Interoperability and Security standards for Digital Medical Devices (DMDs)

Status: Validated | *Classification: Public* | Version: *V1.2.2*

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

Document history			
Version	Date	Author	Comments
V0.1.0 Consultation	28/07/2022	ANS	Version for consultation (DMDs)
V0.2.0	08/12/2022	ANS	Unified version for consultation (DMDs including remote monitoring DMD) ▪ Modification of the part " 2.1 Scope of application of the standard ". ▪ Renumbering of requirements in part 2 following the deletion of requirement INS 36 in the Excel repository ▪ Modifications on the profiles: o Renaming of the "User Electronic Identification" profile to "User Access” o Renaming of the " Electronic User Authentication - ApCV" profile to "User Access - ApCV" (now optional) o Addition of a "Professional Access" profile regrouping the requirements of the "Health Directory (Annuaire Santé)", "Pro Santé Connect (PSC)", and "Electronic identification of health, medico-social and social sector actors (ASPP)" sections (previously in the "General" profile) o Removed the INS 46 requirement from the "General" profile and added it to the new "Copy of identity documents storage" profile ▪ Update of information on the "ANA2" annex ▪ Restructuring of the document
V1.2.1	27/01/2023	ANS	▪ Correction of the scope of application of the reference system. ▪ Correction of definitions including: o Modification of the definition of Manufacturer o Addition of the product definition. ▪ Correction of the version numbers of the different documents mentioned
V1.2.2	09/02/2023	ANS	▪ Clarification of the scope of the standard ▪ Moving blocks from the "Purpose of the standards" section to the "Scope of the standards" section ▪ Possibility of not systematically activating the 2-factor authentication of users in certain cases.

Regulatory framework

Reference	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]	Order of April 4, 2022 concerning intangible electronic means of identification made available to professionals and individuals in the health, social and medico-social sectors for the use of digital health services https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045551195

TABLE OF CONTENTS

Definitions

Unless otherwise indicated, capitalized terms used in this document have the meanings attributed to them below:

Medical Device Software: Any software that meets the definition of a medical device set forth in Article 2 of Regulation (EU) 2017/745 and 2017/746 of the European Parliament and of the Council of 5 April 2017 concerning medical devices, amending Directive 2001/83/CE, Regulation (CE) No. 178/2002 and Regulation (CE) No. 1223/2009, and repealing Council Directives 90/385/CEE and 93/42/CEE (or that has been awarded the CE marking under EU Directives 93/42 or 90/385)

Medical device accessory (definition from Article 2 of Regulation (EU) 2017/74): A "medical device accessory" is any item that, while not itself a medical device, is intended by its manufacturer to be used with a given medical device(s) to enable the use of the medical device(s) in accordance with its intended purpose(s) or to specifically and directly contribute to the medical function of the medical device(s) according to its intended purpose(s).

Digital medical device (DMD): Any Medical Device with embedded digital functions including, if applicable, an accessory if the latter is inseparable from the DMD.

Product: Any DMD can also be called a product.

Manufacturer or Operator: Any individual or legal entity, public or private, or any group of persons, with or without legal personality, which publishes the certified software. When several distinct legal entities are involved in the same application for certification, they designate among themselves a leader, who carries the main component of the software and has a mandate from the other entity or entities involved. The manufacturer can also be referred to as "industrial" in the standard.

Requirements: The certification requirements are defined in the interoperability and security repository. These requirements are written in compliance with the ISO 10781 standard.

Generic Line: A generic description (or line) represents a set of medical activities that have the same indication, perform the same function, for which the DMDs have common characteristics called "technical specifications" and for which the operators meet the same minimum requirements, in particular the qualification of healthcare professionals and the provisions necessary to ensure the quality of care. An DMDs operator may apply for generic online registration after obtaining certification of the DMD's compliance with the interoperability and security framework and the technical specifications that apply to the DMD.

Brand name: An operator of a digital medical device may apply for registration as a brand name, after obtaining certification of compliance of the digital medical device with the interoperability and safety standards for DMDs, when it does not meet the technical specifications of any registered generic line or when it claims an improvement in the medical service made possible by its DMD. This registration can only be made after receiving the opinion of the *Commission nationale d'évaluation des dispositifs médicaux et des technologies de santé (CNEDiMTS).*

User: In all interoperability and security standards, a user is considered to be the physician or a member of the team who manages the patient.

Glossary

Abbreviations / Acronyms	**Signification**
ADELI	Automation of Lists (“Automatisation des Listes“) (Directory of health professionals being replaced by the RPPS)
ANS	Agence du Numérique en Santé (“Digital Health Agency“)
CDA	Clinical Document Architecture
CI-SIS	ANS Health Information Systems Interoperability Framework (“Cadre d’Interopérabilité des Systèmes d’Information de Santé de l’ANS“)
CGU	Terms and Conditions of Use (“Conditions Générales d’Utilisation“)
CNDA	“Centre National de Dépôt et d’Agrément“ (Organization authorizing software to exchange health data)
CNIL	“Commission Nationale de l’Informatique et des Libertés“
CPS / CPx	Health Professional Card (“Carte de Professionnel de Santé“)
FINESS	National file of health and social establishments (“Fichier National des Établissements Sanitaires et Sociaux“)
GIE	Economic Interest Grouping (“Groupement d’Intérêt Économique“) e.g.: GIE SESAM-Vitale ensures the interoperability of Health Insurance services
GRADeS	Regional support groups for the development of e-health (“Groupements Régionaux d’Appui au Développement de l’e-Santé“) (Formerly GCS: “Groupements de Coopération Sanitaire“)
HAS	High Authority for Health (“Haute Autorité de Santé“)
GUI	Graphical User Interface

Abbreviations / Acronyms	**Signification**
INSEE	National Institute of Statistics and Economic Studies (“Institut National de la Statistique et des Études Économiques“)
IGC	Key Management Infrastructure (Infrastructure de Gestion de Clés)
INS	National Health Identity (“Identité Nationale de Santé“) (not to be confused with the national health identifier which is only a part of it) Composed of: INS number + OID + 5 strict reference traits / identity criteria
LPS	Healthcare Professional Software (“Logiciel de Professionnel de Santé“) (generic abbreviation for an application used by a healthcare professional, inside or outside a healthcare facility)
MIE	An electronic means of identification (“Moyen d’Identification Electronique“) is a tangible and/or intangible device containing a personal identifier and used to authenticate to a digital service, in health in this document. In the eIDAS regulation, an electronic means of identification is associated with a low, substantial or high level of guarantee depending on the level of security it offers..
MSSanté	Secure Health Messaging (“Messagerie Sécurisée de Santé“)
NIR NIA	Registration number in the National Register of Identification of Natural Persons (“Numéro d'Inscription au Répertoire national d'identification des personnes physiques“) (or Social Security number) Waiting Identification Number (“Numéro d'Identification d'Attente“)
OID	Object Identifier (“Identifiant d’Objets“)
PP	Natural Person (“Personne Physique“)
PS	Health professional (“Professionnel de Santé“ (acteur de santé humain))
PGSSI-S	General Security Policy for Health Information Systems (“Politique Générale de Sécurité des Systèmes d’Information de Santé“)
GDPR	General Data Protection Regulation
RNIV	National Identitovigilance Repository (“Référentiel National d’Identitovigilance“)

Abbreviations / Acronyms	**Signification**
RPPS	Shared Directory of Health Professionals (“Répertoire Partagé des Professionnels de Santé“)
SI	Information System (“Système d’Information“)

1 PREAMBLE

The interoperability and safety reference system for Medical Devices with Digital Functions (DMDs) is composed of the following document and its annexes:

- Appendix 1: List of documents mentioned in the reading guide and I&S standards document
- Appendix 2: Declaration of compliance with legal and regulatory provisions on the protection of personal data
- Appendix 3: Exigences_référentiel_FR_DMN_V1.2.2.xlsx
- Appendix 4: Requirements_reference_EN_DMDs_V1.2.2.xlsx

This standard replaces the interoperability and safety standard for remote monitoring DMDs on which the ANS based its development, with a broader scope.

It is intended for manufacturers or distributors of digital medical devices who wish to apply for registration, modification or renewal of an DMDs on the list of medical products and services or on the list of remote medical monitoring activities, after obtaining a certificate of conformity mentioned in paragraph 5 of article R165-4 and in I and II of article R162-76 of the French social security code. It was first put out to public consultation in August, October and December 2022, and now takes into account the feedback from these consultations.

2 INTEROPERABILITY AND SECURITY STANDARDS FOR DIGITAL MEDICAL DEVICES (DMDS)

2.1 Purpose of the standards

This standard defines, in the form of requirements, the minimum level of guarantees expected for which the NSA will issue a certificate of conformity for DMDs. These requirements cover the following functional areas:

- National Health Identity (« Identité Nationale de Santé » or INS)
- Health Data portability
- Electronic identification of actors in the health, medico-social and social sectors
- Electronic identification of users
- Health Directory
- Administration, security and traceability of the system data
- Health data protection
- Pro Santé Connect

2.2 Scope of the standard

A certificate of compliance with these interoperability and security standards provided for in Article L. 1470-5 of the Public Health Code, drawn up by the public interest group mentioned in Article L. 1111-24 of the Public Health Code (ANS), is issued:

- To remote monitoring DMDs before registering on the list of brand name remote monitoring activities pursuant to Article R162-76 I. of the Social Security Code,
- To remote monitoring DMDs before registering on the list of remote monitoring activities on a generic line in application of article R162-76 II. of the Social Security Code,
- DMDs other than telemonitoring DMDs before being registered on the list of reimbursable products and services in application of article R165-4, 5° of the Social Security Code,
- DMDs before they are reimbursed in advance by the health insurance system under 3° of II of article L162-1-23 of the social security code,
- DMDs before they are covered on a transitional basis by the health insurance system under I of article L. 165-1-5 of the Social Security Code.

These standards apply to the certificates of compliance mentioned in paragraph 5 of article R165-4 and in I and II of article R162-76 of the Social Security Code. For the purposes of these standards, a digital medical device is defined as a tool (medical devices integrating digital functions including, where appropriate, an accessory if the latter is inseparable from the DMD) which:

- Have obtained CE marking in accordance with regulations 2017/745 or 2017/746, or possibly under European directives 93/42 or 90/385 or 98/79,
- Involve the processing of personal data within the meaning of the General Data Protection Regulation n°2016/679 of 27 April 2016,
- Are intended for individual use.

DMDs may also include an intermediation platform (e.g. management of Health Insurance teleservices: INSi, DMP...) developed by a subcontractor of the operator.

All of the proof of requirements must be provided in all cases, whether or not the operator uses an intermediation platform.

2.3 Recipients of the document

The interoperability and security standards for Digital Medical Devices is intended for digital health companies involved in the medical device sector (software publishers, DMDs manufacturers and operators) wishing to have a DMD registered on the list of reimbursable products and services or on the list of remote medical monitoring activities.

2.4 National Health Identity (“Identité Nationale de Santé” or INS) (requirements n°1 to 65)

Since January 1, 2021, the law requires that health data be referenced with the National Health Identifier (see [INS]). The requirements relating to the INS in the repository are taken from the Guide to the implementation of the INS in software, appended to the "Référentiel Identifiant National de Santé", published in the official journal on 08/06/2021.

The elements to be considered for the standards are as follows:

- ***Guide d’implémentation INS***[INS3]**:** This document has been drawn up with the participation of business and information systems referents from health structures and regions (ARS and GRADeS). It is intended for software suppliers concerned by the referencing of health data with the INS. It describes the rules defined in the INS repository and in the national identity surveillance repository (RNIV). The objective of this document is to

homogenize the implementation of the INS throughout the country by defining common management rules, in compliance with the RNIV.
Scope: INS implementation actions focus on the business rules necessary to properly reference Health data with INS in software. It does not describe the actions to be implemented to ensure that the user being cared for (physically or remotely) corresponds to the digital identity used (during administrative or medical care). These actions are described in the RNIV.

- ***Téléservice Identité Nationale de Santé (INS) INSi [INS2]*****:** This document, developed by the GIE SESAM-VITALE describes all the functional and technical aspects of the INS teleservice. The INS teleservice (INSi), integrated into healthcare professionals softwares, allows only health and medico-social actors respecting the safety conditions recalled in the ***Référentiel Identifiant National de Santé[INS1]*** to acquire (or verify) the INS of a patient, and its associated identity traits, in order to meet the purposes set out by the legislative texts governing the use of the INS.

- ***Référentiel Identifiant National de Santé[INS1]:*** This document describes the conditions and procedures to be implemented for the referencing of all personal health data with the National Health Identity (or INS).

- **Data matrix INS[INS5]:** When documents containing personal health data for a user with a qualified INS are produced, to be used in paper format, his INS data matrix code must be present on these documents.

- **CNDA approval:** As part of the verification of compliance with the I&S standards document, the remote health monitoring system must have an approval from the national center for filing and approval (“Centre National de Dépôt et D’Agrément” or CNDA) authorizing the system to call the INS teleservice. Proof of the CNDA approval will be requested.

- **Interoperability:** In the event of the retrieval of patient identities from a third-party system, the remote health monitoring system must be able to receive IHE PAM standard data streams or HL7 ADT messages (see the document: *Gestion de l’INS en intra hospitalier flux HL7 – IHE PAM transaction ITI 30*[INS4]).

You are reminded not to disseminate personal health data in the context of the various tests/data sets that may be requested by the NSA, and to limit yourself to transmitting only fictitious or anonymized data. Additional information (including the INS test datasets needed to generate proofs of compliance) for the INS deployment can be found at: INS - Référentiels et déploiement de l'Identité Nationale de Santé | Portail Industriels (esante.gouv.fr)

2.5 Pro Santé Connect (requirements n°66 to 71)

Pro Santé Connect (or PSC) is a digital service, designed to secure the electronic identification and authentication of professionals in the health, medico-social and social sectors registered in the shared directory of professionals working in the health system (“*répertoire partagé des professionnels intervenant dans le système de santé*” or RPPS), to other various digital services, including remote health monitoring systems covered in this document.

The elements to be considered for the standards are as follows:

- As specified in the I&S standards document, the requirements to be met by digital services providers are described in the ***référentiel Pro Santé Connect*** **[PSC1]**.

  Please note: Use of the OpenID protocol is necessary for Pro Santé Connect implementation.

2.6 Health Directory (“Annuaire Santé”) (requirements n°72 to 76)

The Health Directory ("*Annuaire Santé*") brings together identification data of healthcare professionals and theirs structures from the various national repositories: the shared directory of professionals working in the health system ("*répertoire partagé des professionnels intervenant dans le système de santé*" or RPPS), the ADELI directory and the FINESS directory. It also contains the secure email addresses of healthcare professionals ("*adresses MSSanté*"), and their CPS card data.

The elements to be considered for the standards are as follows:

- ***Dossier des Spécifications Fonctionnelles et Techniques Fichiers d'extraction des données en libre accès de l'annuaire esanté.fr*** **[ANA1]:** This document presents information on the structure and content of the Health Directory ("*Annuaire Santé*") data, as well as how-to procedures to access it.

- **Access procedures to the *Répertoire sectoriel de référence des personnes physiques* by FHIR API[ANA2].**

2.7 Data portability (requirement n°77)

The manufacturer must commit to ensuring that the remote digital medical device allows the export of all the health data it processes. The export format must be readable, usable, and documented by the manufacturer.

2.8 Electronic identification of actors in the health, medico-social and social sectors (requirements n°79 to 89)

Professionals are sometimes required to connect to the DMD. Their electronic identification must be at a sufficiently high level of assurance when not done through Pro Santé Connect, to protect patient data.

The elements to be considered for the standards are as follows:

- ***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]**: The objectives of this document are to define the methods of electronic identification of persons working in the health, medico-social and social sectors as well as the credentials and authentication devices that can be used for these persons, depending on the context of use. It is limited to the identification and authentication stage of professional when accessing digital health services.

This document offers a definition of digital services labelled as "sensitive" which are subject to specific requirements: within the I&S standards document, any remote health monitoring system is considered as a sensitive digital service, and compliance to these requirements is therefore expected.

2.9 Electronic identification of users (requirements n°78 and n°89 to 101)

Patients being monitored may be required to log in to the DMDs. Their electronic identification must have a sufficient level of guarantee to protect patient health data. This includes electronic identification with two authentication factors. This electronic identification can include the use of the France Connect identity federator.

The elements to be considered for the standards are as follows:

- ***Référentiel d'identification électronique des usagers de la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S)*** **[PGSSI-S IE USAGER]:** The objectives of this document are to define the methods of electronic identification of non-professional users of digital health services as well as the credentials and authentication devices that can be used for these persons, depending on the context of use. It is limited to the identification and authentication stage of non-professionals users when accessing digital health services.

2.10 Administration (requirement n°102)

Different user profiles may have access to the DMDs functions, so the DMDs must be able to manage the different profiles, rights and authorizations according to these profiles.

2.11 Health Data Protection (requirement n°103)

This standard reminds DMDs operators that their devices must comply with legislative and regulatory provisions relating to the protection of personal data, in particular those:

- Of law n° 78-17 of January 6, 1978, relating to data processing, files and freedoms,
- Of Regulation (EU) 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (GDPR) and in particular the requirements of Article 28 (processor), Article 32 (security of processing) and Article 35 (conducting a Data Protection Impact Assessment ("Analyse d'impact relative à la protection des données" or AIPD).

DMD operators must produce a Declaration of compliance with legal and regulatory provisions relating to the protection of personal data[1] - see Appendix 3.3.

2.12 Profiles

Some requirements of the interoperability and security standards document may not apply to all remote health monitoring systems depending on the use cases covered by a given remote health monitoring system (see examples below).

Therefore, to avoid applying requirements from the I&S standards document that would not be relevant to the use cases covered by a given solution, the requirements are grouped by profiles that must be chosen by the candidates when submitting their application.

Certain requirements are thus conditional and are only applicable according to the profiles selected by the candidate for its remote health monitoring system.

Indications for choice of profiles:

- The "General" profile is mandatory.
- For the INS, the mandatory requirements are listed in the "General" profile: these are the minimum requirements for any MISP deployed in a healthcare facility that has deployed an Administrative Management Solution (AMS) that manages the facility's identity repository.

[1] Specified in paragraph 3.2 Appendix 2: Declaration of compliance with legal and regulatory provisions on the protection of personal data

As it is possible that not all healthcare institutions have yet implemented an Administrative Management Solution (AMS) that manages their institution's identity repository, it is proposed that DMDs manufacturers cover the specific requirements of an identity repository solution.

Thus, the **"Identity Repository"** profile can also be chosen (if the DMN allows the creation/modification of identities).

If the manufacturer selects this profile, his solution must also respect an additional minimum profile among the following two:

- "**Identity repository in health facilities**" ("Référentiel d'identités en Etablissement de Santé"),
- "**Identity repository in ambulatory medicine**" ("Référentiel d'identités hors Etablissement de Santé").

A final profile can be chosen for solutions that store copies of credentials under the name "**Copy of identity documents storage**".

- Regarding the electronic authentication of patients, the associated requirements are all present in the profile "**User Access**".

  The "**User Access**" profile must be selected if the solution has a patient access.

  The Digital Medical Device (DMD) Interoperability and Security standards require a 2-factor user authentication method. Therefore, the System must implement this authentication method (IEU requirement 9.1).
  As stated in the electronic user identification repository (#3.4. Means Transition Electronic Identification), the provider of a digital health service is responsible for the security measures implemented to protect personal health data. As such, this standard encourages the adoption of a substantial level of electronic identification means in the near future. Each provider must take into account in its decision, for example through a risk analysis, the specificities of its service and the type and volume of data processed.
  In order to take into account the case where the activation of the two-factor authentication of users reduces the use of the solution and leads to a loss of chance for the patient, the DMD manufacturer may under its responsibility not systematically activate the two-factor authentication.

  If the Carte Vitale application is used for electronic user authentication, an additional profile must be selected: "**User Access – ApCV**".

- Concerning the electronic identification of healthcare professionals, the associated requirements are all present in the "**Professional Access**" profile.

  The "**Professional Access**" profile must be selected for all DMNs, as long as the solution has professional access.

Example 1: *"I am a manufacturer who offers a solution used in hospitals, without patient access, which recovers patient identities from the hospital IS, I only need to select the "General" profile".*

Example 2: *"I am a manufacturer who offers a remote monitoring solution, used in healthcare facilities, with patient access via the ApCV, which creates patient identities, I must select the profiles:*

- *"General";*
- *"Health Professional Access";*
- *"Identity Repository" and "Health Care Facility Identity Repository";*
- *"User Access";*
- *"User Access – ApCV".*

Example 3: *I am a manufacturer who offers a solution defined as a Digital Medical Device used for patients with sleep apnea, used outside of a healthcare facility, which creates patient identities, I must select the profiles:*

- *"General";*
- *"Identity repository" and "Identity repository outside a health care institution";*
- *"User Access".*

3 ANNEXES

3.1 Appendix 1: List of documents mentioned in the reading guide and I&S standards document

#	Document	Version	Link
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	• Retrieving an authentication token via the Gravitee Manager API: https://portal.api.esante.gouv.fr/ • Connect to the FHIR API Open Access Health Directory: https://gateway.api.esante.gouv.fr/fhir/ • API getting started guide: https://ansforge.github.io/annuaire-sante-fhir-documentation/pages/quick-start/readme • The StructureDefinition are published on GitHub: https://github.com/ansforge/annuaire-sante-api-openfhir • Demonstration GUI to generate simple queries: https://portail.openfhir.annuaire.sante.fr/ • *If you want to make more complex queries, we also have documented various tools to make the API easier to use:* *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, october 2020	https://www.sesam-vitale.fr/web/sesam-vitale/cahier-des-charges

#	Document	Version	Link
For all requests concerning the ApCV, please contact Bruno Noury (Assurance Maladie) via the G_nius website: https://gnius.esante.gouv.fr/fr/reglementation/fiches-reglementation/apcv ***All requests should be in French.***			
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
For all requests concerning the INS teleservice, please contact the GIE SESAM Vitale service center: centre-de-service@sesam-vitale.fr For all requests concerning the CNDA approval procedure, please contact the CNDA service center: support.cnda@assurance-maladie.fr ***All requests should be in French.***			
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

#	Document	Version	Link
For all requests concerning Pro Santé Connect, please contact the ANS dedicated team: prosanteconnect.editeurs@esante.gouv.fr ***All requests should be in French.***			
HAS1	Télésurveillance médicale du patient insuffisant rénal chronique	Version for notice	*https://www.has-sante.fr/upload/docs/application/pdf/2022-01/avis_referentiel_insuffisance_renale_chronique.pdf*
HAS2	Télésurveillance médicale du patient insuffisant respiratoire chronique	Version for notice	*https://www.has-sante.fr/upload/docs/application/pdf/2022-01/avis_referentiel_insuffisance_respiratoire_chronique.pdf*
HAS3	Télésurveillance médicale du patient diabétique	Version for notice	*https://www.has-sante.fr/upload/docs/application/pdf/2022-01/avis_referentiel_diabete.pdf*
HAS4	Télésurveillance médicale du patient insuffisant cardiaque chronique	Version for notice	*https://www.has-sante.fr/upload/docs/application/pdf/2022-01/avis_referentiel_insuffisance_cardiaque_chronique_2022-01-24_09-34-42_519.pdf*
HAS5	Télésurveillance médicale du patient porteur de prothèse cardiaque implantable à visée thérapeutique	Version for notice	*https://www.has-sante.fr/upload/docs/application/pdf/2022-03/avis_referentiel_protheses_cardiaques_implantables_a_visee_therapeutique.pdf*

3.2 Appendix 2: Declaration of compliance with legal and regulatory provisions on the protection of personal data

Declaration of compliance with legislative and regulatory provisions on the protection of personal data of operators of Digital medical devices (DMDs)

This document is intended for operators of digital medical devices (DMD)[2] wishing to register for reimbursement by the French health insurance system.

Its purpose is to remind DMDs operators that their devices must comply with all legislative and regulatory provisions relating to the protection of personal data, in particular those of Law No. 78-17 of January 6, 1978 relating to information technology, files and freedoms and regulation (UE) 2016/679 du 27 avril 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, as well as, where applicable, the rules relating to the hosting of health data provided for by Article L. 1111-8 of the Public Health Code.

Compliance with these provisions is a prerequisite for applying for certification of compliance with the interoperability and security standards for digital medical devices.

In the event of non-compliance with these provisions, any DMDs operator may be subject to sanctions in the event of an inspection by the French Data Protection Authority (Commission nationale de l'informatique et des libertés or "CNIL"), in accordance with Article 58 of the GDPR.

DMD operator name:

Name of the DMD concerned by the request for certification of conformity and its version number:

☐ By checking this box**, I declare that I have implemented measures to ensure the security of processing**, in accordance with Article 32 of the GDPR.

- Article 32 of the GDPR – Security of processing:

  - 1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

    a) the pseudonymisation and encryption of personal data;

    b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

    c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

    d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

[2] Any Medical Device that has obtained the CE mark, in accordance with Regulation 2017/745 and 2017/746 (or possibly under European Directives 93/42 or 90/385), and provided that the Medical Device has one or more of the following functions:
• Identification and authentication of healthcare professionals
• Identification and authentication of patients
• Processing of personal data within the meaning of the General Data Protection Regulation n°2016/679 of 27 April 2016

- 2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

- 3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

- 4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

☐ By checking this box, **I declare** that, insofar as the processing involves sensitive data and/or is carried out on a large scale, **I have carried out a data protection impact assessment** in accordance with Article 35 of the GDPR.

- Article 35 of the GDPR - Data protection impact assessment, especially:

  - Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. 2A single assessment may address a set of similar processing operations that present similar high risks.

.

☐ By checking this box, **I declare that I have ensured that my potential subcontractors provide sufficient data protection guarantees and that I have concluded a subcontract with them** in accordance with Article 28 of the GDPR.

- Article 28 of the GDPR – Processor, especially:

  - 3) Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. 2That contract or other legal act shall stipulate, in particular, that the processor:

    a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

    b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

    c) takes all measures required pursuant to Article 32;

    d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;

    e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

    f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;

    g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;

h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

This declaration is to be attached to the application for certification of conformity to the interoperability and safety reference system.

Date:

First Name, Last Name and Signature of DMD Operator Representative:

3.3 Appendix 3: Exigences_référentiel_FR_DMN_V1.2.2.xlsx

The specific document that lists the requirements, compliance scenarios and evidence in French is the following:

- Exigences_référentiel_FR_DMN_V1.2.2.xlsx

3.4 Appendix 4: Requirements_reference_EN_DMDs_V1.2.2.xlsx

The specific document that lists the requirements, compliance scenarios and evidence in English is the following:

- Requirements_reference_EN_DMDs_V1.2.2.xlsx