	PDT-PART-FIC	Le partage de répertoires ou de données hébergées localement sur les postes de travail est à proscrire
Suppression des données sur les postes partagés	PDT-SUPPR-PART	Les données présentes sur les postes partagés (portable de prêt, par exemple) doivent être supprimées entre deux utilisations, dès lors que les utilisateurs ne disposent pas du même besoin d'en connaître.
Chiffrement des données sensibles	PDT-CHIFF-SENS	Une solution de chiffrement labellisée doit être mise à disposition des utilisateurs et des administrateurs afin de chiffrer les données sensibles stockées sur les postes de travail, les serveurs, les espaces de travail, ou les supports amovibles.
Fourniture de supports de stockage amovible	PDT-AMOV	Les supports de stockage amovibles (clés USB et disque durs externes, notamment) doivent être fournis aux utilisateurs par l'équipe locale chargée des SI.
Accès à distance aux SI de l'entité	PDT-NOMAD-ACCES	Les accès à distance aux SI de l'entité (accès dits « nomades ») doivent être réalisés via des infrastructures homologuées. L'usage de réseaux privés virtuels (VPN) de confiance est nécessaire.
Pare-feu local	PDT-NOMAD-PAREFEU	Un pare-feu local conforme aux directives nationales doit être installé sur les postes nomades.
Stockage local d'information sur les postes nomades	PDT-NOMAD-STOCK	Le stockage local d'information sur les postes de travail nomades doit être limité au strict nécessaire. Les informations sensibles doivent être obligatoirement chiffrées par un moyen de chiffrement labellisé.
Filtre de confidentialité	PDT-NOMAD-FILT	Pour les postes de travail nomades manipulant des données sensibles, un filtre de confidentialité doit être fourni et être positionné sur l'écran dès lors que le poste est utilisé en dehors de l'entité.
Configuration des interfaces de connexion sans fil	PDT-NOMAD-CONEX	La configuration des interfaces de connexion sans fil doit interdire les usages dangereux de ces interfaces.
Désactivation des interfaces de connexion sans fil	PDT-NOMAD-DESACTIV	Des règles de configuration des interfaces de connexion sans fil (Wifi, Bluetooth, 3G...), permettant d'interdire les usages non maîtrisés et d'éviter les intrusions via ces interfaces, doivent être définies et appliquées. Les interfaces sans fil ne doivent être activées qu'en cas de besoin.
Durcissement des imprimantes et copieurs multifonctions	PDT-MUL-DURCISS	Les imprimantes et copieurs multifonctions hébergés localement dans une entité doivent faire l'objet d'un durcissement en termes de sécurité : changement des mots de passe initialement fixés par le « constructeur », désactivation des interfaces réseau inutiles, suppression des services inutiles, chiffrement des données sur le disque dur lorsque cette fonctionnalité est disponible, configuration réseau statique.
Sécurisation de la fonction de numérisation	PDT-MUL-SECNUM	Lorsqu'elle est activée, la fonction de numérisation sur les copieurs multifonctions hébergés dans une entité doit être sécurisée. Les mesures de sécurité suivantes doivent notamment être appliquées : envoi de documents uniquement à destination d'une adresse de messagerie interne à l'entité, envoi uniquement à une seule adresse de messagerie.
Sécuriser la configuration des autocommutateurs	PDT-TEL-MINIM	Les autocommutateurs doivent être maintenus à jour au niveau des correctifs de sécurité. Leur configuration doit être durcie. La définition et l'affectation des droits d'accès et des privilèges aux utilisateurs (transfert départ-départ, entrée en tiers, interphonie, autorisation de déblocage, renvoi sur numéro extérieur, substitution, substitution de privilège, interception d'appel dirigé, etc.) doivent faire l'objet d'une attention particulière. Une revue de la programmation téléphonique doit être organisée périodiquement.
Codes d'accès téléphoniques	PDT-TEL-CODES	Il est nécessaire de sensibiliser les utilisateurs au besoin de modifier le code d'accès de leur téléphone et de leur messagerie vocale.
Limiter l'utilisation du DECT	PDT-TEL-DECT	Les communications réalisées au travers du protocole DECT sont susceptibles d'être interceptées, même si les mécanismes d'authentification et de chiffrement que propose ce protocole sont activés. Il est recommandé d'attribuer des postes téléphoniques filaires aux utilisateurs dont les échanges sont les plus sensibles.
Utiliser les outils de vérification automatique de la conformité	PDT-CONF-VERIF	Un outil de vérification régulière de la conformité des éléments de configuration des postes de travail doit être mis en place, afin d'éviter une dérive dans le temps de ces éléments de configuration.

