AGENCE
DU NUMÉRIQUE
EN SANTÉ

Référentiel d'Interopérabilité et de Sécurité des Dispositifs Médicaux Numériques (DMN)

Statut : *Validé* | *Classification :* *Publique* | Version : *V1.2.2*

Agence du Numérique en Santé
9, rue Georges Pitard – 75015 Paris
T. 01 58 45 32 50
esante.gouv.fr

Historique du document			
Version	Date	Auteur	Commentaires
V0.1.0 Concertation	28/07/2022	ANS	Version pour concertation (DMN hors télésurveillance)
V0.2.0	08/12/2022	ANS	Version unifiée pour concertation (DMN dont DMN de télésurveillance) ▪ Modification de la partie « 2.1 Périmètre d'application du référentiel » ▪ Renumérotation des exigences dans la partie 2 suite à la suppression de l'exigence INS 36 dans le référentiel Excel ▪ Modification sur les profils : o Renommage du profil « Identification électronique des Usagers » en « Accès Usager » o Renommage du profil « Authentification électronique des Usagers - ApCV » en « Accès Usager - ApCV » (désormais optionnel) o Ajout d'un profil « Accès Professionnel » regroupant les exigences des sections « Annuaire Santé », « Pro Santé Connect (PSC) », et « Identification électronique des Acteurs des secteurs sanitaires, médico-social et social (ASPP) » (précédemment dans le profil « Général ») o Sortie de l'exigence INS 46 du profil « Général » et ajout de celle-ci au nouveau profil « Stockage des copies de titres d'identité » ▪ Mise à jour des informations sur l'annexe « ANA2 » ▪ Restructuration du document
V1.2.1	27/01/2023	ANS	▪ Correction du périmètre d'application du référentiel ▪ Correction des définitions dont : o Modification de la définition d'Editeur o Ajout de la définition de produit ▪ Correction des numéros de versions des différents documents mentionnés
V1.2.2	09/02/2023	ANS	▪ Précisions sur le périmètre d'application du référentiel ▪ Déplacement de blocs de la partie « Objet du référentiel » dans « Périmètre d'application du référentiel » ▪ Possibilité de ne pas activer systématiquement l'authentification des usagers à 2 facteurs dans certains cas.

Réglementation

Renvoi	Document
[ART_L1470]	Article L. 1470-5 du code de la santé publique https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000043497489
[RGDP]	Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27/04/2016 (« règlement général relatif à la protection des données ») https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679

[HDS]	Article L1111-8 du code de la santé publique https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006685779/2022-06-23/
[INS]	Arrêté du 27 mai 2021 portant approbation des modifications apportées au référentiel « Identifiant national de santé » https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043618501
[LFSS]	Article 36 - LOI n° 2021-1754 du 23 décembre 2021 de financement de la sécurité sociale pour 2022 https://www.legifrance.gouv.fr/jorf/article_jo/JORFARTI000044553494
[Art_L162-48]	Articles L. 162-48 à L. 162-57 du code de la sécurité sociale (issus de la LOI n° 2021-1754 du 23 décembre 2021 de financement de la sécurité sociale pour 2022) https://www.legifrance.gouv.fr/codes/id/LEGISCTA000044565906/
[MIE]	Arrêté du 4 avril 2022 relatif à des moyens d'identification électronique immatériels mis à disposition des professionnels, personnes physiques des secteurs sanitaire, social et médico-social pour l'utilisation des services numériques en santé. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045551195

TABLE DES MATIERES

DEFINITIONS

Sauf mention contraire, les termes et expressions commençant par une majuscule et employés dans le présent document ont la signification qui leur est attribuée ci-après :

Logiciel Dispositif Médical : Tout logiciel répondant à la définition du dispositif médical énoncée à l'article 2 du règlement (UE) 2017/745 et 2017/746 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, le règlement (CE) n° 178/2002 et le règlement (CE) n° 1223/2009 et abrogeant les directives du Conseil 90/385/CEE et 93/42/CEE (ou ayant obtenu le marquage CE au titre des directives européennes 93/42 ou 90/385 ou 98/79).

Accessoire de dispositif médical (définition provenant de l'article 2 du règlement (UE) 2017/74) : On appelle « accessoire de dispositif médical » tout article qui, sans être lui-même un dispositif médical, est destiné par son fabricant à être utilisé avec un ou plusieurs dispositifs médicaux donnés pour permettre une utilisation de ce ou ces derniers conforme à sa ou leur destination ou pour contribuer spécifiquement et directement à la fonction médicale du ou des dispositifs médicaux selon sa ou leur destination.

Dispositif Médical Numériques (DMN) : Tout Dispositif Médical intégrant des fonctions numériques comprenant le cas échéant un ou plusieurs accessoires de collecte associés.

Produit : Tout DMN pourra être également appelé produit.

Editeur, ENS, Exploitant ou Fabricant : Toute personne physique ou morale, publique ou privée, ou tout groupement de personnes, doté ou non de la personnalité morale, qui édite le logiciel certifié. Lorsque plusieurs personnes morales distinctes sont parties prenantes à la mise en œuvre du logiciel, elles désignent entre elles un chef de file, lequel porte le composant principal du logiciel et dispose d'un mandat de la part de la ou des autres entités impliquées. L'éditeur peut également être désigné par les termes « industriel » ou « fabricant » dans le référentiel.

Exigences : Les exigences de conformité sont définies dans le référentiel d'interopérabilité et de sécurité. Ces exigences sont rédigées dans le respect de la norme ISO 10781.

Ligne générique : Une description (ou ligne) générique représente un ensemble d'activités médicales qui ont la même indication, remplissent la même fonction, dont les DMN présentent des caractéristiques communes appelées « spécifications techniques » et pour lesquelles les opérateurs répondent aux mêmes exigences minimales, notamment la qualification des professionnels de santé et les dispositions nécessaires pour assurer la qualité des soins.

Nom de marque : Un exploitant de dispositif médical numérique peut demander une inscription en nom de marque, après avoir obtenu la certification de conformité du dispositif médical numérique au référentiel d'interopérabilité et de sécurité des Dispositifs Médicaux Numériques, lorsqu'il ne répond aux spécifications techniques d'aucune ligne générique inscrite ou qu'il revendique une amélioration de la prestation médicale rendue possible par son DMN. Cette inscription ne peut se faire qu'après avis de la Commission nationale d'évaluation des dispositifs médicaux et des technologies de santé (CNEDiMTS).

Utilisateur : Est considéré comme utilisateur dans le référentiel d'interopérabilité et de sécurité des Dispositifs Médicaux Numériques, le médecin ou une personne de l'équipe qui prend en charge le patient.

Usager : Est considéré comme usager le patient.

GLOSSAIRE

Abréviations / Acronymes	Signification
ADELI	Automatisation des Listes (Répertoire de professionnels de santé en cours de remplacement par le RPPS)
Annuaire Santé / ANN	L'Annuaire Santé recense les professionnels de santé enregistrés dans les répertoires nationaux RPPS et ADELI et leurs situations d'exercice. Ces données proviennent des autorités chargées de leur enregistrement (ordres professionnels, ARS, service de santé des armées)
ANS	Agence du Numérique en Santé
CDA	Clinical Document Architecture
CI-SIS	Cadre d'Interopérabilité des Systèmes d'Information de Santé de l'ANS
CGU	Conditions Générales d'Utilisation
CNDA	Centre National de Dépôt et d'Agrément (Organisme autorisant les logiciels à échanger des données de santé)
CNIL	Commission Nationale de l'Informatique et des Libertés
CPS / CPx	Carte de Professionnel de Santé
ENS	Entreprise du Numérique en Santé
FINESS	Fichier National des Établissements Sanitaires et Sociaux
GIE	Groupement d'Intérêt Économique Ex : le *GIE SESAM-Vitale* réalise l'interopérabilité des services de l'Assurance Maladie
GRADeS	Groupements Régionaux d'Appui au Développement de l'e-Santé (Anciennement GCS : Groupements de Coopération Sanitaire)

Abréviations / Acronymes	Signification
HAS	Haute Autorité de Santé
IHM	Interface Homme-Machine
INSEE	Institut National de la Statistique et des Études Économiques
IGC	Infrastructure de Gestion de Clés
INS	Identité Nationale de Santé (à ne pas confondre avec l'identifiant national de santé qui n'en est qu'une partie) (Composé de : matricule INS + OID + 5 traits stricts de référence / critères d'identité)
LATM	Liste des Activités de Télésurveillance Médicale
LPPR	Liste des Produits et Prestations Remboursables
LPS	Logiciel de Professionnel de Santé (abréviation générique désignant une application utilisée par un professionnel de santé, dans ou hors Établissement de Santé)
MIE	Un moyen d'identification électronique (MIE) est un dispositif matériel et/ou immatériel contenant un identifiant personnel et utilisé pour s'authentifier sur un service numérique, en santé dans le présent document. Dans le règlement eIDAS, un moyen d'identification électronique est associé à un niveau de garantie faible, substantiel ou élevé selon le niveau de sécurité qu'il offre.
MSSanté	Messagerie Sécurisée de Santé
NIR NIA	Numéro d'Inscription au Répertoire national d'identification des personnes physiques (ou Numéro de Sécurité Sociale) Numéro d'Identification d'Attente
OID	Object Identifier (Identifiant d'Objets)
PP	Personne Physique
PS	Professionnel de Santé (acteur de santé humain)

Abréviations / Acronymes	Signification
PGSSI-S	Politique Générale de Sécurité des Systèmes d'Information de Santé
RGPD	Règlement Général sur la Protection des Données
RNIV	Référentiel National d'Identitovigilance
RPPS	Répertoire Partagé des Professionnels de Santé
SI	Système d'Information

1 PREAMBULE

Le référentiel d'interopérabilité et de sécurité des Dispositifs médicaux numériques (DMN) est constitué du document suivant assorti de ses annexes :

- Annexe 1 : Liste des spécifications techniques mentionnées dans le référentiel
- Annexe 2 : Déclaration de conformité aux dispositions législatives et réglementaires relatives à la protection des données à caractère personnel
- Annexe 3 : Exigences_référentiel_FR_DMN_V1.2.2.xlsx
- Annexe 4 : Requirements_reference_EN_DMDs_V1.2.2.xlsx

Le présent référentiel vient se substituer au référentiel d'interopérabilité et de sécurité des DMN de télésurveillance sur lequel l'ANS s'est appuyée pour l'élaborer, avec un périmètre plus large.

En effet ce référentiel s'adresse aux fabricants ou aux distributeurs de dispositifs médicaux numériques qui souhaitent solliciter l'inscription, la modification ou le renouvellement d'un DMN sur la liste des produits et prestations médicales ou sur la liste des activités de télésurveillance médicale, après obtention d'un certificat de conformité mentionné à l'alinéa 5° de l'article R165-4 et au I et II de l'article R162-76 du code de la sécurité sociale. Il a été mis une première fois en concertation publique en août 2022, puis en octobre 2022 et décembre 2022, et prend désormais en compte les retours de ces concertations.

2 REFERENTIEL D'INTEROPERABILITE ET DE SECURITE DES DISPOSITIFS MEDICAUX NUMERIQUES (DMN)

2.1 Objet du référentiel

Le présent référentiel définit, sous forme d'exigences, le niveau minimum de garanties attendu pour lequel sera délivré par l'ANS un certificat de conformité des DMN. Ces exigences couvrent les domaines fonctionnels suivants :

- Identité Nationale de Santé (INS)
- Portabilité des données de santé
- Identification électronique des acteurs des secteurs sanitaire, médico-social et social
- Identification électronique des usagers
- Annuaire de santé
- Administration, sécurisation et traçabilité des données du système
- Protection des données de santé
- Pro Santé Connect

2.2 Périmètre d'application du référentiel

Un certificat de conformité au présent référentiel d'interopérabilité et de sécurité prévu à l'article L. 1470-5 du code de la santé publique établis par le groupement d'intérêt public mentionné à l'article L. 1111-24 du code de la santé publique (ANS) est délivré :

- Aux DMN de télésurveillance avant de s'inscrire à la liste des activités de télésurveillance en nom de marque en application de l'article R162-76 I. du code de la sécurité sociale,
- Aux DMN de télésurveillance avant de s'inscrire à la liste des activités de télésurveillance sur une ligne générique en application de l'article R162-76 II. du code de la sécurité sociale,
- Aux DMN hors DMN de télésurveillance avant de s'inscrire à la liste des produits et produits et prestations remboursables en application du 5° de l'article R165-4 du code de la sécurité sociale,
- Aux DMN avant d'être pris en charge de manière anticipée par l'assurance maladie au titre du 3°du II de l'article L162-1-23 du code de la sécurité sociale,
- Aux DMN avant d'être pris en charge de manière transitoire par l'assurance maladie au titre du I de l'article L. 165-1-5 du code de la sécurité sociale.

Le présent référentiel s'applique aux certificats de conformité mentionnés à l'alinéa 5° de l'article R165-4 et au I et II de l'article R162-76 du code de la sécurité sociale. Au sens du présent référentiel, on entend par dispositif médical numérique les outils (DM intégrant des fonctions numériques comprenant le cas échéant un accessoire dans le cas où celui-ci est indissociable du DMN) qui :

- Ont obtenu le marquage CE conformément aux règlements 2017/745 ou 2017/746, ou éventuellement au titre des directives européennes 93/42 ou 90/385 ou 98/79,
- Impliquent un traitement de données à caractère personnel au sens du règlement général relatif à la protection des données n°2016/679 du 27 avril 2016
- Sont destinés à un usage individuel.

Les DMN peuvent aussi comprendre une plateforme d'intermédiation (par exemple la gestion des téléservices de l'Assurance Maladie : INSi, DMP…) développée par un sous-traitant de l'exploitant.

L'ensemble des preuves aux exigences est à fournir dans tous les cas, que l'exploitant fasse par exemple appel à une plateforme d'intermédiation ou non.

2.3 Destinataires du document

Le référentiel d'Interopérabilité et de Sécurité des Dispositifs Médicaux Numériques s'adresse aux entreprises du numérique en santé (ENS) intervenant dans le secteur des dispositifs médicaux (éditeurs de logiciels, fabricants de DMN et exploitants) souhaitant l'inscription sur la liste des produits et prestations remboursables ou sur la liste des activités de télésurveillance médicale d'un DMN.

2.4 Identité Nationale de Santé (exigences n°1 à 65)

Depuis le 1er janvier 2021, la loi impose de référencer les données de santé avec l'Identifiant National de Santé (voir [INS]). Les exigences relatives à l'INS du référentiel sont issues du Guide d'implémentation de l'INS dans les logiciels, annexé au « Référentiel Identifiant National de Santé », publié au journal officiel le 08/06/2021.

Les éléments à prendre en compte pour le référentiel sont les suivants :

- **Guide d'implémentation INS [INS3] :** ce document a été élaboré avec la participation des référents métiers et systèmes d'information de structures de santé et de régions (ARS et GRADeS). Il s'adresse aux fournisseurs de logiciels concernés par le référencement des données de santé avec l'INS. Il décline à leur attention les règles définies dans le référentiel INS et dans le référentiel national d'identitovigilance (RNIV). Ce document a pour objectif d'homogénéiser, par la définition de règles de gestion communes, la mise en œuvre de l'INS à travers le territoire, dans le respect du RNIV.
  Périmètre : Les actions de mise en œuvre de l'INS se concentrent sur les règles de gestion nécessaires au bon référencement des données de Santé avec l'INS dans les logiciels. Il ne décrit pas les actions à mettre en œuvre pour s'assurer que l'usager pris en charge (physiquement ou à distance) correspond à l'identité numérique utilisée (lors de sa prise en charge administrative ou médicale). Ces actions sont décrites dans le RNIV.

- **Guide d'intégration Téléservice Identité Nationale de Santé (INS) INSi [INS2] :** Ce document, élaboré par le GIE SESAM-VITALE décrit tous les aspects fonctionnels et techniques du téléservice INSi de recherche de l'INS. Le téléservice INS intégré au LPS (INSi) permet aux seuls acteurs de la santé et du médico-social respectant les conditions de sécurité rappelées par le référentiel INS[INS1] d'acquérir (ou de vérifier) l'INS et les traits d'identité de référence d'un patient pour répondre aux finalités prévues par les textes encadrant l'usage de l'INS.

- **Référentiel Identifiant National de Santé [INS1] :** Le référentiel INS, décrit les conditions et modalités de mise en œuvre de l'obligation de référencement des données de santé avec l'identité 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 identifiant d'attente (NIA) uniquement pour la prise en charge sanitaire et le suivi médico-social (les autres usages du NIR ne sont pas couverts).

- **Data matrix INS[INS5] :** En cas de production de données de santé au format papier pour un usager ayant une INS qualifiée, son data matrix INS (code-barre) devra être présent sur ces documents.

- **Homologation CNDA :** Dans le cadre de la vérification de la conformité au référentiel d'Interopérabilité et de Sécurité des DMN, le DMN devra avoir passé une homologation auprès du Centre Nationale de Dépôt et D'Agrément (CNDA) autorisant le DMN à appeler le téléservice de recherche de l'INSi, dont un justificatif sera demandé.

- **Interopérabilité :** En cas de récupération de l'identité d'un système tiers, la solution doit avoir la capacité nécessaire à réceptionner des flux d'IHE PAM ou des messages HL7 ADT (voir le référentiel : Gestion de l'INS en intra hospitalier flux HL7 – IHE PAM transaction ITI 30[INS4]).

Il est rappelé de ne pas diffuser de données de santé à caractère personnel dans le cadre des différents tests/jeux de données qui seraient demandés par l'ANS, et se limiter à transmettre exclusivement des données fictives ou anonymisées. Vous trouverez des informations complémentaires (dont les jeux de données de test INS nécessaires pour la génération des preuves de conformité) pour le déploiement de l'INS à l'adresse suivante : INS - Référentiels et déploiement de l'Identité Nationale de Santé | Portail Industriels (esante.gouv.fr)

2.5 Pro Santé Connect (exigences n°66 à 71)

Pro Santé Connect (PSC) est le fédérateur de l'identification électronique des professionnels des secteurs sanitaire, médico-social et social enregistrés au Répertoire Partagé des Professionnels de Santé (RPPS). Il leur permet notamment de s'authentifier aux services numériques en santé, via leur carte de professionnel de santé (CPS) ou leur application mobile équivalente (e-CPS), en fluidifiant le parcours entre divers services auxquels ils sont amenés à se connecter. Il permet aussi aux fournisseurs de services numériques comme les DMN, de récupérer de manière standardisée l'identité sectorielle (identifiant RPPS, profession, etc.), à jour, du professionnel qui s'identifie électroniquement au DMN.

Ce fédérateur est accessible, au choix, via une redirection dans un navigateur web depuis le DMN, ou directement depuis le DMN, grâce au flux dénommé Client Initiated Backchannel Authentication Flow (CIBA).

Les éléments à prendre en compte pour le référentiel sont les suivants :

- Les exigences à respecter sont décrites dans la spécification technique Pro Santé Connect[PSC1].
  Point d'attention : la mise en œuvre du protocole OpenID est nécessaire pour l'implémentation de Pro Santé Connect.

2.6 Annuaire Santé (exigences n°72 à 76)

L'annuaire santé rassemble les données d'identification des professionnels de santé et de leurs structures provenant des différents répertoires sectoriels nationaux : le répertoire partagé des professionnels intervenant dans le système de santé (RPPS), le répertoire ADELI (encore utilisé temporairement d'ici à son prochain décommissionnement) et le répertoire FINESS. Elles sont complétées par les adresses MSSanté et les données des cartes CPS.

Les éléments à prendre en compte pour le référentiel sont les suivants :

- **Dossier des Spécifications Fonctionnelles et Techniques Fichiers d'extraction des données en libre accès de l'annuaire esante.gouv.fr [ANA1] :** ce document présente les informations sur la structuration et le contenu des données présentes dans l'annuaire santé, ainsi que ses modalités d'accès.
- **Modalités d'accès au répertoire sectoriel de référence des personnes physiques par API FHIR[ANA2].**

2.7 Portabilité des données (exigences n°77)

L'industriel doit s'engager à ce que le DMN permette l'export de l'ensemble des données de santé qu'il traite. Le format d'export devra être lisible, exploitable, et documenté par l'industriel.

2.8 Identification électronique des acteurs des secteurs sanitaire, médico-social et social (exigences n°79 à 88)

Des professionnels peuvent être amenés à se connecter au DMN. Leur identification électronique doit être à un niveau de garantie suffisant lorsqu'elle ne se fait pas par Pro Santé Connect, pour protéger les données des patients.

Les éléments à prendre en compte pour le référentiel sont les suivants :

- **Référentiel d'identification électronique des acteurs de santé (personnes physiques) de la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S)[PGSSI-S IE ASPP]** : Ce document a pour objectif de définir les modalités d'identification électronique des personnes physiques intervenant dans les secteurs sanitaire, médico-social et social ainsi que les différents identifiants et dispositifs d'authentification utilisables pour ces personnes physiques en fonction du cadre d'usage. Il se limite à l'étape d'identification et d'authentification des professionnels personnes physiques accédant à des services numériques de santé.

Ce référentiel propose une définition des services numériques dits « sensibles » qui sont soumis à certaines exigences : dans le cadre du référentiel d'interopérabilité et de sécurité des DMN, tout DMN est considéré comme un service numérique sensible, le respect des DMN à ces exigences est donc attendu.

2.9 Identification électronique des Usagers (exigences n°78 et n°89 à 101)

Les patients suivis peuvent être amenés à se connecter au DMN. Il faut que leur identification électronique ait un niveau de garantie suffisant, pour protéger les données de santé des patients. Cela passe notamment par une identification électronique à deux facteurs d'authentification (voir précisions supplémentaires dans le paragraphe "Profils"). Cette identification électronique peut inclure l'utilisation du fédérateur d'identité France Connect.

Les éléments à prendre en compte pour le référentiel sont les suivants :

- **Référentiel d'identification électronique des usagers de la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S)**[PGSSI-S IE USAGER] : Ce document a pour objectif de définir les règles applicables à l'identification électronique des usagers des services numériques de santé - patients/citoyens - et de préciser notamment les différents identifiants et dispositifs d'authentification utilisables pour ces personnes, en fonction du cadre d'usage. Ce référentiel se limite à l'étape d'identification et d'authentification des usagers accédant à des services numériques de santé.

2.10 Administration (exigence 102)

Différents profils d'utilisateurs peuvent être amenés à accéder aux fonctions du DMN, celui-ci doit donc être en mesure de gérer les profils, les droits et les habilitations différents en fonction ces profils.

2.11 Protection des Données de Santé (exigence 103)

Le présent référentiel rappelle aux exploitants de DMN que leurs dispositifs doivent être conformes aux dispositions législatives et réglementaires relatives à la protection de données personnelles, notamment à celles :

- De la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés,
- Du règlement (UE) 2016/679 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 (RGPD) et notamment aux exigences de l'Article 28 (sous-traitant), de l'Article 32 (sécurité des traitements) et de l'article 35 (réalisation d'une Analyse d'impact relative à la protection des données (AIPD).

Les exploitants de DMN doivent produire une déclaration de conformité aux dispositions législatives et réglementaires relatives à la protection des données personnelles[1] - cf. Annexe 3.3.

2.12 Profils

Certaines exigences du référentiel d'interopérabilité et de sécurité des DMN peuvent ne pas s'appliquer à tous les DMN en fonction des cas d'usage couverts par un DMN donné.

Aussi, pour éviter d'appliquer des exigences du référentiel qui ne seraient pas pertinentes par rapport aux cas d'usage couverts par un DMN, les exigences sont regroupées par profil qui devra être choisi par le candidat lors de l'évaluation de sa conformité aux exigences posées par ce référentiel.

[1] Précisé au paragraphe 3.2 Déclaration de conformité aux dispositions législatives et réglementaires relatives à la protection des données à caractère personnel

Certaines exigences sont ainsi conditionnelles et ne sont applicables qu'en fonction des profils retenus par le candidat.

Indications de choix des profils :

- Le profil « **Général** » est obligatoire à minima ;

- Pour l'INS, les exigences obligatoires sont inscrites dans le profil **« Général »** : ce sont les exigences minimales pour tout DMN déployé en médecine de ville ou dans un établissement de santé qui a déployé une solution de Gestion Administrative (GAM) qui gère le référentiel d'identités de l'établissement.
  Comme il est possible que tous les établissements de santé n'aient pas encore mis en place une solution de Gestion Administrative (GAM) qui gère le référentiel d'identités de leur établissement, il est proposé aux fabricants de DMN de couvrir les exigences spécifiques à une solution référentiel d'identités.

  Ainsi, le profil « **Référentiel d'identité** » peut également être choisi (si le DMN permet la création / la modification des identités).

  En cas de sélection de ce profil par l'industriel, sa solution devra également respecter un profil minimum supplémentaire parmi les 2 suivants :

  - « **Référentiel d'identités en Etablissement de Santé** » ;
  - « **Référentiel d'identités hors Etablissement de Santé** ».

  Un dernier profil peut être choisi pour les solutions qui stockent des copies de titres d'identité sous le l'appellation « **Stockage des copies de titres d'identités** ».

- Concernant l'identification électronique des usagers, les exigences associées sont toutes présentes au sein du profil « **Accès Usager** ».

  Le profil **« Accès Usager** » est à sélectionner obligatoirement dès lors que la solution possède un accès patient.

  Le Référentiel d'Interopérabilité et de Sécurité des Dispositifs Médicaux Numériques (DMN) exige une méthode d'authentification des usagers à 2 facteurs. Le Système doit donc implémenter cette méthode d'authentification (exigence IEU 9.1).
  Comme indiqué dans le référentiel d'identification électronique des usagers (#3.4. Moyens identification électronique de transition), le fournisseur d'un service numérique de santé est responsable des mesures de sécurité mises en œuvre pour la protection des données de santé à caractère personnel. Ainsi, ce référentiel encourage l'adoption d'un moyen d'identification électronique de niveau substantiel à brève échéance. Chaque fournisseur doit prendre en compte dans sa décision, par exemple via une analyse de risque, les spécificités de son service et le type et la volumétrie des données traitées.
  Pour tenir compte du cas où l'activation de l'authentification des usagers à 2 facteurs diminue l'usage de la solution et entraîne une perte de chance pour l'usager, le fabricant du DMN peut sous sa responsabilité ne pas activer systématiquement l'authentification à deux facteurs.

  En cas de recours à l'Application Carte Vitale pour l'authentification électronique des usagers, un profil supplémentaire doit être choisi : « **Accès Usagers – ApCV** ».

- Concernant l'identification électronique des professionnels de santé, les exigences associées sont toutes présentes au sein du profil « **Accès Professionnel** » :

  Le profil « **Accès Professionnel** » est à sélectionner obligatoirement pour tout DMN, dès lors que la solution possède un accès professionnel.

Exemple 1 : Je suis un industriel qui propose une solution (hors télésurveillance) utilisée en milieu hospitalier, sans accès patient, qui récupère les identités patient du SI hospitalier, je dois uniquement sélectionner le profil « Général ».

Exemple 2 : Je suis un industriel qui propose une solution de télésurveillance, utilisée en établissement de santé, avec accès patient via l'ApCV, qui créé les identités patient, je dois sélectionner les profils :

- *« Général » ;*
- *« Accès Professionnel de Santé » ;*
- *« Référentiel d'identité » et « Référentiel d'identités en Etablissement de Santé » ;*
- *« Accès Usager » ;*
- *« Accès Usagers – ApCV ».*

Exemple 3 : Je suis un industriel qui propose une solution définie comme un Dispositif Médical Numérique utilisé à destination de patients atteints d'apnée du sommeil, utilisé hors d'un établissement de santé, qui crée les identités patients, je dois sélectionner les profils :

- *« Général » ;*
- *« Référentiel d'identité » et « Référentiel d'identités hors Etablissement de Santé » ;*
- *« Accès Usager »*

3 ANNEXES

3.1 Annexe 1 : Liste des spécifications techniques mentionnées dans le référentiel

#	Référentiel	Version	Lien vers le référentiel
ANA1	Dossier des Spécifications Fonctionnelles et Techniques Fichiers d'extraction des données en libre accès de l'annuaire esanté.fr	V2	https://esante.gouv.fr/securite/annuaire-sante/acceder-aux-donnees
ANA2	Modalités d'accès au répertoire sectoriel de référence des personnes physiques par API FHIR	NA	• Récupération d'un jeton d'authentification via l'API Manager Gravitee : https://portal.api.esante.gouv.fr/ • Connexion à l'API FHIR Annuaire Santé en libre accès : https://gateway.api.esante.gouv.fr/fhir/ • Guide de démarrage de l'API : https://ansforge.github.io/annuaire-sante-fhir-documentation/pages/quick-start/readme • Les StructureDefinition sont publiées sur GitHub : https://github.com/ansforge/annuaire-sante-api-openfhir • IHM de démonstration permettant de générer des requêtes simples : https://portail.openfhir.annuaire.sante.fr/ • *Si vous désirez faire des requêtes plus complexes, nous avons également documenté différents outils facilitant la prise en main de l'API :* *annuaire-sante-fhir-documentation/Implementations at main · ansforge/annuaire-sante-fhirdocumentation*
APCV1	Addendum 8 au Cahier des Charges éditeurs pour la facturation SESAM-Vitale	CDC 1.40-Addendum 8, octobre 2020	https://www.sesam-vitale.fr/web/sesam-vitale/cahier-des-charges

#	Référentiel	Version	Lien vers le référentiel
Pour toutes demandes concernant l'ApCV, voir site G_nius : https://gnius.esante.gouv.fr/fr/reglementation/fiches-reglementation/apcv			
INS1	Référentiel Identifiant National de Santé	V 2.0	https://esante.gouv.fr/sites/default/files/media_entity/documents/ANS_R%C3%A9f%C3%A9rentiel_Identifiant_National_de_Sant%C3%A9_V2.0.pdf
INS2	Téléservice Identifiant National de Santé (INS) intégré aux LPS SEL-MP-043	V04-00-00	https://industriels.sesam-vitale.fr/group/teleservice-insi
INS3	Guide d'implémentation de l'identité INS dans les logiciels	v2	https://esante.gouv.fr/sites/default/files/media_entity/documents/INS_Guide%20implementation_V2_0.pdf
INS4	Gestion de l'INS en intra-hospitalier flux HL7 – IHE PAM transaction ITI 30	v25	http://www.interopsante.org/412_p_15688/documents-publics-de-reference.html
INS5	INS Format Datamatrix	v2	https://esante.gouv.fr/sites/default/files/media_entity/documents/ANS%20-%20Datamatrix%20INS%20v2.2.pdf
Pour toutes demandes concernant la partie intégration / développement de l'appel au téléservice INSi, contacter le centre de service du GIE SESAM Vitale : centre-de-service@sesam-vitale.fr Pour toutes demandes concernant la démarche d'autorisation CNDA (convention, phase de test, ...), contacter le support du CNDA : support.cnda@assurance-maladie.fr			
PGSSI-S IE ASPP	Référentiel d'identification électronique des acteurs de santé (personnes physiques)	v1.0	https://esante.gouv.fr/sites/default/files/media_entity/documents/referentiel-didentification-electronique---acteurs-des-secteurs-sanitaire%2C-medico-social-et-social-%5Bpersonnes-physiques%5D_1.zip
PGSSI-S IE USAGER	Référentiel d'identification électronique des usagers	v1.0	https://esante.gouv.fr/sites/default/files/media_entity/documents/referentiel-didentification-electronique---usagers_0.zip
PSC1	Référentiel Pro Santé Connect	v1.8.4	https://industriels.esante.gouv.fr/produits-et-services/pro-sante-connect/referentiel-psc

#	Référentiel	Version	Lien vers le référentiel
Pour toutes demandes d'accompagnement au sujet de Pro Santé Connect, contacter l'équipe dédiée ANS : *prosanteconnect.editeurs@esante.gouv.fr*			

3.2 Annexe 2 : Déclaration de conformité aux dispositions législatives et réglementaires relatives à la protection des données à caractère personnel

Déclaration de conformité aux dispositions législatives et réglementaires relatives à la protection des données à caractère personnel des exploitants de dispositifs médicaux numériques

Ce document s'adresse aux exploitants de Dispositifs médicaux numériques (DMN)[2] souhaitant s'inscrire dans un dispositif de prise en charge ou de remboursement par l'Assurance Maladie.

Il a pour objet de rappeler aux exploitants de DMN que leurs dispositifs doivent être conformes à l'ensemble des dispositions législatives et réglementaires relatives à la protection de données personnelles, notamment à celles de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et du règlement (UE) 2016/679 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 ainsi que, le cas échéant, aux règles relatives à l'hébergement des données de santé prévu par l'article L. 1111-8 du code de la santé publique.

Le respect de ces dispositions constitue un prérequis au dépôt d'une demande de certification de conformité au référentiel d'interopérabilité et de sécurité des dispositifs médicaux numériques.

En cas de non-respect de ces dispositions, tout exploitant de DMN s'expose à des sanctions en cas de contrôle par la Commission nationale de l'informatique et des libertés (CNIL), conformément à l'Article 58 du RGPD.

Nom de l'exploitant de DMN :

Nom du DMN concerné par la demande de certification de conformité et son numéro de version :

☐ En cochant cette case, **je déclare avoir mis en œuvre des mesures permettant d'assurer la sécurité des traitements,** conformément à l'article 32 du RGPD**.**

- Article 32 du RGPD – Sécurité du traitement : :
    - 1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins :

      a) la pseudonymisation et le chiffrement des données à caractère personnel ;

      b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;

      c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;

[2] Tout Dispositif Médical ayant obtenu le marquage CE, conformément au règlement 2017/745 et 2017/746 (ou éventuellement au titre des directives européennes 93/42 ou 90/385), et à condition que le Dispositif Médical dispose d'une ou de plusieurs des fonctions suivantes :
O Identification et authentification de professionnels de santé
O Identification et authentification de patients
O Stockage de données concernant la santé telles que définies par l'article 4 du règlement général sur la protection des données (RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016)

d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

- 2. Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite.

- 3. L'application d'un code de conduite approuvé comme le prévoit l'article 40 ou d'un mécanisme de certification approuvé comme le prévoit l'article 42 peut servir d'élément pour démontrer le respect des exigences prévues au paragraphe 1 du présent article.

- 4. Le responsable du traitement et le sous-traitant prennent des mesures afin de garantir que toute personne physique agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne les traite pas, excepté sur instruction du responsable du traitement, à moins d'y être obligée par le droit de l'Union ou le droit d'un État membre.

☐ En cochant cette case, **je déclare,** dans la mesure où le traitement porte sur les données sensibles et/ou est réalisé à grande échelle, **avoir réalisé une analyse d'impact relative à la protection des données,** conformément à l'article 35 du RGPD.

- Article 35 du RGPD - Analyse d'impact relative à la protection des données, notamment :

  - 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.

☐ En cochant cette case, **je déclare veiller à ce que mes sous-traitants éventuels présentent des garanties suffisantes en matière de protection des données et avoir conclu un contrat de sous-traitance avec ces derniers,** conformément à l'article 28 du RGPD.

- Article 28 du RGPD – Sous-traitant, notamment :

Le traitement par un sous-traitant est régi par un contrat ou un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre, qui lie le sous-traitant à l'égard du responsable du traitement, définit l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, et les obligations et les droits du responsable du traitement. Ce contrat ou cet autre acte juridique prévoit, notamment, que le sous-traitant :

a) ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement, y compris en ce qui concerne les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel le sous-traitant est soumis; dans ce cas, le sous-traitant informe le responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public;

b) veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;

c) prend toutes les mesures requises en vertu de l'article 32 ;

d) respecte les conditions visées aux paragraphes 2 et 4 pour recruter un autre sous-traitant ;

e) tient compte de la nature du traitement, aide le responsable du traitement, par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, à s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits prévus au chapitre III ;

f) aide le responsable du traitement à garantir le respect des obligations prévues aux articles 32 à 36, compte tenu de la nature du traitement et des informations à la disposition du sous-traitant ;

g) selon le choix du responsable du traitement, supprime toutes les données à caractère personnel ou les renvoie au responsable du traitement au terme de la prestation de services relatifs au traitement, et détruit les copies existantes, à moins que le droit de l'Union ou le droit de l'État membre n'exige la conservation des données à caractère personnel ; et

h) met à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations prévues au présent article et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits (…).

La présente déclaration est à joindre au dossier de demande de certification de conformité au référentiel d'interopérabilité et de sécurité

Fait le :

Prénom, Nom et signature du représentant de l'exploitant de DMN :

3.3 Annexe 3 : Exigences_référentiel_FR_DMN_V1.2.2.xlsx

Le document spécifique qui liste les exigences, les scénarios de conformité et les preuves en français est le suivant :

- Exigences_référentiel_FR_DMN_V1.2.2.xlsx

3.4 Annexe 4 : Requirements_reference_EN_DMDs_V1.2.2.xlsx

Le document spécifique qui liste les exigences, les scénarios de conformité et les preuves en anglais est le suivant :

- Requirements_reference_EN_DMDs_V1.2.2.xlsx