GOUVERNEMENT
Liberté
Égalité
Fraternité

Délégation au numérique
en santé

AGENCE
DU NUMÉRIQUE
EN SANTÉ

Référentiel INS-Identité Nationale de Santé

Statut : Validé | Classification : Public | Version : v2.1

SOMMAIRE

Exigences
L'ensemble des exigences du référentiel est identifiable par un encadré gris

1. SYNTHESE DU REFERENTIEL

Objet du référentiel

Le référentiel « Identité nationale de santé », ci-après INS, décrit les conditions et modalités de mise en œuvre de l'obligation de référencement des données de santé avec l'INS.

Ce référentiel concerne notamment le référencement des données de santé avec le numéro d'inscription au répertoire national d'identification des personnes physiques (NIR) ou le numéro d'immatriculation d'attente (NIA) uniquement pour la prise en charge sanitaire et le suivi médico-social (les autres usages du NIR ne sont pas couverts).

La présente version du référentiel (V2.1 – 2023) annule et remplace la version du référentiel publiée en annexe de l'arrêté du 27 mai 2021 (V2.0 – mai 2021). – journal officiel du 8 juin 2021.

Champ d'application :

Afin de protéger les données de santé qu'elle référence, l'INS est restreinte à un nombre limité d'acteurs constituant un cercle de confiance dont les contours sont réglementairement définis. Pour ces acteurs, le référencement des données de santé avec l'INS est obligatoire.

L'appartenance à ce cercle de confiance repose sur l'appréciation de quatre critères :

- la finalité du traitement ;
- le champ d'application organique de l'obligation d'utilisation du NIR comme matricule INS ;
- la nécessité de référencer les données manipulées à l'aide de l'INS ;
- le fait qu'aucun texte ou autre obstacle légitime ne s'oppose à l'identification de l'usager.

Seuls les acteurs de la santé et du médico-social concourant à la prise en charge de l'usager, au suivi médico-social de la personne, ou menant des actions de prévention sont tenus d'utiliser l'INS. Ils peuvent recourir à un tiers en qualité de sous-traitant au sens de la loi Informatique et Libertés pour la mise en œuvre de cette obligation.

En dehors de ce cercle de confiance, le référencement des données de santé avec l'INS est interdit, sauf pour les acteurs disposant d'un fondement légal spécifique.

Impacts pour les professionnels inclus dans le champ d'application

Les professionnels inclus dans le champ d'application ont l'obligation de référencer les données de santé avec l'INS, mais il n'y a pas d'obligation de supprimer l'identifiant local (voir 4.3.3). En priorité, le déploiement de l'INS au sein du système d'information concerne le(s) logiciel(s) gérant les identités des usagers et le(s) logiciel(s) de gestion du dossier informatisé des usagers.

Afin d'assurer la qualité du référencement des données de santé avec l'INS, celle-ci doit être qualifiée dès que possible. Pour ce faire, deux critères doivent être respectés :

- le matricule INS et les traits d'identité doivent être récupérés via les opérations du téléservice INSi (recherche ou vérification) ou à partir de l'Appli carte Vitale (carte Vitale dématérialisée) ;
- l'identité de la personne doit être vérifiée en respectant des procédures d'identitovigilance décrites dans le Référentiel national d'identitovigilance (RNIV) joint en annexe.

Impacts techniques

L'INS (le matricule INS et les traits d'identité de référence) doit bénéficier des mêmes mesures de sécurité que les données de santé. Cependant le niveau de sécurité nécessaire doit être revu, notamment, en procédant à une mise à jour de l'évaluation des risques (étude de risques, étude d'impact sur la vie privée).

Un champ doit être implémenté (ou le champ identifiant devra être multivalué) dans les systèmes d'information pour renseigner le matricule INS, notamment afin d'éviter toute confusion avec d'autres champs ayant pour valeur le NIR (numéro INSEE, numéro de sécurité sociale…). En effet, à titre d'exemple, le matricule INS et le numéro utilisé pour les remboursements par la sécurité sociale peuvent être différents pour une même personne (pour les ayants droit, on aurait l'utilisation du matricule INS du patient pour la prise en charge et l'utilisation du NIR de l'ouvrant droit pour le remboursement des soins). Conformément aux règles communes de l'identitovigilance, le matricule INS seul n'apporte pas de garantie suffisante, il doit être accompagné des traits d'identité provenant des bases de référence nationales. Les traits d'identités récupérés des bases de référence remplacent dès que possible les traits d'identité locaux.

Sauf exceptions définies dans le RNIV, les données issues des téléservices (matricule INS, OID et traits d'identité de référence) ne devront pas être modifiées localement mais uniquement par consultation (ou requête) des téléservices ou par récupération depuis l'Appli carte Vitale.

2. INTRODUCTION

2.1. Objet du document

Les conditions et modalités d'utilisation du NIR comme INS sont précisées aux articles R. 1111-8-1 à R. 1111-8-7 du code de la santé publique (CSP). Il prévoit notamment **l'établissement d'un référentiel qui** :

> *« [..] définit les modalités de mise en œuvre de l'obligation de référencement des données de santé avec l'identifiant national de santé prévue au III de l'article R. 1111-8-1.*
>
> *[…] précise les procédures de surveillance et de gestion des risques et erreurs liés à l'identification des personnes prises en charge devant être mises en œuvre par les professionnels, établissements, services et organismes mentionnés à l'article R. 1111-8-3*
>
> *[…] ainsi que les mesures de sécurité applicables aux opérations de référencement de données à caractère personnel mentionnées au même article. »*
>
> 🕮 *Article R. 1111-8-7 du CSP*

Le présent document **constitue le référentiel prévu à l'article R. 1111-8-7**, ci-après « référentiel INS ». Il a pour objectif de préciser les modalités de mise en œuvre de l'INS **dans les services numériques en santé**.

Ce référentiel :

- détermine les acteurs auxquels s'applique l'obligation de référencer les données de santé à caractère personnel avec l'INS et en précise les conditions et modalités d'utilisation ;
- précise les mesures de sécurité à mettre en œuvre ;
- décrit, au travers du Référentiel national d'identitovigilance qui lui est annexé, l'ensemble des règles à mettre en place par les organismes responsables du référencement dans ce domaine ;
- propose en annexe un guide d'implémentation de l'INS dans les logiciels, à destination des éditeurs de logiciels qui équipent les professionnels et établissements intervenant dans la prise en charge sanitaire ou médico-sociale.

Ce référentiel n'a pas vocation à décrire l'ensemble des règles de sécurité s'appliquant aux données de santé mais uniquement à préciser les mesures de sécurité devant être appliquées du fait du référencement des données de santé par l'INS.

Précision sémantique

Le terme d'identité nationale de santé désigné sous l'acronyme INS dans le présent référentiel est à distinguer du NIR se référant au numéro d'inscription au répertoire national d'identification des personnes physiques.

Il convient de ne pas confondre :

- le matricule INS, qui a pour valeur le NIR ou le NIA, et dont l'usage est réservé pour le référencement de données de santé à des fins de prise en charge sanitaire ou de suivi médico-social (au sens de l'article L. 1111-8-1 I du CSP) ;

- le NIR pour les autres usages décrits dans le décret n° 2019-341 du 19 avril 2019 relatif à la mise en œuvre de traitements comportant l'usage du numéro d'inscription au répertoire national d'identification des personnes physiques ou nécessitant la consultation de ce répertoire.

Le NIR n'est qualifié de matricule INS que lorsqu'il est utilisé pour référencer des données de santé à des fins de prise en charge sanitaire ou de suivi médico-social.

En pratique, un individu a un seul NIR mais ce NIR peut être utilisé à différentes fins, chacune s'accompagnant de règles spécifiques (des précisions sont apportées au chapitre **« 3.1.3** Usages **» de ce présent référentiel).**

2.2. Contexte

2.2.1. Destinataires du document

Le référentiel s'adresse aux professions concernées par la prise en charge à des fins sanitaires et médico-sociales et plus généralement à toutes les personnes impliquées dans la mise en œuvre et l'usage de services numériques en santé exploitant des données de santé à caractère personnel (responsables du référencement des données de santé, prestataires de services, éditeurs, etc.) afin de réaliser la prise en charge à des fins sanitaires et médico-sociales des personnes.

Dans la mesure où l'INS doit être intégrée à des processus métier, l'ensemble des acteurs de la chaîne métier est concerné par les mesures de sécurité détaillées dans le présent référentiel.

2.2.2. L'obligation d'utilisation de l'identité nationale de santé

Les articles R. 1111-8-1 à R. 1111-8-7 du Code de la Santé Publique prévoient que le **numéro d'inscription au répertoire** national d'identification des personnes physiques (dit « NIR » ou numéro de sécurité sociale) **constitue désormais l'identifiant national dans les champs de la santé et du médico-social**.

> *« Le numéro d'inscription au répertoire national d'identification des personnes physiques **est utilisé comme identifiant de santé** des personnes **pour leur prise en charge à des fins sanitaires et médico-sociales**, dans les conditions prévues à l'article L. 1110-4. »*
>
> *📖 Article L. 1111-8-1.-I. du CSP*
>
> *« Tout autre identifiant **ne peut être utilisé pour le référencement des données de santé qu'en cas d'impossibilité de pouvoir accéder à l'identifiant national de santé**, afin de ne pas empêcher la prise en charge sanitaire et médico-sociale des personnes »*
>
> *📖 Article R. 1111-8-1 du CSP*

2.2.3. Les bénéfices escomptés

Le développement des services numériques dans les champs de la santé et du médico-social ne pourra devenir effectif que si les conditions juridiques, organisationnelles et techniques requises pour créer et maintenir la confiance des acteurs qui les utilisent sont mises en œuvre.

La qualité de l'identification des usagers constitue l'un des piliers de cette confiance. Elle permet en effet :

- d'éviter des erreurs d'identification des personnes prises en charge (doublons, collisions, …) ;
- de s'assurer de la bonne association des données de santé à caractère personnel avec la personne à laquelle elles se rapportent et de faciliter la détection d'erreur d'attribution de documents ;
- d'améliorer le suivi d'un usager dans le cadre des parcours de soins, en facilitant la circulation, l'échange et l'agrégation des données de sa prise en charge par les divers constituants des systèmes d'information impliqués.

La fluidité des échanges et du partage d'informations de santé au bénéfice de la prise en charge coordonnée de l'usager dépend de la confiance accordée à l'indexation des données partagées, de l'assurance de traiter du même usager entre partenaires issus de disciplines différentes et de la libération de contraintes géographiques non corrélées avec la mobilité des usagers.

Le recours à une identité nationale de santé réunit ces conditions. Elle permet le référencement fiable et univoque des données de santé des usagers sous réserve du respect de règles édictées dans le présent référentiel. Ces règles reposent essentiellement sur :

- d'une part, la bonne identification des usagers, par le biais de procédures d'identitovigilance rigoureuses spécifiées dans le Référentiel national d'identitovigilance ;
- d'autre part, le bon référencement des données de santé, par le recours à un identifiant unique et pérenne sur le territoire (le NIR) en s'appuyant sur des bases de référence.

Ce choix est conforme à la liberté d'appréciation laissée par l'article 87 du règlement européen sur la protection des données personnelles, ci-après « RGPD », relatif au traitement d'un numéro d'identification national.

> *« Les États membres peuvent préciser les conditions spécifiques du traitement d'un numéro d'identification national ou de tout autre identifiant d'application générale. Dans ce cas, le numéro d'identification national ou tout autre identifiant d'application générale n'est utilisé que sous réserve des garanties appropriées pour les droits et libertés de la personne concernée adoptées en vertu du présent règlement. »*
>
> *🕮 Article 87 du RGPD*

Identifiant de portée nationale, le NIR associé aux traits d'identité est apparu comme la solution la plus adaptée au législateur pour identifier les usagers du système de santé, référencer leurs données administratives et de santé et en favoriser la diffusion entre acteurs de la prise en charge, cela dans le respect des règles relatives à la confidentialité des données de santé, au cadre d'échange et de partage des données de santé, fixés notamment par les articles L. 1110-4 et L. 1111-8 du code de la santé publique et par la loi Informatique et Libertés.

3. CARACTERISTIQUES DU NIR ET DU NIA

Les textes prévoient que le matricule INS est :

1) le numéro d'inscription au répertoire national d'identification des personnes physiques (NIR) (Article L. 1111-8-1 du CSP) ;
2) ou le numéro d'immatriculation d'attente (NIA) pour les personnes en instance d'attribution d'un NIR (Art. R. 1111-8-1.-I du CSP).

Tout autre identifiant ne peut être utilisé pour référencer des données de santé qu'en cas d'impossibilité de pouvoir accéder à l'identité nationale de santé, afin de ne pas empêcher la prise en charge sanitaire et médico-sociale des personnes.

Cela peut concerner notamment :

- des personnes qui n'ont pas vocation à disposer d'un NIR ou d'un NIA comme par exemple les touristes étrangers (i.e. non-résidents nationaux) ;
- des personnes disposant ou ayant vocation à disposer d'un NIR, inconnu au moment de la prise en charge comme, par exemple, des personnes dont l'identité n'est pas déterminable au moment de la prise en charge (exemple personne inconsciente, personne prise en charge en situation d'urgence dont on ignore l'identité) ;
- des nouveau-nés pendant le délai de quelques jours nécessaires à la déclaration de leur naissance aux services d'état civil et à leur enregistrement dans le RNIPP
- des personnes bénéficiant d'une prise en charge anonyme ;
- des personnes disposant d'un NIR temporairement non vérifiable auprès du téléservice INSi par défaillance technique ponctuelle.

Un autre identifiant, lorsqu'il est nécessaire à la prise en charge sanitaire ou médico-sociale, peut continuer d'être utilisé localement lorsque les données de santé sont référencées par l'INS.

3.1. Le numéro d'inscription au répertoire (NIR)

> *« Le numéro d'inscription au répertoire national d'identification des personnes physiques est utilisé comme identifiant de santé des personnes pour leur prise en charge à des fins sanitaires et médico-sociales, dans les conditions prévues à l'article L. 1110-4. »*
>
> *Article L. 1111-8-1 du CSP*

Le numéro d'inscription au répertoire (NIR) est un identifiant unique attribué à toute personne inscrite au répertoire national d'identification des personnes physiques (RNIPP).

Les informations traitées par le RNIPP et les éléments constitutifs du NIR sont définis dans les règles relatives au RNIPP. Les principales caractéristiques du RNIPP et du NIR sont décrites ci-après.

Le NIR est attribué par l'INSEE pour les personnes nées en France métropolitaine et dans les départements et régions d'outre-mer (DROM) ou par la CNAV par délégation de l'INSEE pour les personnes nées à

l'étranger et dans les collectivités d'outre-mer (COM), au travers du système miroir du RNIPP, le SNGI, qui est en réplication quotidienne du RNIPP.

3.1.1. Population couverte et modalités d'affectation

Sont enregistrées dans le RNIPP et disposent ainsi d'un NIR :

- l'ensemble des personnes né en France métropolitaine ou dans un DROM, à leur naissance sur la base des actes de naissance établis par les officiers d'état civil ;
- les personnes nées à l'étranger ou dans les COM, suite à leur affiliation auprès d'un organisme de protection sociale.

Le NIR est pérenne, il reste définitivement attribué à la personne et à elle seule, et en cas très exceptionnel de changement de NIR le lien avec le NIR précédent est conservé.

3.1.2. Composition

La forme du NIR est spécifiée par le décret n° 82-103 du 22 janvier 1982 [D82-103].

Le NIR est formé de 13 caractères (chiffres ou lettres) :

- le sexe (1'chiffre)
- l'année de naissance (2 chiffres)
- le mois de naissance (2 chiffres)
- le lieu de naissance (5 caractères)
  Attention : dans certains cas les caractères ne sont pas représentatifs d'une codification géographique (c'est le cas, par exemple, pour certains nouveau-nés afin d'éviter des collisions avec des personnes nées cent ans auparavant ou pour les usagers de même sexe dont le rang de naissance est supérieur à 999 dans le même lieu de naissance pour les même mois et année de naissance)
- les 3 chiffres suivants correspondent à un numéro d'ordre qui permet de distinguer les personnes nées au même lieu à la même période.

Une clé de contrôle à 2 chiffres complète le NIR.

Le matricule INS est composé des 13 caractères et de la clé de contrôle.

3.1.3. Usages

Il existe plusieurs usages du NIR, qui ne se limitent pas à une seule sphère d'utilisation (ainsi par exemple le NIR est utilisé comme identifiant par la plupart des organismes de protection sociale, dans le cadre de la relation employeur-employé, etc.).

Dans le cadre du présent référentiel, il convient de distinguer deux finalités d'usages en raison de leur proximité :

- le NIR en tant que matricule INS associé aux traits d'identité, pour référencer les données de santé dans le cadre de la prise en charge sanitaire et médico-sociale Dans ce contexte d'usage, le NIR considéré est celui de l'usager, c'est-à-dire de la personne prise en charge (bénéficiaire des soins) ;

- le NIR dans le processus de remboursement des frais relatifs à la prise en charge de l'usager par l'Assurance Maladie. Par exemple, dans le cas du régime général de sécurité sociale, le NIR utilisé pour le remboursement est celui de l'ouvrant droit (qui peut être différent de celui de l'usager).

Le présent référentiel concerne uniquement les conditions et modalités d'utilisation du NIR en tant que matricule de l'identité nationale de santé pour référencer des données de santé dans un contexte de prise en charge sanitaire et médico-social des personnes.

En outre, le présent référentiel ne concerne pas les conditions et modalités d'utilisation du NIR dans le cadre de projets de recherche, finalité couverte par les dispositions du dernier alinéa de l'article 30 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, et autorisée dans les conditions prévues à la section 3 du chapitre III du titre II de la même loi.

> *« L'utilisation de l'identifiant national de santé ne peut avoir d'autre objet que ceux mentionnés au premier alinéa, sauf traitement de l'identifiant de santé à des fins de recherche dans le domaine de la santé tel que mentionné au dernier alinéa de l'article 30 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, et autorisé dans les conditions prévues à la section 3 du chapitre III du titre II de la même loi ».*
>
> *📖 Article R.1111-8-2 du CSP*

3.2. Le numéro d'immatriculation d'attente (NIA)

> *« I. - […] Pour les personnes en instance d'attribution d'un numéro d'inscription au répertoire national d'identification des personnes physiques et jusqu'à l'attribution de ce numéro, le matricule de l'identifiant national de santé est le numéro d'immatriculation d'attente (NIA), attribué par la Caisse nationale d'assurance vieillesse des travailleurs salariés à partir des données d'état civil et mentionné au 1° de l'article R. 114-26 du code de la sécurité sociale. »*
>
> *📖 Article R.1111-8-1 du CSP*

Pour toute personne qui ne dispose pas encore de NIR et pour laquelle une procédure d'affectation de NIR est en cours, le numéro d'immatriculation d'attente (NIA) attribué au cours de cette procédure doit être utilisé comme matricule de l'identité nationale de santé.

Dans la très grande majorité des cas, le NIA est identique au NIR qui sera affecté à la personne. Dans le cas exceptionnel où la procédure de vérification des pièces justificatives fait apparaître la nécessité de correction d'éléments d'identité ayant un impact sur le NIR, le NIR attribué est différent du NIA. Dans tous les cas, le lien entre le NIR et le NIA est conservé dans les bases de référence.

4. MESURES JURIDIQUES

4.1. Cadre juridique à respecter

L'utilisation d'un identifiant est prévue dans le règlement européen sur la protection des données personnelles[1]. En application de ce même texte (article 87), les États membres qui font le choix de mettre en place un numéro d'identification national peuvent préciser les conditions spécifiques du traitement de ce numéro. Au surplus, le fait de procéder au référencement des données de santé avec l'INS constitue un traitement au sens de l'article 4 du règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données – « RGPD ») et de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (dite loi Informatique et Libertés – LIL).

Pour ces motifs, le numéro d'identification national n'est utilisé que sous réserve des garanties appropriées pour les droits et libertés de la personne concernée.

Pour déterminer les garanties appropriées pour référencer des données de santé avec l'INS, les règles applicables aux données de santé doivent être prises en compte. Les données de santé sont des données à caractère personnel particulièrement protégées dans la mesure où elles ont trait à la vie privée de la personne concernée. Elles font donc l'objet de mesures juridiques et de sécurité particulières dont le respect doit être assuré par chaque responsable de service numérique en santé.

Ainsi, à titre d'illustration, le responsable de traitement de données de santé est tenu de respecter le règlement européen sur la protection des données personnelles, la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et, le cas échéant selon son statut juridique, la Politique générale de sécurité des systèmes d'information en santé (PGSSI-S), la Politique de sécurité des systèmes d'information pour les ministères chargés des affaires sociales (PSSI-MCAS) et les règles applicables dans le cadre du Référentiel Général de Sécurité (RGS) et, d'une manière plus générale, les référentiels adoptés en application de l'article L. 1470-5 du code de la santé publique.

Par ailleurs, des règles spécifiques peuvent être définies en fonction de la finalité du service numérique en santé (dossier du patient, dispositif de télémédecine, etc.) dans lequel est réalisé le référencement des données de santé avec l'INS.

4.2. Nature juridique du matricule INS

Le matricule INS est une donnée à caractère personnel, identifiante.

[1] Extrait du Considérant n°35 du RGPD : *« Les données à caractère personnel concernant la santé devraient comprendre l'ensemble des données se rapportant à l'état de santé d'une personne concernée qui révèlent des informations sur l'état de santé physique ou mentale passé, présent ou futur de la personne concernée. Cela comprend des informations sur la personne physique collectées lors de l'inscription de cette personne physique en vue de bénéficier de services de soins de santé ou lors de la prestation de ces services au sens de la directive 2011/24/UE du Parlement européen et du Conseil (9) au bénéfice de cette personne physique ; un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l'identifier de manière unique à des fins de santé ; »*

Le matricule INS n'est pas en lui-même une donnée de santé. Cependant, dès qu'il est associé à une donnée de santé, le régime juridique de la donnée de santé s'applique à lui, en tenant compte de son contexte d'usage, par exemple au sein d'un dossier patient informatisé. C'est en ce sens que les garanties appropriées à cet ajout sont liées aux garanties apportées pour protéger les données de santé qui ont vocation à être référencées avec le matricule INS.

En outre, des règles spécifiques ont été fixées par le législateur français pour encadrer le recours au NIR comme matricule de l'identité nationale de santé explicitées dans le présent référentiel.

Le fait de n'indexer les données de santé que sur le matricule INS (c'est-à-dire en ôtant toute référence à d'autres éléments identifiants tels que le nom, le prénom…) **maintient le caractère personnel et identifiant de ces données, qui ne sauraient être considérées comme pseudonymisées dans ce cas**.

4.3. Régime juridique applicable au référencement des données avec l'INS

Le régime juridique applicable au référencement est constitué de l'ensemble des exigences suivantes à mettre en œuvre :

1) Identifier le(s) responsable(s) de la prise en compte des exigences juridiques et de leur mise en œuvre.
2) Respecter l'obligation de référencer les données avec l'INS (sauf dans le cas d'une dérogation légale).
3) Respecter la liste des données concernées par l'opération de référencement.
4) Transmettre les données référencées avec l'INS uniquement aux acteurs légitimes à en être destinataires.
5) Respecter les droits des personnes dont les données sont référencées avec l'INS.
6) Respecter la durée de conservation.

L'ensemble de ces exigences sont décrites ci-dessous :

4.3.1. Identification du responsable de la prise en compte des exigences juridiques et de leur mise en œuvre

Identification du responsable en application du code de la santé publique

En application des règles du code de la santé publique, le responsable du respect des exigences juridiques propres au référencement des données de santé avec l'INS fait obligatoirement partie du **cercle des acteurs de confiance** délimité à l'article R. 1111-8-3 du CSP.

En dehors de ce cercle de confiance, le référencement de données avec l'INS est interdit, sauf pour les acteurs disposant d'un fondement législatif ou réglementaire spécifique (ex : Mon espace santé, Appli carte Vitale, etc.).

> *« Le référencement de données mentionnées à l'article R. 1111-8-2 à l'aide de l'identifiant national de santé ne peut être réalise que par des professionnels, établissements, services et organismes mentionnés à l'article L. 1110-4 et par des professionnels constituant une équipe de soins en application de l'article L. 1110-12 et intervenant dans la prise en charge sanitaire ou médico-sociale de la personne concernée […] »*
>
> *📖 Article R. 1111-8-3 du CSP*

« Toute personne prise en charge par un professionnel de santé, un établissement ou service, un professionnel ou organisme concourant à la prévention ou aux soins dont les conditions d'exercice ou les activités sont régies par le présent code, le service de santé des armées, un professionnel du secteur médico-social ou social ou un établissement ou service social et médico-social mentionné au I de l'article L. 312-1 du code de l'action sociale et des familles […] »

📖 Article L. 1110-4 du CSP

« Pour l'application du présent titre, l'équipe de soins est un ensemble de professionnels qui participent directement au profit d'un même patient à la réalisation d'un acte diagnostique, thérapeutique, de compensation du handicap, de soulagement de la douleur ou de prévention de perte d'autonomie, ou aux actions nécessaires à la coordination de plusieurs de ces actes, et qui :

1° Soit exercent dans le même établissement de santé, au sein du service de santé des armées, dans le même établissement ou service social ou médico-social mentionné au I de l'article L. 312-1 du code de l'action sociale et des familles ou dans le cadre d'une structure de coopération, d'exercice partagé ou de coordination sanitaire ou médico-sociale figurant sur une liste fixée par décret

2° Soit se sont vu reconnaître la qualité de membre de l'équipe de soins par le patient qui s'adresse à eux pour la réalisation des consultations et des actes prescrits par un médecin auquel il a confié sa prise en charge

3° Soit exercent dans un ensemble, comprenant au moins un professionnel de santé, présentant une organisation formalisée et des pratiques conformes à un cahier des charges fixé par un arrêté du ministre chargé de la santé. »

📖 Article L. 1110-12 du CSP

En raison de la nécessité de protéger les données de santé et d'éviter une propagation non maîtrisée de l'INS, son recours n'est rendu possible – et même obligatoire – qu'au profit de catégories d'acteurs constituant un cercle de confiance dont les contours sont réglementairement définis.

Le cercle de confiance est une notion fonctionnelle qui permet d'exprimer le fait que l'obligation d'utiliser l'INS pèse sur une communauté fermée d'acteurs directement concernés par la finalité attachée à l'INS c'est-à-dire les acteurs participant à la prise en charge sanitaire ou au suivi médico-social des personnes.

Exigence n°1

[EXI 01] Chaque acteur impliqué dans le référencement des données de santé à caractère personnel doit s'interroger sur l'obligation de recourir à l'INS (et a contrario sur le fait qu'il puisse ne pas avoir le droit d'utiliser l'INS) au regard de son appartenance au cercle de confiance ; de la finalité du référencement dans un objectif de prise en charge sanitaire ou médico-sociale ; de la nécessité à procéder à un tel référencement et de l'absence d'obstacle à ce référencement.

Identification du responsable en application de la législation relative à la protection des données personnelles

Le responsable du respect des exigences juridiques propres au référencement des données de santé avec l'INS est dénommé responsable de traitement s'il est responsable de la finalité et des moyens mis en œuvre

pour réaliser le traitement que constitue l'opération de référencement des données de santé. Il peut déléguer l'opération de référencement des données de santé avec l'INS à un sous-traitant.

Le contrat qui définit le rôle du sous-traitant doit préciser les conditions et modalités dans lesquelles le sous-traitant agit au nom et pour le compte du responsable de traitement afin de procéder au référencement des données de santé avec l'INS. Le contrat doit formaliser l'engagement du sous-traitant à être conforme au présent référentiel, et décrire les catégories de mesures mises en place pour en assurer le respect.

La responsabilité conjointe prévue à l'article 26 du RGPD peut être mise en œuvre, à condition que soit identifié que l'un des responsables de traitements fait partie du cercle de confiance.

En synthèse, les principaux acteurs de la chaîne de référencement sont :

1) *Le responsable de traitement au sein duquel le référencement avec l'INS est opéré.*
   Exemples : le directeur d'un établissement de santé pour un dossier patient informatisé, le médecin libéral pour son dossier médical géré par un logiciel de gestion de cabinet, le pharmacien pour son dossier dans son logiciel de gestion d'officine, etc.
2) *Le responsable du référencement* : Il s'agit dans la grande majorité des cas de la même personne que le responsable du traitement de données de santé à caractère personnel. Cependant, il peut également s'agir d'un prestataire en lien contractuel avec le responsable de traitement ; ce contrat formalisera s'il agit en qualité de *sous-traitant* ou de *responsable conjoint*.
3) *L'éditeur de la solution logicielle ayant pour finalité le traitement de données de santé* : il fournit une solution intégrant l'INS. Il est dans une position de prestataire ; le contrat qui le lie avec le responsable de traitement devra préciser le cas échéant s'il manipule des données personnelles et dans ce cas, s'il concourt à l'opération de référencement.
4) *Le ministère chargé de la santé et la Cnam*, co-responsables du « téléservice INSi », mis à disposition opérationnellement par la Cnam conformément à l'article R. 1111-8-6 du code de la santé publique.
5) *L'assurance maladie* responsable de l'Appli carte Vitale.

Chaque acteur a vocation à assumer ses responsabilités dans la chaîne de gestion des données référencées par l'INS conformément à la réglementation sur la protection des données personnelles (RGPD et loi « informatique et libertés ») et aux dispositions du code de la santé publique.

RESPONSABLE DE TRAITEMENT

*«**Responsable du traitement**», la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre; »*

📖 Article 4.7 du RGPD

RESPONSABLES CONJOINTS

*« 1. Lorsque deux responsables du traitement ou plus déterminent **conjointement** les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement. Les responsables conjoints du traitement définissent de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences du présent règlement, notamment en ce qui concerne l'exercice des droits de la personne concernée, et*

leurs obligations respectives quant à la communication des informations visées aux articles 13 et 14, par voie d'accord entre eux, sauf si, et dans la mesure, où leurs obligations respectives sont définies par le droit de l'Union ou par le droit de l'État membre auquel les responsables du traitement sont soumis. Un point de contact pour les personnes concernées peut être désigné dans l'accord.

*2. **L'accord** visé au paragraphe 1 reflète dûment les rôles respectifs des responsables conjoints du traitement et leurs relations vis-à-vis des personnes concernées. Les grandes lignes de l'accord sont mises à la disposition de la personne concernée.*

3. Indépendamment des termes de l'accord visé au paragraphe 1, la personne concernée peut exercer les droits que lui confère le présent règlement à l'égard de et contre chacun des responsables du traitement. »

📖 Article 26 du RGDP

SOUS-TRAITANT

« 1. Lorsqu'un traitement doit être effectué pour le compte d'un responsable du traitement, celui-ci fait uniquement appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée. »

📖 Article 28 du RGPD

*« Les données à caractère personnel ne peuvent faire l'objet d'une opération de traitement de la part d'un **sous-traitant**, d'une personne agissant sous l'autorité du responsable du traitement ou de celle du sous-traitant, que sur instruction du responsable du traitement.*

Toute personne traitant des données à caractère personnel pour le compte du responsable du traitement est considérée comme un sous-traitant au sens de la présente loi.

Le sous-traitant doit présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité mentionnées à l'article 34. Cette exigence ne décharge pas le responsable du traitement de son obligation de veiller au respect de ces mesures.

*Le **contrat** liant le sous-traitant au responsable du traitement comporte l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données et prévoit que le sous-traitant ne peut agir que sur instruction du responsable du traitement. »*

📖 Article 35 du RGPD

Exigence n°2

[EXI 02] Si le responsable du référencement des données avec l'INS a recours à un sous-traitant ou s'il agit en tant que co-responsable de ce traitement, il est tenu de préciser la répartition des rôles et responsabilités ainsi que l'étendue des droits et obligations de chaque partie prenante dans un contrat. Le contrat doit formaliser l'engagement du sous-traitant à être conforme au présent référentiel, et décrire les catégories de mesures mises en place pour en assurer le respect.

4.3.2. Obligation de référencer les données avec l'INS et dérogations légales

L'ensemble des acteurs faisant partie du cercle de confiance décrit au point 4.3.1 sont tenus de référencer les données de santé et les données administratives des personnes prises en charge à des fins sanitaires ou

médico-sociales. L'INS ne peut être utilisée à d'autres fins que le référencement de ces données pour ces finalités.

Fondement légal de l'obligation dans le Code de la santé publique

L'utilisation du numéro d'inscription au répertoire national d'identification des personnes physiques comme matricule de l'identité nationale de santé des personnes pour leur prise en charge à des fins sanitaires et médico-sociales est obligatoire en application de l'article L. 1111-8-1 du code de la santé publique.

> *« Le numéro d'inscription au répertoire national d'identification des personnes physiques est utilisé comme identifiant de santé des personnes pour leur prise en charge à des fins sanitaires et médico-sociales, dans les conditions prévues à l'article L. 1110-4 »*
>
> 🕮 *Article L.1111-8-1 du CSP*
>
> *« L'utilisation de l'identifiant national de santé ne peut avoir d'autre objet que ceux mentionnés au premier alinéa, sauf traitement de l'identifiant de santé à des fins de recherche dans le domaine de la santé tel que mentionné au dernier alinéa de l'article 30 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, et autorisé dans les conditions prévues à la section 3 du chapitre III du titre II de la même loi. »*
>
> 🕮 *Article R.1111-8-2 du CSP*

Dérogation légale de l'obligation dans le Code de la santé publique

Le législateur a prévu un cas de dérogation à l'obligation d'utiliser l'INS en raison d'un obstacle légitime de procéder au référencement. Il s'agit du cas dans lequel il est impossible de procéder au référencement, par exemple dans le cas d'une prise en charge en urgence.

En outre, la dérogation à l'obligation légale d'utiliser l'INS peut provenir d'un texte s'opposant à l'identification (exemple : texte imposant l'anonymat).

Il appartient donc au professionnel sur qui pèse l'obligation de procéder au référencement de vérifier qu'il ne se trouve pas dans un cas de dérogation.

> *« Le numéro d'inscription au répertoire national d'identification des personnes physiques est utilisé comme identifiant de santé des personnes pour leur prise en charge à des fins sanitaires et médico-sociales, dans les conditions prévues à l'article L. 1110-4 »* 🕮 *Article L.1111-8-1 du CSP*
>
> *« II.-Tout autre identifiant ne peut être utilisé pour le référencement des données de santé qu'en cas d'impossibilité de pouvoir accéder à l'identifiant national de santé, afin de ne pas empêcher la prise en charge sanitaire et médico-sociale des personnes. Il est procédé au référencement des données mentionnées à l'article R. 1111-8-2 avec l'identifiant national de santé dès qu'il est possible d'y accéder.*
>
> *III.- Lorsque l'identification d'une personne par un professionnel, un établissement, un service ou organisme mentionné à l'article R. 1111-8-3, est nécessaire pour sa prise en charge à des fins sanitaires ou médico-sociales, cette identification ne peut être faite que par l'identifiant national de santé […] »*
>
> 🕮 *Article R.1111-8-1 du CSP*

Fondement de la licéité de l'utilisation de l'INS et du référencement des données de santé en application de la LIL/RGPD

L'opération de référencement résultant de la mise en œuvre de l'obligation légale de référencer les données de santé avec l'INS constitue un traitement licite.

> *Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie :*
>
> *c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;* 🕮 *Article 6 du RGPD*

Exigence n°3

[EXI 03] Un acteur est tenu de référencer les données de santé avec l'INS au titre de son appartenance au cercle de confiance et du respect de la finalité d'une prise en charge sauf s'il se trouve dans un cas de dérogation légale. Il lui revient alors la charge de pouvoir le justifier.

Imbrication du traitement de référencement dans un traitement de données de santé

L'opération de référencement des données de santé avec l'INS s'inscrit dans la majorité des configurations dans un traitement de données de santé plus large ayant une finalité s'inscrivant nécessairement dans le domaine de la prise en charge sanitaire ou médico-sociale (mise en œuvre d'un dossier patient informatisé, traitement d'imagerie médicale, télésurveillance, …).

Lorsque le responsable du référencement des données de santé avec l'INS, appartenant au cercle de confiance, diffère du responsable du traitement des données de santé, le partage des rôles et des responsabilités entre eux doit être explicité et formalisé dans un contrat, notamment pour préciser la répartition des obligations à respecter au titre de la législation relative à l'INS et de la loi Informatique et libertés modifiée.

Au surplus, l'utilisation doit rester conforme à la finalité du référencement, c'est-à-dire exclusivement sanitaire ou médico-sociale. Outre la prise en charge médicale et le suivi médico-social de la personne, cette utilisation peut concerner les fonctions nécessaires pour assurer le suivi social ou la gestion administrative des personnes prises en charge.

> *L'utilisation de données de santé et de données administratives référencées avec l'identifiant national de santé n'est autorisée dans le cadre d'un traitement de données à caractère personnel que si les deux conditions suivantes sont remplies : 1° Le traitement a une finalité exclusivement sanitaire ou médico-sociale, y compris les fonctions nécessaires pour assurer le suivi social ou la gestion administrative des personnes prises en charge ; 2° Le traitement est mis en œuvre dans le respect des dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.*
>
> 🕮 *Article R1111-8-4 CSP*

4.3.3. Catégories de données concernées (INS et éléments d'identité)

Les catégories de données concernées par l'opération de référencement des données de santé sont recensées à l'article R. 1111-8-2 du code de la santé publique. Seules ces catégories de données sont concernées par l'obligation légale d'utiliser l'INS pour les référencer.

1/ Le matricule INS

L'obligation de référencement par le matricule INS (R. 1111-8-3 III) n'implique pas de supprimer tout autre identifiant local (exemple : IPP) pour le remplacer par l'INS.

Il est rappelé que la législation relative à la protection des données personnelles prévoit un principe de minimisation des données.

Aussi, il appartient au responsable du référencement de documenter les motifs justifiant la coexistence de plusieurs identifiants et de veiller à prendre les mesures de sécurité adaptées. Le recours à l'INS est obligatoire depuis le 1er janvier 2021. Le maintien des identifiants locaux permet notamment de gérer :

- la priorité donnée à la prise en charge de toute personne (y compris celles qui ne disposent pas de matricule INS comme les touristes, ou les personnes arrivant en état d'urgence dont on ignore l'identité…) ;
- les cas d'indisponibilité des téléservices ou motif légitime invoqué par les acteurs de la prise en charge et faisant obstacle à une association immédiate ;
- les situations non liées à la prise en charge sanitaire ou médico-sociale (ex : identifiants utilisés pour la gestion hôtelière…).

2/ Les éléments d'identité ou traits d'identité [2]

Les éléments d'identité mentionnés à l'article R. 1111-8-6 du CSP sont :

- le nom de naissance ;
- la liste des prénoms de naissance ;
- le sexe ;
- la date de naissance ;
- le lieu de naissance (code géographique officiel).

3/ Les données de santé et les données administratives

Il s'agit des données de santé et des données administratives de toute personne bénéficiant ou appelée à bénéficier d'un acte diagnostique, thérapeutique, de prévention, de soulagement de la douleur, de compensation du handicap ou de prévention de la perte d'autonomie, ou d'interventions nécessaires à la coordination de plusieurs de ces actes.

Le responsable du référencement doit associer l'INS à toute donnée de santé à caractère personnel produite par son SIS, y compris les données historisées.

[2] Par convention dans ce document, le terme trait d'identité désigne les éléments d'identité mentionnés à l'article R.1111-8-6 du CSP.

Sont inclus dans les données administratives les traits d'identité provenant des bases de référence nationales.

Exigence n°4
[EXI 04] Chaque acteur tenu d'utiliser l'INS doit limiter son usage au seul référencement des données de santé et administratives des personnes prises en charge.

4.3.4. Catégorie des acteurs légitimes à être destinataires des données référencées avec l'INS

Pour rappel, conformément aux dispositions de l'article L. 1110-4 du CSP, les données de santé ne peuvent être échangées que par les acteurs faisant partie du cercle de confiance. Dès lors, le responsable du référencement des données de santé avec l'INS (matricule INS et traits des bases nationales de référence : nom de naissance, liste des prénoms de naissance, date de naissance, sexe, code géographique officiel du lieu de naissance) doit veiller à ne pas communiquer les données ainsi référencées à des destinataires n'ayant pas à en connaitre.

Exigence n°5
[EXI 05] L'émetteur de données référencées avec l'INS doit s'assurer que le destinataire fait partie du cercle de confiance.
I.- Toute personne prise en charge par un professionnel de santé, un établissement ou service, un professionnel ou organisme concourant à la prévention ou aux soins dont les conditions d'exercice ou les activités sont régies par le présent code, le service de santé des armées, un professionnel du secteur médico-social ou social ou un établissement ou service social et médico-social mentionné au I de l'article L. 312-1 du code de l'action sociale et des familles a droit au respect de sa vie privée et du secret des informations la concernant. *Excepté dans les cas de dérogation expressément prévus par la loi, ce secret couvre l'ensemble des informations concernant la personne venue à la connaissance du professionnel, de tout membre du personnel de ces établissements, services ou organismes et de toute autre personne en relation, de par ses activités, avec ces établissements ou organismes. Il s'impose à tous les professionnels intervenant dans le système de santé.* *II.- Un professionnel peut échanger avec un ou plusieurs professionnels identifiés des informations relatives à une même personne prise en charge, à condition qu'ils participent tous à sa prise en charge et que ces informations soient strictement nécessaires à la coordination ou à la continuité des soins, à la prévention ou à son suivi médico-social et social.* *III.- Lorsque ces professionnels appartiennent à la même équipe de soins, au sens de l'article L. 1110-12, ils peuvent partager les informations concernant une même personne qui sont strictement nécessaires à la*

coordination ou à la continuité des soins ou à son suivi médico-social et social. Ces informations sont réputées confiées par la personne à l'ensemble de l'équipe.

Le partage, entre des professionnels ne faisant pas partie de la même équipe de soins, d'informations nécessaires à la prise en charge d'une personne requiert son consentement préalable, recueilli par tout moyen, y compris de façon dématérialisée, dans des conditions définies par décret pris après avis de la Commission nationale de l'informatique et des libertés.

III bis.- Un professionnel de santé, exerçant au sein du service de santé des armées ou dans le cadre d'une contribution au soutien sanitaire des forces armées prévue à l'article L. 6147-10, ou un professionnel du secteur médico-social ou social relevant du ministre de la défense peuvent, dans des conditions définies par décret en Conseil d'Etat, échanger avec une ou plusieurs personnes, relevant du ministre de la défense ou de la tutelle du ministre chargé des anciens combattants, et ayant pour mission exclusive d'aider ou d'accompagner les militaires et anciens militaires blessés, des informations relatives à ce militaire ou à cet ancien militaire pris en charge, à condition que ces informations soient strictement nécessaires à son accompagnement. Le secret prévu au I s'impose à ces personnes. Un décret en Conseil d'Etat définit la liste des structures dans lesquelles exercent les personnes ayant pour mission exclusive d'aider ou d'accompagner les militaires et anciens militaires blessés.

IV.- La personne est dûment informée de son droit d'exercer une opposition à l'échange et au partage d'informations la concernant. Elle peut exercer ce droit à tout moment.

V.- Le fait d'obtenir ou de tenter d'obtenir la communication de ces informations en violation du présent article est puni d'un an d'emprisonnement et de 15 000 euros d'amende.

En cas de diagnostic ou de pronostic grave, le secret médical ne s'oppose pas à ce que la famille, les proches de la personne malade ou la personne de confiance définie à l'article L. 1111-6 reçoivent les informations nécessaires destinées à leur permettre d'apporter un soutien direct à celle-ci, sauf opposition de sa part. Seul un médecin est habilité à délivrer, ou à faire délivrer sous sa responsabilité, ces informations.

Le secret médical ne fait pas obstacle à ce que les informations concernant une personne décédée soient délivrées à ses ayants droit, son concubin ou son partenaire lié par un pacte civil de solidarité, dans la mesure où elles leur sont nécessaires pour leur permettre de connaître les causes de la mort, de défendre la mémoire du défunt ou de faire valoir leurs droits, sauf volonté contraire exprimée par la personne avant son décès. Toutefois, en cas de décès d'une personne mineure, les titulaires de l'autorité parentale conservent leur droit d'accès à la totalité des informations médicales la concernant, à l'exception des éléments relatifs aux décisions médicales pour lesquelles la personne mineure, le cas échéant, s'est opposée à l'obtention de leur consentement dans les conditions définies aux articles L. 1111-5 et L. 1111-5-1.

VI.- Les conditions et les modalités de mise en œuvre du présent article pour ce qui concerne l'échange et le partage d'informations entre professionnels de santé, non-professionnels de santé du champ social et médico-social et personnes ayant pour mission exclusive d'aider ou d'accompagner les militaires et anciens

militaires blessés sont définies par décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés.

📖 *Article L. 1110-4 du CSP*

4.3.5. Droits des personnes dont les données sont référencées avec l'INS

Absence de droit d'opposition

Les personnes dont les données sont référencées avec l'INS peuvent exercer les droits qu'elles détiennent en application du régime juridique applicable aux services numériques en santé utilisant l'INS. Des règles particulières ont été fixées concernant les droits de ces personnes à l'égard de l'opération de référencement des données de santé avec l'INS.

Il est réglementairement prévu que la personne concernée ne dispose pas de droit d'opposition au référencement de ses données de santé avec l'INS, afin de ne pas risquer de paralyser l'obligation d'utiliser l'INS. Pour autant, le droit d'opposition existe toujours, pour motif légitime, au profit de la personne concernée à l'égard par exemple de son dossier patient informatisé.

Droit à l'information

L'usager concerné par le référencement de ses données de santé avec son INS doit être informé de l'utilisation de l'INS par le responsable de l'obligation de référencement, qui doit tenir compte de son contexte d'usage.

Aussi, l'information doit porter sur la présentation des objectifs poursuivis par l'utilisation de l'INS et sur l'absence de droit d'opposition. Cette information doit être un élément d'une information plus large, délivrée au titre des modalités de prise en charge sanitaire ou du suivi médico-social dont la personne fait l'objet.

Informations à fournir lorsque des données à caractère personnel sont collectées auprès de la personne concernée

1. Lorsque des données à caractère personnel relatives à une personne concernée sont collectées auprès de cette personne, le responsable du traitement lui fournit, au moment où les données en question sont obtenues, toutes les informations suivantes :

a) l'identité et les coordonnées du responsable du traitement et, le cas échéant, du représentant du responsable du traitement ;

b) le cas échéant, les coordonnées du délégué à la protection des données ;

c) les finalités du traitement auquel sont destinées les données à caractère personnel ainsi que la base juridique du traitement ;

d) lorsque le traitement est fondé sur l'article 6, paragraphe 1, point f), les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers ;

e) les destinataires ou les catégories de destinataires des données à caractère personnel, s'ils existent ; et

f) le cas échéant, le fait que le responsable du traitement a l'intention d'effectuer un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale, et l'existence ou l'absence

d'une décision d'adéquation rendue par la Commission ou, dans le cas des transferts visés à l'article 46 ou 47, ou à l'article 49, paragraphe 1, deuxième alinéa, la référence aux garanties appropriées ou adaptées et les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition;

2. En plus des informations visées au paragraphe 1, le responsable du traitement fournit à la personne concernée, au moment où les données à caractère personnel sont obtenues, les informations complémentaires suivantes qui sont nécessaires pour garantir un traitement équitable et transparent :

a) la durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ;

b) l'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, la rectification ou l'effacement de celles-ci, ou une limitation du traitement relatif à la personne concernée, ou du droit de s'opposer au traitement et du droit à la portabilité des données ;

c) lorsque le traitement est fondé sur l'article 6, paragraphe 1, point a), ou sur l'article 9, paragraphe 2, point a), l'existence du droit de retirer son consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci ;

d) le droit d'introduire une réclamation auprès d'une autorité de contrôle ;

e) des informations sur la question de savoir si l'exigence de fourniture de données à caractère personnel a un caractère réglementaire ou contractuel ou si elle conditionne la conclusion d'un contrat et si la personne concernée est tenue de fournir les données à caractère personnel, ainsi que sur les conséquences éventuelles de la non-fourniture de ces données ;

f) l'existence d'une prise de décision automatisée, y compris un profilage, visée à l'article 22, paragraphes 1 et 4, et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.

3. Lorsqu'il a l'intention d'effectuer un traitement ultérieur des données à caractère personnel pour une finalité autre que celle pour laquelle les données à caractère personnel ont été collectées, le responsable du traitement fournit au préalable à la personne concernée des informations au sujet de cette autre finalité et toute autre information pertinente visée au paragraphe 2.

4. Les paragraphes 1, 2 et 3 ne s'appliquent pas lorsque, et dans la mesure où, la personne concernée dispose déjà de ces informations.

📖 Article13 du RGPD

<u>Informations à fournir lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée</u>

1. Lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée, le responsable du traitement fournit à celle-ci toutes les informations suivantes :

a) l'identité et les coordonnées du responsable du traitement et, le cas échéant, du représentant du responsable du traitement ;

b) le cas échéant, les coordonnées du délégué à la protection des données ;

c) les finalités du traitement auquel sont destinées les données à caractère personnel ainsi que la base juridique du traitement ;

d) les catégories de données à caractère personnel concernées ;

e), le cas échéant, les destinataires ou les catégories de destinataires des données à caractère personnel;

f) le cas échéant, le fait que le responsable du traitement a l'intention d'effectuer un transfert de données à caractère personnel à un destinataire dans un pays tiers ou une organisation internationale, et l'existence ou l'absence d'une décision d'adéquation rendue par la Commission ou, dans le cas des transferts visés à l'article 46 ou 47, ou à l'article 49, paragraphe 1, deuxième alinéa, la référence aux garanties appropriées ou adaptées et les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition;

2. En plus des informations visées au paragraphe 1, le responsable du traitement fournit à la personne concernée les informations suivantes nécessaires pour garantir un traitement équitable et transparent à l'égard de la personne concernée :

a) la durée pendant laquelle les données à caractère personnel seront conservées ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ;

b) lorsque le traitement est fondé sur l'article 6, paragraphe 1, point f), les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers ;

c) l'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, la rectification ou l'effacement de celles-ci, ou une limitation du traitement relatif à la personne concernée, ainsi que du droit de s'opposer au traitement et du droit à la portabilité des données ;

d) lorsque le traitement est fondé sur l'article 6, paragraphe 1, point a), ou sur l'article 9, paragraphe 2, point a), l'existence du droit de retirer le consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci ;

e) le droit d'introduire une réclamation auprès d'une autorité de contrôle ;

f) la source d'où proviennent les données à caractère personnel et, le cas échéant, une mention indiquant qu'elles sont issues ou non de sources accessibles au public ;

g) l'existence d'une prise de décision automatisée, y compris un profilage, visée à l'article 22, paragraphes 1 et 4, et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.

3. Le responsable du traitement fournit les informations visées aux paragraphes 1 et 2 :

a) dans un délai raisonnable après avoir obtenu les données à caractère personnel, mais ne dépassant pas un mois, eu égard aux circonstances particulières dans lesquelles les données à caractère personnel sont traitées ;

b) si les données à caractère personnel doivent être utilisées aux fins de la communication avec la personne concernée, au plus tard au moment de la première communication à ladite personne ; ou

c) s'il est envisagé de communiquer les informations à un autre destinataire, au plus tard lorsque les données à caractère personnel sont communiquées pour la première fois.

4. Lorsqu'il a l'intention d'effectuer un traitement ultérieur des données à caractère personnel pour une finalité autre que celle pour laquelle les données à caractère personnel ont été obtenues, le responsable du traitement fournit au préalable à la personne concernée des informations au sujet de cette autre finalité et toute autre information pertinente visée au paragraphe 2.

5. Les paragraphes 1 à 4 ne s'appliquent pas lorsque et dans la mesure où :

a) la personne concernée dispose déjà de ces informations ;

b) la fourniture de telles informations se révèle impossible ou exigerait des efforts disproportionnés, en particulier pour le traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques sous réserve des conditions et garanties visées à l'article 89, paragraphe 1, ou dans la mesure où l'obligation visée au paragraphe 1 du présent article est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement. En pareils cas, le responsable du traitement prend des mesures appropriées pour protéger les droits et libertés ainsi que les intérêts légitimes de la personne concernée, y compris en rendant les informations publiquement disponibles ;

c) l'obtention ou la communication des informations sont expressément prévues par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis et qui prévoit des mesures appropriées visant à protéger les intérêts légitimes de la personne concernée ; ou

d) les données à caractère personnel doivent rester confidentielles en vertu d'une obligation de secret professionnel réglementée par le droit de l'Union ou le droit des États membre, y compris une obligation légale de secret professionnel.

📖 Article14 du RGPD

Exigence n°6

[EXI 06] Les responsables du référencement doivent informer les personnes concernées que leurs données de santé sont référencées avec l'INS et qu'elles ne disposent pas de droit d'opposition, mais de droits d'accès, de rectification et de limitation.

4.3.6. Durée de conservation

Pour déterminer la durée de conservation de l'INS, le responsable de l'obligation de référencement doit tenir compte de son contexte d'usage et des outils mis en œuvre pour tracer cette prise en charge ou ce suivi. L'INS permettant le référencement des données recensées au point 4.3.3 du présent référentiel, elle doit être conservée aussi longtemps que les données qu'elle référence.

Ainsi, par exemple, lorsque l'opération de référencement est réalisée dans le référentiel d'identité d'un établissement de santé, la durée de conservation est fixée à l'article R. 1112-7 du code de la santé publique (en moyenne 20 ans).

En tout état de cause, une durée de conservation doit impérativement être fixée en application de la loi informatique et libertés modifiée et du RGPD.

Exigence n°7

[EXI 07] Les responsables du référencement doivent fixer la durée de conservation de l'INS en fonction de son contexte d'usage. L'INS étant utilisée pour référencer des données, sa durée de conservation doit être identique à celle des données qu'elle référence.

5. MESURES DE SECURITE LIEES AU REFERENCEMENT DES DONNEES DE SANTE PAR L'INS

L'adjonction de l'INS dans des bases de données constitutives de traitement(s) de données de santé apporte un risque complémentaire sur l'ensemble du traitement qu'il convient de circonscrire.

Dans la mesure où l'opération de référencement s'inscrit dans une base de données constitutive d'un traitement de données de santé dont la finalité répond à un objectif de prise en charge et dont les utilisateurs sont les professionnels, établissements et services mentionnés à l'article R. 1111-8-3, **le responsable de ce traitement devra inclure et appliquer les mesures du présent référentiel dans son analyse de risque et son analyse d'impact relative à la protection des données.**

C'est pourquoi le présent référentiel impose des exigences à prendre en compte dans les analyses de risques et l'analyse d'impact relative à la protection des données.

Il est possible que le responsable des données de santé référencées avec l'INS diffère du responsable de l'opération de référencement, dans ce cas, il importe de décrire la répartition des rôles de façon formalisée entre les responsables.

5.1. Réalisation ou mise à jour de l'analyse d'impact relative à la protection des données (AIPD)

Au titre des garanties exigées pour protéger les données de santé qui ont vocation à être référencées avec l'INS, l'article 35 du RGPD prévoit la conduite d'une analyse d'impact relative à la protection des données (ou étude d'Impact sur la vie privée – ou Privacy Impact Assessment), lorsqu'un traitement de données personnelles est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées.

La CNIL énonce[3] que « généralement, les traitements qui remplissent au moins deux des critères suivants doivent faire l'objet d'une analyse d'impact » :

- collecte de données sensibles ;
- collecte de données personnelles à large échelle.

Par exemple, le DPI tenu par un établissement de santé devrait faire l'objet d'une AIPD intégrant la description de l'analyse relative à l'utilisation de l'INS pour référencer les données de santé.

Le responsable de traitement est tenu par l'obligation de s'assurer de la conformité de son traitement au RGPD.

S'il a désigné un délégué à la protection des données, il lui demande conseil et le charge de vérifier l'exécution de l'AIPD.

Si un sous-traitant intervient dans le traitement, il doit fournir son aide et les informations nécessaires à la réalisation de l'AIPD.

[3] https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-lanalyse-dimpact-relative-la-protection-des-donnees-aipd

Le responsable de traitement devrait également demander l'avis des personnes concernées (par le biais d'une enquête, d'un sondage, d'une question formelle aux représentants du personnel), ou le justifier sinon.

Idéalement, les métiers (maîtrise d'ouvrage), les équipes chargées de la mise en œuvre (maîtrise d'œuvre), et la personne chargée de la sécurité des systèmes d'information devraient également participer au processus de réalisation de l'AIPD et à sa validation.

Il convient de consulter la CNIL lorsque l'AIPD indique que le niveau de risque résiduel reste élevé. Dans ce cas, l'AIPD est transmise à la CNIL.

Il faut également transmettre son AIPD :

- quand la législation nationale d'un État membre l'exige ;
- en cas de contrôle par la CNIL.

1. Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires.

📖 Article 35 du RGPD

Exigence n°8

[EXI 08] Les mesures mises en œuvre pour veiller au respect du présent référentiel doivent être formalisées notamment pour en attester, par exemple dans les documents établis dans le cadre de l'analyse d'impact sur la vie privée.

5.2. Homologation de sécurité

Le référencement des données avec l'INS nécessite une mise à jour de l'analyse de risques et, le cas échéant, son homologation de sécurité. L'AIPD peut être intégrée à l'analyse de risque globale.

Le cloisonnement des données fait partie des bonnes pratiques de sécurité informatique. Il est nécessaire d'assurer un équilibre entre les avantages fonctionnels à référencer directement un jeu de données avec l'INS et les risques pour les personnes concernées en cas de violation de ces données.

Les grandes catégories de risques à réviser, suite à l'arrivée de l'INS, par les responsables du référencement sont :

- l'impossibilité d'accéder aux données (données de santé, matricule INS et traits des bases nationales de référence) (perte de disponibilité) ;
  - les cas de perte de disponibilité sont distingués selon qu'ils relèvent de l'accès au SI de santé ou de l'accès aux téléservices ;

- la bonne association entre l'INS et les éléments d'identité est effectuée par les personnes chargées du référencement à l'aide du téléservice INSi, sauf en cas d'indisponibilité des téléservices ou motif légitime invoqué par ces personnes faisant obstacle à une association immédiate.

► la modification des données (données de santé, INS) (perte d'intégrité) ;
- les mesures appliquées aux données de santé doivent également être appliquées à l'INS ;
- des mesures spécifiques à la gestion de l'INS (cf. chapitre « 5.4 Mesures minimales à mettre en œuvre pour l' » de ce présent référentiel) doivent également être appliquées ;
- des mesures spécifiques à l'identitovigilance (cf. chapitre « 5.4.1 Gestion de l'identité » du présent référentiel) ;

► l'accès non autorisé aux données (données de santé, INS) (perte de confidentialité) ;
- les mesures appliquées aux données de santé doivent également être appliquées à l'INS ;
- la politique de contrôle d'accès doit être revue (cf. chapitre « 5.5.3 Contrôle d'accès » du présent référentiel) ;
- des mesures spécifiques d'authentification doivent être appliquées (cf. chapitre « 5.5.3 Contrôle d'accès » du présent référentiel) ;

► l'impossibilité d'imputer des actions effectuées sur les données (données de santé, INS) (perte d'auditabilité).
- des mesures spécifiques de traçabilité doivent être mises en place (cf. chapitre « 5.4.3 Traçabilité » du présent référentiel).

Exigence n°9

[EXI 09] Le responsable du référencement des données de santé doit justifier du respect des mesures du présent référentiel. Ces mesures peuvent figurer sur l'homologation de sécurité que le responsable du référencement peut avoir à réaliser (ou à mettre à jour).

5.3. Qualification de l'INS

5.3.1. Récupération de l'INS

Pour récupérer l'INS (matricule INS et les traits d'identité des bases nationales de référence), les acteurs du cercle de confiance ont deux possibilités :

1) Appeler le téléservice INSi (cf. chapitre 5.3.2 de ce présent référentiel) :
   - Par une opération de recherche du téléservice INSi ;
   - Par une opération de vérification du téléservice INSi suite à un échange avec un acteur du cercle de confiance, éventuellement après avoir saisi manuellement le matricule INS et les traits d'identité.
     Dans ce dernier cas la vérification du matricule INS et des traits d'identité grâce au téléservice de vérification est obligatoire. La bonne association entre l'identité nationale de santé et les éléments d'identité est effectuée par les ouvrant-droit chargées du référencement à l'aide des téléservices

d'accès ou de vérification, sauf en cas d'indisponibilité des téléservices ou motif légitime invoqué par ces personnes faisant obstacle à une association immédiate.

2) Utiliser l'Appli carte Vitale

L'Appli carte Vitale est une version dématérialisée de la carte Vitale permettant notamment l'identification électronique de l'utilisateur de l'application, à distance ou en présentiel, à différents services numériques. Elle permet de récupérer l'INS (matricule + traits d'identité), directement au statut « qualifiée » pour les utilisateurs de l'application et, le cas échéant, pour ses ayants droit.

Le professionnel peut alors intégrer l'INS de l'usager depuis son logiciel, par scan du QR code ou lecture NFC, ou grâce à l'authentification à distance si l'usager réalise des démarches en ligne.

5.3.2. Téléservice INSi

« Des téléservices permettent aux professionnels, établissements, services ou organismes mentionnés à l'article R. 1111-8-3 d'accéder au numéro d'inscription au répertoire national des personnes physiques et de vérifier son exactitude dans le respect du référentiel mentionné à l'article R. 1111-8-7. Ils sont mis en œuvre par la Caisse nationale de l'assurance maladie.

« Le référencement des données de santé nécessite l'association de l'identifiant national de santé et d'éléments d'identité provenant du répertoire national d'identification des personnes physiques. Ces éléments d'identité sont précisés par le référentiel mentionné à l'article R. 1111-8-7. La bonne association entre l'identifiant national de santé et les éléments d'identité est effectuée par les personnes chargées du référencement en application du premier alinéa à l'aide des téléservices d'accès ou de vérification, sauf en cas d'indisponibilité des téléservices ou motif légitime invoqué par ces personnes faisant obstacle à une association immédiate. Les téléservices comprennent plusieurs modalités d'accès, dont l'accès par lecture électronique de la carte mentionnée à l'article L. 161-31 du code de la sécurité sociale du bénéficiaire des actes, dénommée carte d'assurance maladie ou dite "carte vitale", ou d'autres modalités présentant des garanties équivalentes, définies dans le référentiel mentionné à l'article R. 1111-8-7 »

« Le recours aux téléservices n'exonère pas les personnes susmentionnées de mettre en place toute procédure de surveillance, de correction et de prévention des erreurs relevant de l'organisation de la prise en charge des personnes et concourant à la maîtrise du risque d'erreur dans l'identification des personnes. »

📖 *Art. R. 1111-8-6 du CSP*

L'appel au TLS n'est requis que dans le cas où la personne chargée du référencement n'a pas récupéré l'INS de la personne prise en charge depuis son Appli carte Vital. (cf. 5.3.1 de ce présent référentiel)

Opérations de recherche et modalités d'accès

Le téléservice mis en œuvre par la Cnam permet de récupérer l'INS du RNIPP (ou une copie conforme du RNIPP tel le SNGI) selon deux modalités d'accès :

- opération n°1 : accès à l'INS via le téléservice INSi en utilisant la Carte Vitale comme intermédiaire pour identifier l'usager. À noter que les traits d'identité remontés par le téléservice sont ceux des bases de référence et non les données de la carte Vitale (la carte Vitale est utilisée pour éviter les erreurs de saisie) ;

- opération n°2 : accès à l'INS via le téléservice INSi en saisissant certains traits d'identité de la personne (en absence de la Carte Vitale).
  - Traits obligatoires pour l'appel de récupération :
    - le nom de naissance
    - le 1er prénom de naissance
    - la date de naissance
    - le sexe

Les téléservices de récupération permettront de récupérer, outre le matricule INS, les traits d'identité suivants :

- le nom de naissance ;
- la liste des prénoms de naissance ;
- le sexe ;
- la date de naissance ;
- le lieu de naissance (code officiel géographique).

Pour la récupération de l'INS, l'usage n°1 est à privilégier pour éviter les situations où plusieurs usagers correspondraient aux mêmes traits d'identité, et les échecs de récupération du fait d'erreurs de saisie.

Opération de vérification et modalités d'accès

Le téléservice mis en œuvre par la Cnam permet également la vérification de l'INS.

- opération n°3 : vérification de l'INS

Les traits d'identité obligatoires pour vérifier le matricule INS et les traits d'identité sont :

- le nom de naissance ;
- un des prénoms de naissance ;
- le sexe ;
- la date de naissance.

L'opération de vérification permet de s'assurer que l'ensemble constitué du matricule INS et des quatre traits obligatoires est cohérent et à jour.

Cette vérification est possible selon deux « modalités d'appel » : unitaire ou en masse.

Indisponibilité et motif légitime

Un motif légitime est un cas de force majeure ou un événement à la fois insurmontable et échappant au contrôle de la personne devant référencer la donnée de santé avec l'INS.

5.3.3. Mesures de qualification de l'INS

La qualité de l'identification des usagers est garantie d'une part par la bonne identification des usagers (par le biais de procédures d'identitovigilance rigoureuses) et d'autre part par la récupération de données d'identité de référence.

De plus, pour assurer la qualité du matricule INS, *« le référencement des données de santé nécessite l'association du matricule identité nationale de santé et d'éléments d'identité provenant du répertoire*

national d'identification des personnes physiques ». Pour cette raison le téléservice INSi fournit les traits d'identité des bases nationales de référence (RNIPP ou copie conforme très récente) pour compléter le matricule INS et ainsi former l'INS.

Pour renforcer la sécurité du bon référencement entre un usager et son matricule INS, la notion d'INS qualifiée a donc été créée dans le cadre de ce référentiel.

Un matricule INS et les traits d'identité sont qualifiés (INS au statut « identité qualifiée ») s'ils réunissent les deux conditions suivantes :

- l'identité de la personne a été validée en respectant des procédures d'identitovigilance ;
- l'INS (matricule INS et les traits d'identité associés) a été récupérée auprès des bases de référence au travers du téléservice INSi ou de l'Appli carte Vitale pour les utilisateurs de l'application et, le cas échéant, pour ses ayants droit.

Le Référentiel national d'identitovigilance définit les règles permettant de définir le statut de l'INS(cf ANNEXES).

Exigence n°10

[EXI 10] L'INS doit être qualifiée dès que possible, c'est-à-dire faire l'objet d'une validation de l'identité de l'usager avec des procédures d'identitovigilance et d'une récupération auprès du téléservice INSi. L'INS qualifiée peut également être récupérée de l'Appli carte Vitale pour les utilisateurs de l'application et, le cas échéant, pour ses ayants droit.

Certains acteurs appartenant au cercle de confiance et tenus par l'obligation de référencer les données de santé avec l'INS ne rencontrent pas nécessairement l'usager physiquement (exemple : anatomo-pathologistes, médecin requis en télé-expertise, etc.), il n'en demeure pas moins que « *le recours aux téléservices n'exonère pas les personnes susmentionnées de mettre en place toute procédure de surveillance, de correction et de prévention des erreurs relevant de l'organisation de la prise en charge des personnes et concourant à la maîtrise du risque d'erreur dans l'identification des personnes*. »).

5.3.4. Qualification à la réception de données médicales, en cas d'identité non préalablement qualifiée par le destinataire

Exigence n°11

[EXI 11] En cas de réception d'une INS non préalablement qualifiée par le destinataire, ce dernier doit effectuer la qualification (procédure d'identitovigilance et appel au téléservice INSi) sauf contractualisation expresse avec l'émetteur.

5.4. Mesures minimales à mettre en œuvre pour l'INS

5.4.1. Gestion de l'identité

Les mesures à mettre en œuvre pour assurer la bonne identification de la personne concernée relèvent de la responsabilité du responsable du référencement. Elles sont décrites dans le Référentiel national d'identitovigilance (RNIV).

Néanmoins, il convient de s'assurer que les exigences suivantes sont respectées :

Exigences n°12 et n°13 : gestion de l'INS

[EXI 12] Une INS non qualifiée ne doit pas être véhiculée en interne ou vers l'extérieur.

[EXI 13] Sauf exceptions identifiées dans le Référentiel national d'identitovigilance, le matricule INS et les traits d'identité de référence provenant du téléservice INSi ne devront pas être modifiés localement.

Exigences n°14 et n°15 : échange et partage avec l'INS

[EXI 14] Dans le cadre d'échanges et de partages de données de santé, l'INS (matricule INS et les traits d'identité des bases de référence) doit être utilisée pour référencer ces données dès lors qu'elle a pu être préalablement qualifiée.

[EXI 15] Dans le cadre d'échanges et de partage de données de santé, les traits d'identité issus des bases nationales de référence doivent obligatoirement être envoyés avec le matricule INS/OID : nom de naissance, le premier prénom de naissance, la liste des prénoms, la date de naissance, le sexe et le lieu de naissance.

Exigences n°16, n°17, 18, n°19 et n°20 : mesures techniques facilitant la gestion de l'INS

[EXI 16] Dès lors que l'INS d'un usager a été qualifiée, le matricule INS et les traits d'identité provenant des bases de référence doivent être utilisés pour l'identification de l'usager, notamment lors des échanges de données de santé le concernant. D'autres identifiants nécessaires à la coordination des échanges peuvent continuer à être transmis s'ils sont strictement nécessaires.

[EXI 17] Les traits d'identité, provenant des bases de référence, récupérés du téléservice INSi doivent remplacer, si cela n'est pas déjà le cas, les traits stricts locaux dans les champs correspondants.

[EXI 18] Le matricule INS et les traits d'identité doivent être accompagnés d'informations confirmant qu'ils ont été qualifiés.

[EXI 19] A l'issue d'un délai paramétrable (à partir de la date d'acquisition), l'opération de vérification du téléservice doit être rappelée pour contrôler l'INS. Ce délai, de l'ordre de 5 ans, doit être défini par le responsable de l'opération de référencement en fonction des usages et du contexte. Cette vérification peut utilement être réalisée à l'occasion d'un épisode de prise en charge ou d'une interaction avec l'usager (identification électronique sur un portail, mise à jour du dossier administratif, etc.).

[EXI 20] L'historique des matricules INS d'une personne doit être conservé (conservation des matricules INS successifs d'une personne, NIA puis NIR et de manière exceptionnelle changement de NIR).

Exigences n°21 et n°22 : Gestion des erreurs liées à l'INS

[EXI 21] Une traçabilité des partenaires avec lesquels des échanges ou des partages de données de santé avec l'INS ont été réalisés doit être mise en œuvre.

[EXI 22] Dans le cas où une rectification de tout ou partie de l'INS est nécessaire, une mesure doit être prévue afin d'assurer la propagation de l'information aux acteurs et aux systèmes auxquels les données ont été transmises conformément à l'article 19 du RGPD

Sensibiliser les utilisateurs de traitements référençant l'INS aux bonnes pratiques élémentaires de sécurité informatique

Chaque utilisateur de traitements référençant l'INS doit, dès son arrivée, être sensibilisé aux bonnes pratiques élémentaires de sécurité informatique. Il doit être informé des enjeux de sécurité, des règles à respecter et des bons comportements à adopter en matière de sécurité des systèmes d'information.

De la sensibilisation autour de l'INS devra être réalisée afin d'aborder *a minima* :

- les objectifs et enjeux de l'INS et du matricule INS, à distinguer des autres usages potentiels du NIR ;
- les règlements et obligations concernés ;
- les consignes de sécurité.

Exigence n°23

[EXI 23] Une mesure de sensibilisation de toutes les personnes qui interviennent dans le référencement de l'identité de l'usager doit être prévue (en particulier sur la distinction à effectuer entre matricule INS et NIR). Cette mesure doit faire l'objet d'une documentation.

5.4.2. Contrôle d'accès

Le responsable du référencement des données de santé avec l'INS doit assurer la continuité du contrôle d'accès à l'INS (base locale contenant les INS, téléservice INSi). Il est garant de toutes les actions qui consistent à sécuriser les accès, notamment au téléservice INSi. Il est responsable de tout mésusage ou infraction concernant l'INS qui serait causée par le non-respect des exigences du présent référentiel ou de négligences dans leur mise en œuvre au sein du traitement référençant l'INS.

Exigence n°24

[EXI 24] La politique de contrôle d'accès doit être revue en prenant en compte l'ajout de l'INS et si nécessaire les accès au téléservice INSi.

Gestion des habilitations

Il est nécessaire :

- de définir quelles populations ou quels processus automatisés sont autorisés à effectuer les différentes opérations du téléservice INSi ;
- de contrôler strictement l'accès au téléservice INSi, en s'assurant que les utilisateurs sont correctement identifiés électroniquement et disposent d'autorisations d'accès légitimes ;
- d'empêcher la dispersion et la duplication de l'INS au sein de traitements non maîtrisés ou soumis à un contrôle d'accès moins strict.

Il convient de noter que les personnes pouvant accéder à l'INS peuvent être différentes des personnes pouvant accéder aux données de santé (exemple : personnel administratif d'un établissement).

Revue des habilitations

Exigence n°25

[EXI 25] Dans la mesure où un service numérique en santé dans lequel s'inscrit l'opération de référencement de données de santé avec l'INS comporte d'autres fonctionnalités ou des fonctionnalités accessibles à des acteurs ne participant pas à la prise en charge (gestion hôtelière, tableaux de pilotage…), le responsable de traitement doit s'assurer de la partition des traitements, des risques et des mesures appropriées notamment dans la gestion des habilitations.

En particulier, la gestion des habilitations et les modalités d'identification électronique des personnes ou des processus automatisés pouvant accéder à l'INS doivent être documentées afin de pouvoir contrôler leur conformité aux référentiels de sécurité applicables.

Des revues régulières des habilitations doivent être menées afin de vérifier que les habilitations attribuées sont toujours justifiées, que les fins d'accès exceptionnels et les retraits d'habilitation liés aux départs ou aux changements de fonction du personnel ont bien été pris en compte, et d'activer le cas échéant les mesures correctives nécessaires.

Identification électronique au téléservice INSi

Plusieurs modalités d'identification électronique permettant d'effectuer les opérations du téléservice INSi sont mises en place :

- une identification électronique des professionnels personnes physiques grâce à leur carte professionnelle sécurisée nominative (CPx nominative) ou à travers du fédérateur de moyens d'identification électronique Pro Santé Connect permettant notamment une identification électronique par CPx nominative et par e-CPS ;
- une identification électronique des professionnels personnes morales grâce à l'utilisation de certificats logiciels de type certificat de personne morale organisation.

Ces identifications reposent sur les produits de certification d'identité provenant de l'autorité IGC-Santé, maintenue par l'Agence du Numérique en Santé.

Afin d'être en mesure d'identifier tout accès frauduleux ou utilisation abusive de données personnelles, ou de déterminer l'origine d'un incident, il est impératif pour l'organisme qui référence les données de santé avec l'INS de mettre en place un mécanisme de traçabilité des transactions effectuées via le téléservice INSi. Ce dispositif doit permettre d'enregistrer et de conserver l'identifiant, la date et l'heure de connexion, la date et l'heure de leur déconnexion et le détail des actions effectuées par l'utilisateur ou le processus à l'origine de l'appel. Ces données ne doivent en principe pas être conservées plus de 6 mois selon les préconisations actuelles de la CNIL. Des procédures de supervision détaillant les modalités de surveillance de ces journaux d'événements pour y détecter automatiquement et/ou manuellement d'éventuelles anomalies ainsi que les conséquences qui s'y attachent, doivent être mises en place. Ces

journaux doivent être disponibles sous 48h en cas de contrôle ou d'investigation par les autorités compétentes.

Cette gestion des traces doit être documentée.

Ces mesures relèvent de la responsabilité directe du responsable de traitement au sein duquel le référencement avec l'INS est opéré. Il lui appartient en effet de s'assurer de la conformité des conditions de mise en œuvre opérationnelle des opérations de référencement et du respect des règles effectives d'accès et de traçabilité rappelées dans le présent référentiel.

Exigence n°26

[EXI 26] L'identification électronique au téléservice INSi s'effectue grâce à un produit de certification de l'autorité de certification IGC-Santé. Cela concerne notamment les cartes CPx nominatives et le fédérateur Pro Santé Connect pour les professionnels personnes physiques, ainsi que les certificats logiciels de type organisation pour les professionnels personnes morales.

Au sein des différents traitements référençant l'INS, l'identification électronique des personnes, physiques ou morales, pouvant y accéder doit être conforme aux référentiels de sécurité en vigueur.

Exigences n°27 et n° 28

[EXI 27] Tout accès à l'INS doit être tracé conformément aux mesures prévues pour garantir la sécurité des données à caractère personnel au titre de la conformité au RGPD.

[EXI 28] En cas d'accès au téléservice INSi par certificat de personne morale, les traces mises en œuvre dans le système appelant le téléservice INSi doivent être conservées pendant la durée préconisée par la CNIL en la matière (actuellement cette durée est fixée à 6 mois) et comporter l'identification nominative de la personne physique ou du processus automatisé à l'origine de l'accès au téléservice. Une analyse régulière de ces traces doit être prévue et réalisée, afin de détecter d'éventuelles anomalies. Cette mesure doit faire l'objet d'une documentation.

5.4.3. Traçabilité

Système de détection d'intrusion

Un système de détection d'intrusion doit être mis en place afin de détecter d'éventuels dysfonctionnements ou tentatives d'accès illicites aux données.

Traçabilité des accès à l'identité qualifiées (matricule INS et traits d'identité (modification, consultation)

Outre le mécanisme de journalisation des appels au téléservice INSi qui doit être mis en place par l'organisme responsable du référencement de l'INS, il est indispensable que cet organisme mette également en œuvre un dispositif assurant la traçabilité des accès aux INS.

Exigence n°29

[EXI 29] Au sein de l'organisme qui référence l'INS, tout accès à l'INS doit être tracé conformément aux mesures prévues pour garantir la sécurité des données à caractère personnel au titre de la conformité au RGPD.

Procéder à des contrôles et audits de sécurité réguliers

La réalisation d'audits réguliers (au moins une fois par an) du système d'information est essentielle car elle permet d'évaluer concrètement l'efficacité des mesures mises en œuvre et leur maintien dans le temps. Ces contrôles et audits permettent également de mesurer les écarts pouvant persister entre la règle et la pratique. Ces contrôles permettront de tester si les mesures de sécurité appliquées suite à l'arrivée de l'INS sont suffisantes pour couvrir les risques associés.

5.4.4. Sécurité des communications

Sécuriser les canaux informatiques (réseaux)

Exigence n°30

[EXI 30] La sécurité des canaux de communication utilisés pour échanger des données de santé comportant l'INS doit être adaptée pour garantir la sécurité de ces données.

5.4.5. Auto homologation téléservice INSi

L'auto-homologation téléservice INSi décrite en annexe 6.4 est une procédure interne, menée par le responsable du référencement (acteur de la prise en charge), préalablement au référencement des données de santé avec l'INS grâce au téléservice INSi.

Exigence n°31

[EXI 31] L'auto-homologation téléservice INSi est obligatoire pour les personnes morales recourant à une identification électronique au moyen d'un certificat logiciel de type organisation pour appeler le téléservice INSi.

La procédure d'auto-homologation téléservice INSi est également recommandée pour les autres acteurs responsables de référencement de l'INS appelant le téléservice INSi.

5.5. Synthèse des exigences

5.5.1. Conformité

▶ [EXI 01] Chaque acteur impliqué dans le référencement des données de santé à caractère personnel doit s'interroger sur l'obligation de recourir à l'INS (et a contrario sur le fait qu'il puisse ne pas avoir le droit d'utiliser l'INS) au regard de son appartenance au cercle de confiance ; de la finalité du

référencement dans un objectif de prise en charge sanitaire ou médico-sociale ; de la nécessité à procéder à un tel référencement et de l'absence d'obstacle à ce référencement.

▶ [EXI 02] Si le responsable du référencement des données avec l'INS a recours à un sous-traitant ou s'il agit en tant que co-responsable de ce traitement, il est tenu de préciser la répartition des rôles et responsabilités ainsi que l'étendue des droits et obligations de chaque partie prenante dans un contrat. Le contrat doit formaliser l'engagement du sous-traitant à être conforme au présent référentiel, et décrire les catégories de mesures mises en place pour en assurer le respect.

▶ [EXI 03] Un acteur est tenu de référencer les données de santé avec l'INS au titre de son appartenance au cercle de confiance et du respect de la finalité d'une prise en charge sauf s'il se trouve dans un cas de dérogation légale. Il lui revient alors la charge de pouvoir le justifier.

▶ [EXI 04] Chaque acteur tenu d'utiliser l'INS doit limiter son usage au seul référencement des données de santé et administratives des personnes prises en charge.

▶ [EXI 05] L'émetteur de données référencées avec l'INS doit s'assurer que le destinataire fait partie du cercle de confiance.

▶ [EXI 06] Les responsables du référencement doivent informer les personnes concernées que leurs données de santé sont référencées avec l'INS et qu'elles ne disposent pas de droit d'opposition, mais de droits d'accès, de rectification et de limitation.

▶ [EXI 07] Les responsables du référencement doivent fixer la durée de conservation de l'INS en fonction de son contexte d'usage. L'INS étant utilisée pour référencer des données, sa durée de conservation doit être identique à celle des données qu'elle référence.

▶ [EXI 08] Les mesures mises en œuvre pour veiller au respect du présent référentiel doivent être formalisées notamment pour en attester, par exemple dans les documents établis dans le cadre de l'analyse d'impact sur la vie privée.

▶ [EXI 09] Le responsable du référencement des données de santé doit justifier du respect des mesures du présent référentiel. Ces mesures peuvent figurer sur l'homologation de sécurité que le responsable du référencement peut avoir à réaliser (ou à mettre à jour).

5.5.2. Gestion de l'identité et identitovigilance

▶ [EXI 10] L'INS doit être qualifiée dès que possible, c'est-à-dire faire l'objet d'une validation de l'identité de l'usager avec des procédures d'identitovigilance et d'une récupération auprès du téléservice INSi. L'INS qualifiée peut également être récupérée de l'Appli carte Vitale pour les utilisateurs de l'application et, le cas échéant, pour ses ayants droit.

▶ [EXI 11] En cas de réception d'une INS non préalablement qualifiée par le destinataire, ce dernier doit effectuer la qualification (procédure d'identitovigilance et appel au téléservice) sauf contractualisation expresse avec l'émetteur.

▶ [EXI 12] Une INS non qualifiée ne doit pas être véhiculée en interne ou vers l'extérieur.

▶ [EXI 13] Sauf exceptions identifiées dans le Référentiel national d'identitovigilance, le matricule INS et les traits d'identité de référence provenant du téléservice INSi ne devront pas être modifiés localement.

▶ [EXI 14] Dans le cadre d'échanges et de partages de données de santé, l'INS (matricule INS et les traits d'identité des bases de référence) doit être utilisée pour référencer ces données dès lors qu'elle a pu être préalablement qualifiée.

▶ [EXI 15] Dans le cadre d'échanges et de partage de données de santé, les traits d'identité issus des bases nationales de référence doivent obligatoirement être envoyés avec le matricule INS : nom de naissance, le premier prénom de naissance, la liste des prénoms, la date de naissance, le sexe et le lieu de naissance.

▶ [EXI 16] Dès lors que l'INS d'un usager a été qualifiée, le matricule INS et les traits d'identité provenant des bases de référence doivent être utilisés pour l'identification de l'usager, notamment lors des échanges de données de santé le concernant. D'autres identifiants nécessaires à la coordination des échanges peuvent continuer à être transmis s'ils sont strictement nécessaires.

▶ [EXI 17] Les traits d'identité, provenant des bases de référence, récupérés du téléservice INSi doivent remplacer, si cela n'est pas déjà le cas, les traits stricts locaux dans les champs correspondants.

▶ [EXI 18] Le matricule INS et les traits d'identité doivent être accompagnés d'informations confirmant qu'ils ont été qualifiés.

▶ [EXI 19] A l'issue d'un délai paramétrable (à partir de la date d'acquisition), l'opération de vérification du téléservice doit être rappelée pour contrôler l'INS. Ce délai, de l'ordre de 5 ans, doit être défini par le responsable de l'opération de référencement en fonction des usages et du contexte. Cette vérification peut utilement être réalisée à l'occasion d'un épisode de prise en charge ou d'une interaction avec l'usager (identification électronique sur un portail, mise à jour du dossier administratif, etc.).

▶ [EXI 20] L'historique des matricules INS d'une personne doit être conservé (conservation des matricules INS successifs d'une personne, NIA puis NIR et de manière exceptionnelle changement de NIR).

▶ [EXI 21] Une traçabilité des partenaires avec lesquels des échanges ou des partages de données de santé avec l'INS ont été réalisés doit être mise en œuvre.

▶ [EXI 22] Dans le cas où une rectification de tout ou partie de l'INS est nécessaire, une mesure doit être prévue afin d'assurer la propagation de l'information aux acteurs et aux systèmes auxquels les données ont été transmises conformément à l'article 19 du RGPD.

▶ [EXI 23] Une mesure de sensibilisation de toutes les personnes qui interviennent dans le référencement de l'identité de l'usager doit être prévue (en particulier sur la distinction à effectuer entre matricule INS et NIR). Cette mesure doit faire l'objet d'une documentation.

5.5.3. Contrôle d'accès

▶ [EXI 24] La politique de contrôle d'accès doit être revue en prenant en compte l'ajout de l'INS et si nécessaire les accès au téléservice INSi.

▶ [EXI 25] Dans la mesure où un service numérique en santé dans lequel s'inscrit l'opération de référencement de données de santé avec l'INS comporte d'autres fonctionnalités ou des fonctionnalités accessibles à des acteurs ne participant pas à la prise en charge (gestion hôtelière, tableaux de pilotage…), le responsable de traitement doit s'assurer de la partition des traitements, des risques et des mesures appropriées notamment dans la gestion des habilitations.
En particulier, la gestion des habilitations et les modalités d'identification électronique des personnes ou des processus automatisés pouvant accéder à l'INS doivent être documentées afin de pouvoir contrôler leur conformité aux référentiels de sécurité applicables.

▶ [EXI 26] L'identification électronique au téléservice INSi s'effectue grâce à un produit de certification de l'autorité de certification IGC-Santé. Cela concerne notamment les cartes CPx nominatives et le fédérateur Pro Santé Connect pour les professionnels personnes physiques, ainsi que les certificats logiciels de type organisation pour les professionnels personnes morales.
Au sein des différents traitements référençant l'INS, l'identification électronique des personnes, physiques ou morales, pouvant y accéder doit être conforme aux référentiels de sécurité en vigueur.

▶ [EXI 27] Tout accès à l'INS doit être tracé conformément aux mesures prévues pour garantir la sécurité des données à caractère personnel au titre de la conformité au RGPD.

▶ [EXI 28] En cas d'accès au téléservice INSi par certificat de personne morale, les traces mises en œuvre dans le système appelant le téléservice INSi doivent être conservées pendant la durée préconisée par la CNIL en la matière (actuellement cette durée est fixée à 6 mois) et comporter l'identification nominative de la personne physique ou du processus automatisé à l'origine de l'accès au téléservice. Une analyse régulière de ces traces doit être prévue et réalisée, afin de détecter d'éventuelles anomalies. Cette mesure doit faire l'objet d'une documentation.

▶ [EXI 29] Au sein de l'organisme qui référence l'INS, tout accès à l'INS doit être tracé conformément aux mesures prévues pour garantir la sécurité des données à caractère personnel au titre de la conformité au RGPD.

5.5.4. Sécurité de communication

▶ [EXI 30] La sécurité des canaux de communication utilisés pour échanger des données de santé comportant l'INS doit être adaptée pour garantir la sécurité de ces données.

5.5.5. Auto homologation téléservice INSi

▶ [EXI 31] L'auto-homologation téléservice INSi est obligatoire pour les personnes morales recourant à une identification électronique au moyen d'un certificat logiciel de type organisation pour appeler le téléservice INSi.

6. ANNEXES

6.1. Définitions des termes utilisés dans ce référentiel

Terme	Définition
Usager	Dans ce référentiel, le terme « **usager** » désigne toute personne physique bénéficiant ou appelée à bénéficier d'un acte diagnostique, thérapeutique, de prévention, de soulagement de la douleur, de compensation du handicap ou de prévention de la perte d'autonomie[4].
Personne	Dans le cadre de ce référentiel, le terme « personne », quand il est utilisé seul, désigne une personne physique.
Traits d'identité	Dans ce présent document, « éléments d'identité » et « traits d'identité » sont utilisés de façon similaire. Un trait d'identité est un élément caractérisant une personne mais qui n'est en règle générale pas suffisant à lui seul pour définir l'identité de cette personne. Les traits d'identité sont considérés au sens large et correspondent à l'ensemble de données collectées lors de l'enregistrement d'une personne physique ou morale. À titre d'exemple non limitatif, on peut citer : **pour les personnes physiques** : ► le nom de naissance ; ► les prénoms de naissance ; ► la date de naissance ; ► le sexe ; ► le lieu de naissance. En fonction du référentiel d'identités considéré, les traits d'identité collectés peuvent être plus ou moins nombreux et de nature diverse. Cependant, ils doivent être suffisants pour caractériser l'identité d'une personne, permettre de la différencier des autres personnes notamment celles qui partagent une partie de ces traits d'identité (ex. : homonymes) et ainsi faire un lien univoque entre un identifiant et l'identité de la personne à laquelle il a été attribué.

[4] Voir [CSP] article R.1111-8-2

Terme	Définition
Identifiant	Un identifiant est un attribut donné à une personne, en lien avec son identité, permettant de différencier deux personnes même dans le cas où leurs traits d'identité sont similaires ou très proches. Un identifiant est constitué selon des règles définies par l'autorité d'affectation. Il peut être constitué d'une suite de caractères numériques ou alphanumériques plus ou moins signifiants (numéro aléatoire, numéro déduit à partir de traits d'identité, concaténation de traits d'identité…). Il y a collision d'identifiants lorsqu'un même identifiant a été attribué à deux personnes différentes dans le même domaine d'identification. Il y a doublon d'identifiants lorsque plusieurs identifiants sont attribués à une même personne dans un même domaine d'identification. L'objectif de l'identification des personnes est d'attribuer un identifiant à chaque personne sans qu'il y ait doublon ni collision.
Type d'identifiant	Deux types d'identifiants peuvent être distingués selon les périmètres d'action des Autorités d'Enregistrement : 1) **Identifiant de portée nationale (ou identifiant « public »)** : l'identifiant de portée nationale est un identifiant attribué à la suite de l'enregistrement dans un référentiel d'identité national par une Autorité d'Enregistrement dûment habilitée (ex. matricule INS). 2) **Identifiant de portée locale (ou identifiant « privé »)** : l'identifiant de portée locale 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. Son utilisation est limitée aux finalités du référentiel (ex. IPP).
Bases nationales de référence	La notion « Bases nationales de référence » ou « Bases de référence » est utilisé pour mentionner le RNIPP ou le SNGI (ou toute copie conforme du RNIPP)
Identité	Ensemble de données, ou traits d'identité, qui constituent la représentation d'une personne physique. L'identité numérique correspond à la représentation d'un individu physique dans un système d'information. Un même usager physique peut ainsi être associé à plusieurs identités numériques selon le système d'information utilisé : employeur, impôts, sécurité sociale, mutuelle, banque, etc.

Terme	Définition
Identification	L'identification correspond aux opérations permettant d'établir l'identité d'un individu au regard de l'état-civil, de le reconnaître comme individu physique, de lui créer un dossier personnel papier et/ou numérique. En santé, on distingue 2 domaines complémentaires dans l'identification des usagers : ► l'identification primaire ; elle comprend l'ensemble des opérations destinées à attribuer à un usager physique, de manière univoque, une identité numérique qui lui est propre dans un système d'information de santé, qu'il s'agisse d'une première prise de contact avec l'usager ou d'une venue ultérieure ; elle recouvre les étapes de recherche, de création, de modification d'une identité ainsi que l'attribution d'un niveau de confiance aux données enregistrées ; ► l'identification secondaire ; elle correspond aux moyens mis en œuvre, à l'occasion de la prise en charge d'un usager physique (soin, administration médicamenteuse, prélèvement biologique, examen d'imagerie médicale, etc.), pour s'assurer que le bon soin sera délivré au bon patient ; elle consiste notamment à vérifier, à chaque étape de sa prise en charge, l'adéquation entre son identité réelle et celle présente sur les documents et outils de prise en charge (dossier physique ou informatique, prescription, étiquette, bon de transport, compte-rendu d'examen, etc.). Le règlement eIDas définit l'identification électronique comme le 'processus consistant à utiliser des données d'identification personnelle sous une forme électronique représentant de manière univoque une personne physique ou morale, ou une personne physique représentant une personne morale.
Identité nationale de santé (INS)	L'INS est une identité numérique qui repose sur les bases nationales de référence. Le terme INS désigne l'ensemble des informations suivantes : ► le matricule INS qui a pour valeur le NIR (ou le NIA) personnel de l'usager, sur 15 caractères ; ► les traits INS qui sont les traits d'identité de référence associés au NIR/NIA dans les bases de référence (nom de naissance, liste des prénom(s) de naissance, sexe, date de naissance et code officiel géographique du lieu de naissance) ; ► l'organisme qui a affecté l'INS, précisé sous la forme d'un OID (object identifier), information habituellement invisible pour le professionnel de santé (le NIR et le NIA ayant chacun leur autorité d'affectation, cela permet de les distinguer).
Domaine d'identification	Un domaine d'identification regroupe au sein d'une organisation toutes les applications qui utilisent le même identifiant pour désigner un patient. Exemples : ► un cabinet médical disposant d'un mode unique d'identification de ses patients est considéré comme un domaine d'identification ; ► un établissement de santé dont tous les logiciels utilisent le même identifiant est un domaine d'identification.
Matricule INS	Le terme matricule INS désigne le NIR ou le NIA utilisé en tant qu'identifiant national de santé.

6.2. Documents cités en référence

Document
Politique de sécurité des systèmes d'information pour les ministères chargés des affaires sociales (PSSI MCAS)
Politique générale de sécurité des systèmes d'information de santé (PGSSI-S)
Référentiel général de sécurité (RGS)
Référentiel National d'Identitovigilance (RNIV)
Guide d'implémentation de l'INS dans les logiciels

6.3. Glossaire

Sigle / Acronyme	Signification
AIPD	Analyse d'impact relative à la protection des données
ANS	Agence du Numérique en Santé
Cnam	Caisse nationale de l'assurance maladie
CNIL	Commission nationale de l'informatique et des libertés
COM	Collectivité d'Outre-mer
CSP	Code de la santé publique
DMP	Dossier médical partagé
DROM	Départements et régions d'Outre-mer
DPI	Dossier patient informatisé
INS	Identité nationale de santé
INSEE	Institut national de la statistique et des études économiques
IPP	Identifiant permanent du patient
NIA	Numéro d'immatriculation d'attente
NIR	Numéro d'inscription au RNIPP
OID	Identifiant d'objet (Object Identifier)
PGSSI-S	Politique générale de sécurité des systèmes d'information de santé
PSSI-MCAS	Politique de sécurité des systèmes d'information pour les ministères chargés des affaires sociales

Sigle / Acronyme	Signification
RNIPP	Répertoire national d'identification des personnes physiques
RNIV	Référentiel National d'Identitovigilance
RGPD	Règlement général sur la protection des données personnelles
RGS	Référentiel général de sécurité
SIS	Systèmes d'information de santé
SNGI	Système national de gestion des identités

6.4. Exigences de sécurité liées aux modalités d'appel du téléservice par certificat serveur à la conduite d'une « auto-homologation téléservice INSi »

L'auto-homologation téléservice INSi est une procédure interne, menée par un acteur de la prise en charge, préalablement à son référencement de l'INS au travers d'une intégration au téléservice INSi.

Classiquement, l'éditeur de logiciels sous-traitant de la personne morale peut accompagner son client dans la réalisation de cette auto-homologation et participer à la commission d'homologation. C'est néanmoins l'acteur de la prise en charge, responsable du référencement de l'INS, qui prononce et signe l'auto-homologation INSi.

D'un point de vue général, les acteurs pourront utilement s'inspirer des bonnes pratiques de l'ANSSI relatives à la démarche d'homologation d'un système d'information[5].

Pour l'auto-homologation INSi, cela consiste notamment à :

- préparer un support documentaire, à minima sous format d'une présentation synthétique et intelligible, qui sera revu par le représentant du responsable de référencement de l'INS,
- tenir une commission d'auto-homologation INSi, préalablement ou dans les deux mois qui suivent la mise en service du référencement, avec le représentant du responsable du référencement (directeur de l'établissement ou son représentant habilité), avec les acteurs pertinents (référent RGPD, référent métier sur l'identitovigilance, direction des systèmes d'information, direction de la sécurité, éditeur de la solution, représentants des patients, etc.) ;
- faire signer par le responsable du référencement le PV de la commission, avec la mention "le service est homologué pour [nombre] mois, [avec les (éventuelles) réserves suivantes : [réserves]]". La durée sera à l'appréciation du responsable du référencement qui pourra utilement prononcer une homologation courte si certaines réserves nécessitent de refaire un point à une brève échéance. Un rappel calendaire sera utilement programmé peu avant l'expiration pour organiser une nouvelle homologation ;

[5] Cf. https://www.ssi.gouv.fr/guide/lhomologation-de-securite-en-neuf-etapes-simples/

- ajouter le PV de la commission (avec le support documentaire de la commission en annexe) dans le registre RGPD, dans une catégorie spécifique au référencement de l'INS. Ce document est conservé et tenu à disposition des responsables du traitement relatif au téléservice INSi, d'une part, ainsi que de tout organisme officiel qui aurait à en connaître (CNIL, ANSSI, etc.).

Le support documentaire devra notamment faire état des points suivants :

- un récapitulatif des différents systèmes d'information qui feront appel au téléservice INSi, ou vers lesquels l'INS sera propagée lors de la qualification de l'INS ;
- pour chacun de ces traitements, et notamment pour ceux faisant appel direct au téléservice INSi, un rappel :
  - des modalités d'identification électronique à ces outils ;
  - des modalités de contrôle d'accès (habilitations) à ces outils, et de revue régulière de ces accès ;
  - des méthodes mises en œuvre pour assurer la traçabilité pendant au moins 6 mois : aux appels au téléservice INSi (par des professionnels ou des processus automatisés), et aux données d'identité.
- les trois risques principaux identifiés vis à vis du référencement de l'INS, leur probabilité et leur criticité, ainsi que les mesures mises en œuvre, à date ou dans le futur, pour les réduire au maximum ;
- les modalités de supervision prévues pour détecter des anomalies dans les appels au téléservice INSi (accès non autorisés au téléservice, temps de réponse anormaux, sollicitation excessive du téléservice, etc.) et sur un accès indésirable aux données d'identité des personnes (consultation excessive de dossiers, consultation du dossier de collègues, etc.) ;
- la procédure à suivre en cas de suspicion de violation de données.

6.5. Référentiel national d'identitovigilance

Les volets 1 à 4 du référentiel national d'identitovigilance, dans leur version de décembre 2024, sont annexés au présent référentiel.

6.6. Guide d'implémentation de l'INS dans les logiciels

Le guide d'implémentation de l'INS à l'attention des éditeurs de logiciels, dans sa version de décembre 2024, est annexé au présent référentiel.