MINISTÈRE
DE LA SANTÉ
ET DE LA PRÉVENTION
*Liberté
Égalité
Fraternité*

Direction générale
de l'offre de soins

NATIONAL IDENTITY SECURITY FRAMEWORK

01

PATIENT IDENTIFICATION PRINCIPLES COMMON TO ALL HEALTHCARE PROVIDERS

3RIV
RÉSEAU DES
RÉFÉRENTS RÉGIONAUX
D'IDENTITOVIGILANCE

RNIV 1 Common Principles • version 1.3 | June 2022

CONTENTS

CONTRIBUTORS

Mr Raphaël Beauffret, DNS

Ms Christelle Boulin, ANS

Mr Bruno Champion, DGS

Ms Elsa Creach, ANS

Ms Céline Descamps, CRIV NA

Mr Thierry Dezerces, ARS Ile de France

Mr Thierry Dubreu, GRADeS IDF (SESAN)

Mr Marc Fumey (HAS)

Dr Gilles Hebbrecht, DGOS

Dr Christine Leclercq, GRADeS Occitanie (e-santé Occitanie)

Ms Bérénice Le Coustumer, DGOS

Mr Mikaël Le Moal, DGOS

Dr Isabelle Maréchal, Rouen University Hospital

Ms Christelle Nozière, CRIV NA

Dr Manuela Oliver, GRADeS PACA (ieSS)

Mr Loïc Panisse, GRADeS Occitanie (e-santé Occitanie)

Ms Emilie Passemard (DNS)

Mr Bertrand Pineau, GRADeS IDF (SESAN)

Ms Isabelle Stach, GRADeS Occitanie (e-santé Occitanie)

Mr Michel Raux, DGOS

Dr Bernard Tabuteau, CRIV NA

Ms Charlotte Voegtlin, GCS Tesis, La Réunion

The team would like to thank the various professionals who helped to improve this document during the consultation phase.

VERSION HISTORY

Version	Date	Context
1.0	2020-10-30	1st release of the document
1.1	2020-12-20	Correction of typos and minor content adjustments
1.2	2021-05-20	Update following CNIL opinion
1.3	2022-06-03	Updated systems to validate or qualify an identity

1 Introduction

1.1 Issues in identifying health care patients

Correctly identifying a patient is a key factor in the safety of their course of treatment. It is the first act in a process that continues throughout the patient's care by the various healthcare professionals involved, whatever their speciality, sector of activity, or care methods.

However, a large number of participants (both healthcare professionals and patients) seem to be unaware of the risks involved in case of imperfect identification. The most common adverse event is the administration of care to the wrong patient. But misidentification can also be a source of delays in care, diagnostic errors, therapeutic errors, incorrect information exchanged between professionals, health data recorded in a file that does not belong to the correct patient (collision), creating multiple files for the same patient (duplicates), and billing errors, among other possibilities.

The identification process is also one of the key elements for the deployment of national health policies and in particular the eHealth roadmap[1]. It is essential that a patient is identified in the same way by all professionals who share health data concerning him/her. The obligation to use the *National Health ID* (INS) from 1 January 2021 is one of the responses to this challenge. It requires the implementation of best practices, respected by everyone, to avoid spreading an INS number incorrectly associated with a digital identity.

As a contributor to trust in the exchange of health data, correct identification is a major national issue for the safety of care. Identity verification is an integral part of a care procedure; it is carried out under the responsibility of the healthcare professional providing the care. The participation of the patient (or if failing that, their relatives), as such a person plays a role in their own security, must be sought whenever possible to facilitate this stage; other than regulatory situations of anonymity of care, the patient cannot object to the verification of their own identity by a healthcare professional.

Healthcare providers and managers of facilities could be held liable if it turned out that the failure to implement best identification practices had caused damage or endangerment to a patient.

1.2 National Identity Security Standard

The purpose of the National Identity Security Standard (RNIV) is to set out the requirements and recommendations to be met in terms of the identification of patients in health or social care settings by the various professionals involved (outpatient clinics, healthcare facilities, social care sector, social actors) in order to control the risks in this field.

Note: The RNIV does not address the issue of the identity required when billing for care: the Assurance Maladie (National Health Insurance Fund) uses identification traits that may differ significantly from the official identity but which are disregarded in the field of identity security.

The RNIV is annexed to the "National Health ID" Reference Document, which it complements. As such, it is enforceable against everyone who contributes to this care by processing health data: Patients, healthcare professionals, agents responsible for creating and modifying identities in the information system, as well as IT publishers, those responsible for processing all the e-health applications[2], the Health Insurance Fund (as manager of the shared medical record, or DMP for short, and project manager of the INSi teleservice) and even complementary organisations (offering care-related services) and social services (when they participate in care).

[1] https://esante.gouv.fr

[2] Not to mention the shared medical record (DMP), the pharmaceutical record (DP), etc.

The RNIV replaces the documents establishing regional identity security rules (standards or charters). It sets the minimum level of security that all stakeholders must apply to patient identification. However, the requirements and recommendations may be supplemented or clarified by practical documents or specific instructions from national, regional, territorial, and/or local authorities.

Note:

The RNIV currently consists of 5 components:

0 - Compendium of key points

1 - Principles of patient identification common to all healthcare providers

2 - Implementation of identity security in health care facilities

3 - Implementation of identity security in non-hospital settings

4. Implementation of identity security by providers in private practice

2 Definitions

2.1 Identity, identification, identity security

Identity is the set of *traits* or characteristics that enable an individual to be recognised and establish their individuality in the eyes of the law (date and place of birth, surname, given name, parentage, etc.). These elements are evidenced by official civil status documents or their digital equivalent.

Identification corresponds to operations that make it possible to establish the identity of an individual with regard to civil status, to recognise that person as a physical individual, and to create a personal paper and/or digital record for them. In health, there are two complementary areas of patient identification:

- *Primary identification*: This includes all the operations intended to assign a unique digital identity to a physical patient in a health information system, whether this is the first contact with the patient or a subsequent visit; it covers the stages of searching for, creating and modifying an identity, as well as assigning a level of trust to the recorded data (see 3.3)
- *Secondary identification*: This corresponds to the means implemented during the management of a physical patient (care, administration of medication, biological sampling, medical imaging examination, etc.) to ensure that the right care is provided to the right patient; it consists in particular of verifying, at each stage of management, that the real identity of the patient corresponds to the identity shown on the documents and management tools (physical or computer file, prescription, label, travel voucher, examination report, etc.)

Digital identity is the representation of a physical individual in an information system (see Annex I). The same physical patient is thus associated with several digital identities depending on the information system used: Employer, taxes, social security, mutual insurance company, bank, etc.

Identity security is defined as the arrangements made to ensure the reliability of patient identification and the security of their health data at all stages of their care. It concerns the understanding of and compliance with the identification rules by everyone, as well as the management of the risks associated with the errors encountered. It is an integral part of data security, which is the responsibility of the identity data controller: legal entity, private practitioner, facility director, eHealth application manager, etc.

2.2 National eHealth ID ("Identité Nationale de Santé" or INS)

The *National eHealth ID* (INS) is a digital identity based on national reference databases (see 3.2). The RNIV uses the term *INS* to refer to all the information that makes up the INS. Each INS includes the following elements:

- the *INS number*, which is the patient's personal NIR (or NIA), 15 characters long
- the *INS traits* which are the reference identity traits associated with the NIR/NIA in the reference databases (surname at birth, given name(s) at birth, sex, date of birth and INSEE code of place of birth)
- the organisation that assigned the INS, specified in the form of an *OID* (*object identifier*), information that is usually invisible to the healthcare professional (the NIR and the NIA each have their own assignment authority, which makes it possible to tell them apart).

Fictitious example of an INS

INS number	*Last name*	*Given name(s)*	*Sex*	*DOB*	*Place of birth*	*OID*
260058815400233	*DARK*	*JEANNE MARIE CECILE*	*F*	*1960-05-30*	*88154*	*1.2.250.1.213.1.4.8*

2.3 Semantic conventions

In the RNIV, the terms *healthcare provider* and *healthcare facility* are used generically to identify the professionals (administrative and nursing) and entities in which they intervene: medical practice, hospital structure, social care establishment, social service, care coordination platform, etc.

As the notion of a *family name* is very often confused with that of a *customary name*, it was decided to use the term *surname at birth* in the RNIV instead of *family name*.

The RNIV also introduces the concepts of *surname used* and *given name used*, which differ in their purpose from the *customary name* and *usual given name*, the definition of which is linked to civil status (see Annex II).

The requirements ("Exi") and recommendations ("Reco") are marked in bold in the text and compiled in Annex III; they concern the information system (SI) and/or professional practices (PP).

As the similarity between certain terms can lead to confusion, the RNIV uses the terms:

- *check* for all consistency assessment operations between several sets of traits
- *qualification/qualify* to the assignment of *Qualified Identity* status to the digital identity
- *retrieval/retrieve* to INS search and retrieval operations
- *validation/validate* to the assignment of *Validated Identity* status to the digital identity
- *verification/verify* to INS verification operations.

3 Best practices in primary identification of patients

The general rules described in this chapter concern the management of the patient's digital identity in health information systems (HIS).

3.1 General rules for the digital registration of a patient

3.1.1 How to search for a record in the local database

3.1.1.1 Searching for existing records

To avoid creating multiple digital identities for the same patient (duplicates) or integrating data into someone else's record (collisions), searching for a patient's record in the facility's identity repository is imperative before creating an identity, according to the methods defined by each facility or health care provider.

The information system must allow a search for a digital identity to be carried out on the basis of:

- **all or part of the INS retrieved after the INSi teleservice query;**
- **the entry of the date of birth, possibly supplemented by the first characters of the surname or given name. [Exi SI 01]**

The use of the INS number for the existing identity search must be secured to avoid any risk of input error. If the INS number is not retrieved electronically, the entry of the 15 characters of the NIR and their validation by the control key is mandatory for any search on the basis of the INS number. [Exi SI 02]

In order to obtain relevant results, it is strongly recommended to limit the number of characters entered when searching for a record based on the first or last name. [Reco PP 01]

e.g. search performed with date of birth + first 3 characters of the surname at birth.

Note: There may be powerful tools for performing a prior art search based on a similarity rate or a phonetic search; they can be used provided that the publisher commits to the security of the results returned and that the healthcare facility validates the practice.

When searching for a patient in the identity database, it is necessary for the information system to query without distinction, with the corresponding data but without taking into account hyphens or apostrophes, the fields Surname at birth and Surname used, as well as the fields Given name(s) at birth, First given name at birth and Given name used. **[Exi SI 03]**

3.1.1.2 Displaying search results

The search results must be displayed in a sufficiently informative way so that the professional can safely determine whether it is possible for them to select the record corresponding to the patient receiving care, or whether a new digital identity must be created. The display must include at least the mandatory traits (see 3.1.3.1)[3] and, if applicable, the dates of the most recent visits. Where possible, it must also report information on the status of the identity and any associated attributes (see 3.3).

3.1.2 How to create a digital identity

There are several possibilities to record a new patient in the facility's information system. The digital identity can be created:

- from the INS traits automatically retrieved after querying the INSi teleservice (see 3.1.2.1)
- by manual entry of identity traits provided directly by the patient or a companion (see 3.1.2.2)
- from the digital identity transmitted by another facility that has provided care to the patient, or by the patient on their own through adapted tools (except for querying the teleservice, see 3.1.2.3)
- based on fictitious or approximate trait in the context of accommodating a patient who is difficult to identify or entitled to anonymity (see 3.1.2.4).

3.1.2.1 Retrieving the INS

It is possible to query the INSi teleservice via the health information system, either by using the patient's Carte Vitale or their entitlement holder's card (see 3.2.1.2), or by entering the traits of the local digital identity (see 3.2.1.3).

[3] The usefulness of displaying the INS number in the search screen results as well as the surname used and given name used is to be decided by the facility

3.1.2.2 Manual entry of identity traits

The quality of the recorded digital identity depends on how it is recorded, depending on whether the identity is collected:

- from an evidence document, depending on the type of document presented (see 3.3.3.2)
- with the help of oral information spoken by the patient, a relative, or any other intermediary
- under very poor conditions (patient is unaccompanied and unconscious, confused, non-French speaking, etc.).

When an identity document is presented, the traits must be recorded as they appear on the document provided (see 3.1.2.4) but in accordance with the recording rules defined in this document: specific instructions are given in Annex IV for the recording of certain traits.

3.1.2.3 Use of a transmitted identity from a different identification domain

In some cases, a patient is recorded without being physically present. This is the case, for example:

- for a service provider who performs a remote procedure (labwork, telemedicine)
- for a professional who receives health data concerning a patient not recorded in the information system that person uses
- in procedures that allow the patient to register online (upstream solutions for making appointments/pre-consultation/pre-admission within an online patient portal)
- when the identity is received in paper form (see 4.2.3.2).

Transmitted traits without an INS number shall be recorded by default with the status Provisional Identity. However, they can be recorded as Validated Identity if the identity of the patient has been verified on the basis of a Substantial eIDAS certified electronic identification scheme (in particular in the case of online appointment booking/pre-admission through a solution offering this level of electronic identification).
When the transmitted identity is accompanied by an INS number, the traits must be checked by querying the INSi teleservice which, if they are correct, allows the INS to be recorded by default in the status Identity retrieved. However, the INS can be recorded as a Qualified Identity if the identity of the patient has been verified on the basis of a Substantial eIDAS certified electronic identification scheme (in particular in the case of online appointment booking/pre-admission through a solution offering this level of electronic identification).
In case of non-compliance, the mandatory traits are recorded with the status Provisional Identity, without keeping the INS number.
Querying the INSi teleservice is mandatory to verify a received INS when the digital identity does not exist or does not have Retrieved or Qualified status. [Exi PP 01]

When this identity is not transmitted by computer but has to be copied manually, it is possible to use the trait search operation to facilitate and secure the retrieval of the traits and the INS number (see 3.2.1.3 and 4.2.3.2).

Annex V develops examples of use cases relating to the identification of remote patients (remote registration, subcontracting, telemedicine, tele-expertise, etc.) and specifies the exemptions concerning service providers contractually bound to facilities that subcontract procedures to them.

3.1.2.4 Creation of a fictitious or approximate identity

There are situations where it is not possible to identify a patient with their true identity:

- a patient is unaccompanied, non-communicative or delirious at intake
- mass intake of victims in exceptional health situations
- a patient is asserting their right to anonymous care.

As the creation of a digital identity is mandatory to record the care, it uses fictitious or approximate traits that will be, if possible, corrected at a later point. The providers concerned must implement an ad hoc procedure which defines how to manage the five mandatory traits that must be filled out (see 3.1.3.1) according to the information that can be collected (see Annex IV). The digital identity must be associated with the attribute *Questionable Identity* or *Fictitious Identity* (see 3.3.2).

3.1.3 What information must be collected?

Correctly identifying a patient requires the recording of a certain amount of information, called "traits", which vary in importance.

Identification traits must be the subject of specific fields in the information system. [Exi SI 04]

3.1.3.1 Invariant traits (mandatory traits)

These are the reference traits that are used to establish the official identity of an individual, without risk of error. Mandatory traits include:

- the surname at birth (family name)
- the first given name at birth[4];
- date of birth
- sex
- place of birth (INSEE code of the commune of birth for people born in France or of the country of birth for others)
- the list of given names at birth
- the INS number (supplemented by its *OID*, see 2.2)[5].

The creation of a digital identity requires the capture of information in at least five mandatory traits: surname at birth, first given name at birth, date of birth, sex, and place of birth. [Exi PP 02]

The fields relating to the list of given names at birth and the INS number are filled in as soon as it is possible to access this information: presentation of an identity document and/or query to the INSi teleservice (in cases where a search for that information is required and authorised). [Exi PP 03]

Example (fictitious):

The official identity of Mrs Jeanne Marie Cécile Dark, widow of Louis, is composed of the reference traits of her INS, without the *OID* (see example in § 2.2):

Last name	*Given name(s)*	*Sex*	*DOB*	*Place of birth*	*INS number*
DARK	*JEANNE MARIE CECILE*	*F*	*1960-05-30*	*88154*	*260058815400233*

Her first given name is JEANNE.

The rules for manual recording of these traits are specified in Annex IV.

3.1.3.2 Other traits (additional traits)

This is personal information that complements a patient's mandatory traits. It is not used to establish the patient's official identity but is essential to facilitate certain operations relating to the patient's care or to risk management-related processing (see 4).

Recorded in dedicated fields, they include (but are not limited to):

- given name and surname used in everyday life
- postal code and/or name of the commune of birth (see Annex IV)

[4] Field retained to ensure compatibility between software, see input methods in Annex 1

[5] See INS Reference Document (https://esante.gouv.fr/sites/default/files/media_entity/documents/ASIP_Référentiel_Identifiant_National_de_Santé_v1.pdf)

- mailing address of the patient
- telephone numbers of the patient or their legal guardian
- e-mail address of the patient or their legal guardian
- photograph[6]
- profession
- social security number of the entitlement holder (relating to the various beneficiaries of a single insured person)
- identities and contact details of the people involved (parent, child, spouse, trusted person, etc.)
- telephone number or e-mail address of the entitlement holder
- contact details of the general practitioner
- other healthcare professionals involved in care
- nature of the identity document presented
- etc.

The information system must allow for the entry of the additional traits *Surname used* and *Given name used*. [Exi SI 05]

It is necessary to fill in as many additional traits as possible, according to the instructions that each facility defines according to their needs. [Exi PP 04]

3.1.3.3 Semantic clarifications

The fields *surname used* and *given name used* are new fields, introduced by the RNIV to collect the identity used by the patient in everyday life. They are intended to facilitate the dialogue between caregiver and patient, particularly in situations of consistency checks relating to secondary identification (before each procedure), the aim being to strengthen the relationship of trust between the professional and the patient and to facilitate the work of the professional and their ability to monitor their patient.

The procedures for collecting these fields are specified in Annex IV.

Example:
Mrs Jeanne, Marie, Cecile, Dark, widow of Louis, has always used her surname at birth in everyday life although her customary name, Louis, is specified on her identity card and she wants this to remain so. Similarly, although this does not comply with civil status rules, she has used the compound name Marie-Cécile since she was very young without ever having it made official.

It is recommended that DARK be entered as the *surname used* and MARIE-CECILE as the *given name used* so that she can continue to be referred to by these traits in her contacts with health care providers.

Note: The name of her deceased husband, as it was never used, does not appear in the additional traits but can be recorded, if necessary, in an "Other" field, if it exists, according to local arbitrations formalised in an ad hoc procedure.

Each healthcare facility or provider, depending on its activities and its patient base, locally defines the rules for populating these fields. The choice can be made to take into account only the customary name and usual given name (in the sense of civil status), mentioned on an identity document or to fill in these fields, as in the example above, with the given name and surname actually used in everyday life. This decision must be logged, formalised, and communicated.

[6] Subject to compliance with likeness rights and the data retention rules in force

3.2 General rules for the use of the INS

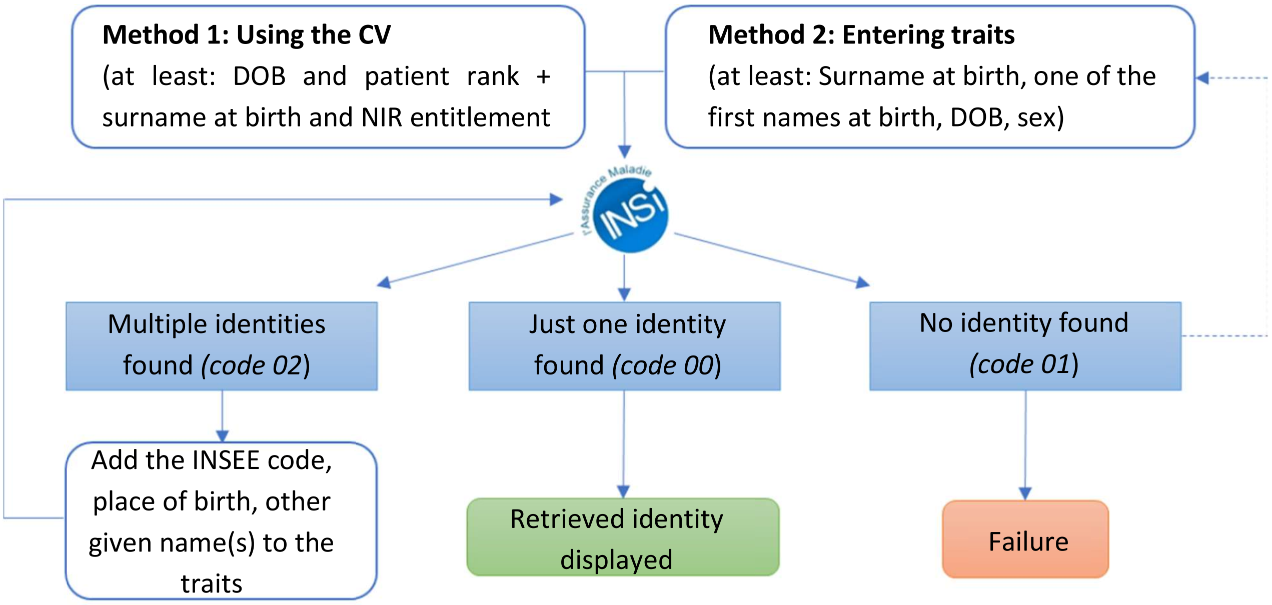
3.2.1 How to retrieve and manage the INS?

3.2.1.1 General

The patient's INS is searched for, retrieved and/or verified by querying a dedicated teleservice called INSi[7]. When required, the query to this teleservice is made through the health information system (HIS) and entails the authentication of the user (e.g. physical CPx card or digital authentication procedure).

The teleservice can be queried in two ways:

- via the Carte Vitale (see 3.2.1.2)[8];
- by entering the identity traits recorded locally or transmitted by a third party (see 3.2.1.3).


Method 1: Using the CV
(at least: DOB and patient rank + surname at birth and NIR entitlement
Method 2: Entering traits
(at least: Surname at birth, one of the first names at birth, DOB, sex)
l'Assurance Maladie INSi
Multiple identities found *(code 02)*
Just one identity found *(code 00)*
No identity found *(code 01)*
Add the INSEE code, place of birth, other given name(s) to the traits
Retrieved identity displayed
Failure

The information retrieved from the INSi teleservice is stored and tracked in the health information system. [Exi SI 06]

Note: For some patients, the INS reference database contains empty (or null) values in the surname, given name, and/or sex fields, and/or in certain parts of the date of birth field (00/00/YYYYY, 00/MM/YYYYY or DD/00/YYYYY). As these data are incompatible with the RNIV rules, the INS of these patients cannot be accepted (see Annex VI). Their digital identity must only be filled in manually (see 3.1.2.2) or from information provided by a third party (see 3.1.2.3), without the ability to retrieve the INS.

Before any integration of the INS into the local digital identity, it is necessary to validate the consistency between the INS traits returned by the INSi teleservice and the traits of the individual receiving care. [Exi PP 05]

The approach to assessing the consistency between sets of traits is detailed in Annex VI.

Note: Outside the regulatory framework of anonymity, the patient cannot object to the use of the INS but must be informed of it[9] and of their right to access and rectify the data.

[7] https://esante.gouv.fr/securite/identifiant-national-de-sante

[8] Currently, the INSi teleservice prohibits the use of the Carte Vitale's fingerprint

[9] See INS Reference Document (https://esante.gouv.fr/sites/default/files/media_entity/documents/ASIP_Référentiel_Identifiant_National_de_Santé_v1.pdf)

3.2.1.2 Search using the Carte Vitale

Querying the INSi teleservice via the Carte Vitale is the preferred method of querying whenever possible. [Exi PP 06]

The procedure uses certain traits collected through the Carte Vitale[10], in a transparent way for the user. A perfect match must be found in order to retrieve the INS. This search may, in some cases, be unsuccessful.

3.2.1.3 Search by entering identity traits

Querying the teleservice by entering traits is not recommended as a first step**.** It must only be used in cases where:

- the Carte Vitale is not presented by the insured person
- access by reading the Carte Vitale is not operational
- the search via the Carte Vitale is unsuccessful
- the digital identity was transmitted by a third party (see 3.1.2.3).

The traits to be used are, at a minimum: surname at birth, one of the given names at birth, sex, date of birth. A perfect match is expected for the identities present in the INSi database. If only one INS is found in the database (code "00"), the teleservice displays the INS traits corresponding to the identity entered and allows it to be retrieved. If several INS identities are found (code "02"), the teleservice does not provide a list; it will be necessary to add to the identity by entering the place of birth (official INSEE geographical code, see Annex IV) or even the other given names at birth. In some cases, this search may be unsuccessful (code "01").

3.2.1.4 Important notes

Querying the INSi teleservice is not appropriate in several situations; for example:

- patient who has no reason to be registered in France (foreign tourist, etc.)
- identity considered questionable or fictitious (see 3.3.2)
- care is for a newborn who has not yet been allocated a NIR (thus also the foetus in utero)
- legal anonymity[11].

3.2.2 What information is returned by the INSi teleservice?

Among the information contained in the INS returned by the INSi teleservice, those that allow the identification of the patient are:

- the *INS number*, consisting of the individual's identification number in the register of natural persons (NIR or NIA);
- *INS traits*, identity traits from the national reference database (SNGI):
    - surname at birth
    - given name(s) at birth (separated by spaces)
    - date of birth
    - sex
    - the geographical code of the place of birth.

<u>Note</u>: The INSi teleservice can also return a “usual given name” recorded in the Assurance Maladie databases; as this is not a reference trait from the civil status database, its retrieval by the information system must be ignored.

3.3 Levels of trust assigned to the local digital identity

[10] INSi Teleservice Integration Guide: http://www.sesam-vitale.fr/documents/20182/75606/SEL-MP-043_01-00_INSi+sans+MR/92d6e408-012d-4dc5-9fd1-d3bdda78735a

[11] Secret childbirth, planning centre, etc.

The recording of identity traits must be associated with information that specifies, according to the methods of collection and consistency control, the level of trust that can be placed in the digital identity created, which has consequences for its subsequent use.

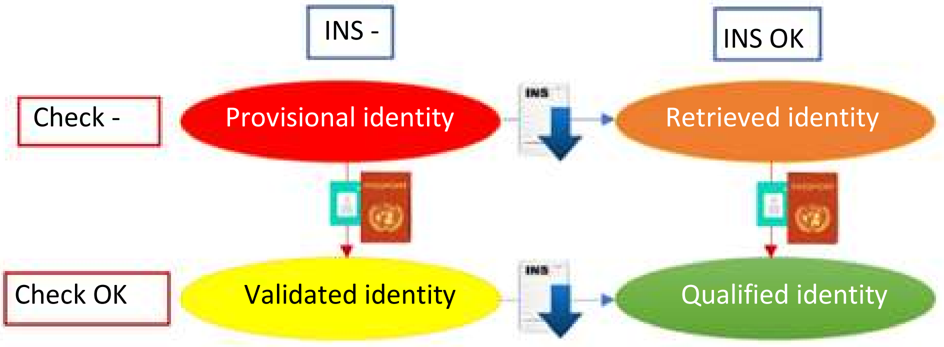
3.3.1 What are the trust statuses of a digital identity?

The trust to be placed in a digital identity corresponds to a pair of factors indicating whether the traits of the digital identity recorded in the HIS:

- are derived from the INS retrieved from the reference databases via the INSi teleservice [I+] or not [I-]
- have been checked for consistency against the traits shown by a high-trust identity document or its digital equivalent [C+] or not [C-].

There are four increasing levels of trust for local digital identity:

- ***provisional identity*** status [I-, C-] is the default status for any digital identity created without using the INSi teleservice
- ***retrieved identity*** status [I+, C-] is assigned when the digital identity is created from the INS retrieved after querying the INSi teleservice (see 3.2.1)
- ***validated identity*** status [I-, C+] is assigned after checking the consistency of the traits recorded in *provisional identity* against those shown by a highly-trusted identification scheme (see 3.3.3.2)
- ***qualified identity*** [I+, C+] status combines the retrieval (or verification) of the INS from the INSi teleservice and checking that the recorded traits are consistent with those shown by a highly-trusted scheme.



Any health information system must be able to assign one of four trust statuses to each stored digital identity. [Exi SI 07]

The assignment of a trust level to any digital identity is mandatory. [Exi PP 07]

Qualified identity status is the only one that allows the INS number to be used when transmitting data within the health information system (HIS)[12].

The information system must ensure that only *qualified identity* status allows the listing of health data exchanged with the INS number, in compliance with the applicable regulations. [Exi SI 08]

Annex VII provides examples of situations where the trust status of the digital identity may change.

3.3.2 What additional attributes can be used?

It is recommended that health information systems allow the use of additional attributes to enable professionals to characterise digital identities requiring special treatment. [Reco SI 01]

[12] Apart from the specific use case of a subcontractor returning the results of a procedure with the INS sent by the prescriber (see Annex 2)

The purpose of the ***similar identity*** attribute is to facilitate the identification and management of digital identities with a high degree of similarity (known near-matches and similar identities), which must be the subject of particular attention[13] on the part of healthcare professionals. It can be associated with each of the four statuses defined above and is not, except in exceptional cases (e.g. post-facto modification of one of the mandatory traits), modified during a status change of an identity. This attribute can be disseminated to all applications in the identification domain.

The attribute ***questionable identity*** makes it possible to trace the existence of a doubt as to the veracity of the collected identity (confused patient, suspected fraudulent use of identity, exceptional health situation, etc.). It can only be associated with a *provisional identity* status. If it is associated with a digital identity that had previously been given a higher trust status, it causes the status to be downgraded to *provisional identity* and, in cases where an INS number was associated, to be deleted (or invalidated).

The ***fictitious identity*** attribute can only be associated with *provisional identity* status. It aims to facilitate the management of:

- so-called sensitive identities, which are subject to specific regulations in terms of anonymisation of care;
- other situations where fictitious identities are created (imaginary traits attributed to a patient unable to state their identify, computer tests, training, etc.).

Note: The notion of a fictitious identity is to be distinguished from "confidential" or "protected" situations where the patient is registered under their real identity but does not wish it to be disclosed.

For digital identities with a *questionable identity* or *fictitious identity* attribute, it must be made impossible for the software:

- **to assign a status other than provisional identity**
- **to make a query to the INSi teleservice. [Exi SI 09]**

Summary matrix of possible associations between statuses and attributes:

		Statuses			
		Provisional ID	Retrieved ID	Validated ID	Qualified ID
Attributes	Similar ID	+	+	+	+
	Questionable ID	+			
	Fictitious ID	+			

3.3.3 Best practices in digital identity validation

3.3.3.1 General rules

Usually, the identity validation and/or qualification procedure is carried out when the patient comes to the centre, by asking them to present a document attesting their identity or by using a highly-trusted identification scheme (see 3.3.3.2).

In order to use a trusted digital identity, it is essential to ensure, at least when the patient first makes physical contact with a facility, that the identity documents presented correspond to the person being cared for. [Exi PP 08]

On subsequent visits, this mandatory consistency check between the real identity and the one recorded may not be justified if the patient is known to the healthcare provider. In a group practice, the level of risk should be assessed according to the population served, the procedures performed, and the turnover of professionals.

[13] Specific tools for the management of these similar identities can be proposed by software editors

For example, a request for an identity certificate for each visit could be made mandatory for facilities or services which carry out risky activities or provide emergency care, etc.

The organisation may decide to carry out the consistency check between the digital identity and the identity present on the ID document at a later point (in back-office mode) by dedicated professionals, using an ad-hoc procedure. In this case, the identity document presented must have been saved by photocopying or scanning[14]. This deferred validation is a good practice for securing this stage when the flow of patients to be received is high and/or when task overload may cause the receiving professionals in that ward to be less vigilant than normal.

Conversely, the practice of "automatic" validation, without relying on a highly trusted identity document (or its digital equivalent), is a dangerous practice for all stakeholders.

Validating a digital identity without being able to check its consistency against a highly trusted identity credential, or its digital equivalent, the type of which is duly recorded in the information system, is strictly prohibited. [Exi PP 09]

3.3.3.2 What systems exist for validating or qualifying an identity?

Only official highly-trusted systems are accepted to change the status from ***provisional identity*** to ***validated identity*** or from ***retrieved identity*** to ***qualified identity***.

For French patients, these are the national identity card and the passport[15]. For minors or in the particular case of certain patients of legal age[16] who do not have one, the family record book (*livret de famille*) or a birth certificate is accepted. In this case, it is necessary that the legal representative, the parent or the descendant, depending on the case (adults vs. minors), can prove their own identity.

For foreign patients, it is the passport, residence permit, or national identity card for nationals of the European Union (EU), Switzerland, Liechtenstein, Norway, Iceland, the Vatican and the Principality of Monaco, San Marino, and Andorra[17].

All other documents have less probative value and cannot be used to validate a digital identity.

Electronic identification schemes may also be used. To allow validation of an eHealth ID, the scheme used must provide a "substantial" or "high" level of assurance as defined in the eIDAS regulation[18].

Note: The submission of a highly-trusted identity document that has passed its validity date does not prevent the status of *validated identity* from being assigned. In case of discrepancies between two highly-trusted identity documents, the passport should be preferred if it is one of the documents presented. In other cases, the data of the most recent document must be taken into account. In the particular case of foreign identity documents that do not mention the patient’s surname at birth, preference must be given to the document showing the identity closest to that of the patient, and the patient must be advised to always present that document when seeking care or social support.

Individual cases must be decided on a case-by-case basis. They must be reported by the facility to the regional identity security contact, who will decide whether the identity can be validated in the absence of the documents mentioned below. The aim is to have an identity as close as possible to that of the patient, by adapting the status.

[14] Subject to compliance with applicable data retention rules

[15] Law no. 2012-410 of 27 March 2012 on the protection of identity

[16] Some people who live in residential care facilities for the dependent elderly do not have identification.

[17] Although these states are not part of the European Union, their nationals can travel to France by identifying themselves only with their national identity card.

[18] https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-reglement-eidas/

The type of identity scheme used to collect the identity must be recorded[19]. Only a highly-trusted document, or its digital equivalent, shall allow the status of *validated identity* or *qualified identity* to be assigned. [Exi SI 10]

3.4 Practical use of identity traits

3.4.1 What are the rules for displaying and editing identity traits?

Except for regulations applicable to sensitive identity situations, the identity traits recorded in the patient's file must be accessible to all professionals who share health data, without there being any doubt as to the nature of each trait displayed.

It is only necessary to display the INS number for healthcare providers who need that information. The professionals involved are to be defined by the facility. It can be replaced by a code and/or colour indicating the status of the identity.

It is important that the nature of each identity trait displayed on documents and human-machine interfaces is easily recognised, without risk of misunderstanding, by all healthcare providers involved. [Exi SI 11]

It is the responsibility of the healthcare facility to define the methods of displaying and editing the traits in the various use cases (human-machine interface, labels, request for examination or prescription of a procedure, examination or stay report, etc.), in compliance with the regulations in force.

At a minimum, the following mandatory traits must be displayed: surname at birth, first given name at birth, date of birth, sex and, on documents containing health information data, the INS number followed by its nature (NIR or NIA) when this information is available and its sharing is authorised. [Exi PP 10]

Note: When filled in, it is recommended that the *surname used* and *given name used* fields also appear on the different media used.

Practical examples are given in Annex VIII.

For the exemption involving identification of biological samples, if a system enabling an identifier to be reliably linked to the identity of the sampled patient is used by the collector, the identity traits might not appear on the label on the tube.

More generally, in addition to a "plain text" display, INS identities are also presented as a datamatrix.

3.4.2 How to use INS traits

The procedures for accepting the identity returned by the INSi teleservice are set out in Annex VI.

After the qualified identity or retrieved identity status has been assigned, the INS traits shall replace, if not already present, the local mandatory traits in the corresponding fields. [Exi SI 12]

These changes must be transmitted to the third-party software used by the facility to care for the patient.

[19] The CNIL recognises the legitimacy of recording an identity document as part of identity verification. It authorises the retention of a paper copy under the same conditions as the medical record for a period of five years from the patient's last visit to the institution, the retention of digital identity documents in encrypted form, and access to this copy for specifically authorised professionals in charge of handling identity-related anomalies, subject to the condition of traceability and the recording of consultations. Storing the document number is not allowed.

Once the identity has been upgraded to qualified identity status, the INS number and the INS traits must be used to identify the patient, particularly when exchanging health data concerning that person. [Exi PP 11]

Note: Other identifiers necessary for the coordination of exchanges may continue to be transmitted.

A number of anomalies may arise in identity management, either due to discrepancies that are revealed after the fact or in connection with the misallocation of the INS. These situations are covered in a dedicated chapter in the RNIV sections about different types of facilities.

4 Managing risks related to patient identification

The basic version of the RNIV only refers to the general principles for organising the fight against adverse events associated with identification errors. More operational elements in terms of the policy, governance. and conduct of risk management to be implemented by healthcare facilities are detailed in the RNIV sections about different types of facilities.

4.1 General

Risk management (RM) is an integral part of the continuous quality improvement process. It is traditionally divided into two complementary approaches depending on when the action is carried out:
- pre-emptive RM, focused on the prevention of avoidable risks
- post-facto RM, designed to detect and analyse errors in order to keep them from recurring

The RM techniques applied to primary or secondary identification errors do not differ from those routinely applied in facilities for other types of risks, per the recommendations of the Haute Autorité de Santé (HAS, France's National Health Authority)[20].

They are based in particular on:
- an a priori *risk map* which aims to list known situations of identification errors, to categorise them in terms of their level of criticality[21] (high, medium, or low) and to identify the measures to be implemented to prevent them
- the implementation of *preventive steps* described in a *quality documentation* specific to identity security
- a *system for reporting adverse events* – whether potential or actual – which allows for the identification of new malfunctioning situations in terms of primary and secondary identification[22]
- *feedback*, which aims to analyse the institutional, organisational and human factors that led to the error and to implement appropriate corrective and/or preventive actions
- formalising *procedures* specifying what to do in activities with a higher risk of error
- training professionals

4.2 Primary identification RM

4.2.1 Security of digital identities

The rules relating to the security of digital identities in HISs are not specific to identity security, but they have a big influence on the security of patient care.

This document merely recalls some of the principles, such as the need for:

[20] https://www.has-sante.fr/jcms/c_1661118/fr/gerer-les-risques

[21] Product of severity and frequency

[22] https://signalement.social-sante.gouv.fr/psig_ihm_utilisateurs/index.html#/accueil

- a *single identity repository* for each facility (or group of facilities) in order to guarantee the consistency of identity data for all the business software programs that share personal information about the patients receiving care
- *mapping the application flows* describing the type of interface implemented between the tools involved in patient identification
- formalising the *clearance policy* and the individual rights (access, modifications) granted to professionals
- prohibiting the use of generic logins, etc.

Facilities must have a single identity repository ensuring data consistency for all software that manages patients' personal information. [Exi SI 13]

The organisations must have an application map detailing in particular the identity-related flows. Non-interfaced tools that require human intervention to update identities must be identified. [Exi PP 12]

An IT charter formalising the rules of access and use of the information system, and in particular for applications managing personal health data, must be drawn up within each group practice. [Exi PP 13]

It is essential that accesses and modifications to identities are logged (date, time, type of modification and professional who carried out the action). Successive retrievals of the INS must also be recorded. [Exi SI 14]

The IT charter is distributed to the professionals present as well as to newcomers, as well as external service providers and contributors.

4.2.2 Management of anomalies in identity databases

The facility must regularly assess the quality of the identity repository (see 4.2.1) of each of the identification domains (see Annex I) in order to be able to detect and address the most common anomalies, whenever possible:
- duplicates (several digital identities corresponding to the same individual)
- collisions (same numerical identity assigned to 2 different individuals)
- inconsistent dates of birth
- sex inconsistent with the given name

It is recommended that the information system must have dedicated functionalities to search for anomalies in the recording of identity traits. [Reco SI 02]

4.2.3 Security when using the INS

4.2.3.1 General

Errors associated with the use of the INS have potentially greater consequences as they can spread beyond the facility (see 1.1). It is therefore necessary to establish special monitoring procedures in this area and to provide instructions for dealing with the various types of undesirable events that may occur.

It is important to formalise procedures that specify what to do:
- when transcribing an INS received in paper format (see 4.2.3.2)
- when a discrepancy between the local digital identity and the INS traits is found during an INSi query (see Annex VI), either during an initial search or during a verification operation (see 4.2.3.3 and 4.2.3.4)
- when it is not possible to qualify the digital identity in the short term due to the lack of highly trusted identity documents
- in the event of an error in the allocation of an INS number to a patient (there must be ways to inform all the providers with whom the facility has shared data using this mistaken identifier).

Healthcare providers affected by the dissemination of an INS-related error must be alerted without delay, using a specific procedure formalised by the facility. [Exi PP 14]

4.2.3.2 *Transcribing the INS received in paper format*

In order to avoid manual transcription errors, it is necessary to use the INSi teleservice for trait retrieval when the patient is absent (see 3.2.1.3). If the identity has been entered manually with the INS number, the INSi teleservice must be used for verification (see 3.1.2.3 and Exi PP 01).

4.2.3.3 *Anomaly identified during identity verification when receiving health data*

A verification operation must be carried out by the recipient when receiving health data associated with an INS for a patient who does not yet have a digital identity with *qualified identity* status. If the verification is not successful, the INS number must not be recorded. After a search of the local database (see 3.1.1.1), the health data may, depending on the situation:

- be associated with a new local digital identity created with the traits of the received identity, with the status *provisional identity*
- be associated with an existing unqualified identity that shares the same mandatory traits, provided that the professional is certain not to create a collision
- not be integrated into the information system, as they cannot be securely attributed to a specific patient, but rather should be used to populate a list of anomalies to be dealt with.

In all cases, it is necessary to send an alert to the sender of the data to inform that person of the existence of the anomaly (see Exi PP 14) and to investigate the cause of the inconsistency reported by the teleservice (see Annex VI).

4.2.3.4 *Anomaly identified during routine verification of the identity databases*

The INS reference document[23] specifies that a verification of qualified identities must be scheduled every 3 to 5 years. If the INSi teleservice provides a negative response regarding a digital identity, the main risk is that of using and transmitting an invalid INS. There must be a procedure for dealing with this situation. Until the reasons why the operation failed are understood, it is necessary to:

- change the status of the digital identity to ***validated identity*** – if it is possible to check the consistency of the identity again from a scanned highly-trusted document – or to ***provisional identity*** if it is not
- delete (or invalidate) the INS number.

4.3 Secondary identification RM

Primary identification best practices alone do not make it possible to secure the care of patients. Professionals still need to ensure that the patient receiving the procedure is the one for whom the care was prescribed. Recommendations to facilitate this secondary identification include:

- the active participation of the patient, whenever possible, in the security of their care and therefore in the verification of their identity before care, and in particular before risky acts ("the patient playing a role in their own security")
- the use of the surname used and the given name used, if any, for direct exchanges with the patient
- the use of physical identification schemes such as wristbands, use of a photograph in the patient's file[24]
- regular checks that the identity of the patient being treated (as stated or verified by the physical identification scheme) is consistent with the one recorded on the documents (prescription, care plan, pill box, label, reports, test results, etc.)
- checking the consistency – in terms of display, presence and naming of identity-related fields – between the different software programs exchanging patient health data within the facility.

[23] https://esante.gouv.fr/sites/default/files/media_entity/documents/ASIP_R%C3%A9f%C3%A9rentiel_Identifiant_National_de_Sant%C3%A9_v1.pdf

[24] Subject to compliance with likeness rights and applicable regulations

4.4 Documentation quality

Group medical practices must formalise the institutional patient identification policy in an identity security charter. [Exi PP 15]

The purpose of the identity security charter, which may be shared among several related facilities, is to reiterate the principles to be followed when:

- collecting a patient's identity
- preventing the risks associated with misidentification
- harmonising practices and promoting a culture of security among professionals
- getting patients involved in this security requirement

It is expressed through operational procedures implemented within the facility – or group of facilities – according to the risks identified and their criticality (see 4.1).

4.5 Quality indicators

Quality indicators are intended to assess the performance of the system. It is important to have information on both primary and secondary identification practices. They are defined within the facility but can also be generalised territorially, regionally, or even nationally. They are specified in the sections on risk policy and risk management in different types of facilities.

4.6 Training and awareness-raising on identity security

Compliance with the identification rules depends on their being understood and assimilated by all stakeholders: Both professionals and patients alike. This area therefore requires particular attention in terms of:

- training and awareness-raising for all professionals in the facility
- regular evaluations of knowledge and practices
- information and awareness-raising for external contacts (ambulance drivers, professionals and patient-facing facilities, technical platforms, etc.)
- information and awareness-raising for patients.

ANNEX I – Identification and matching domains

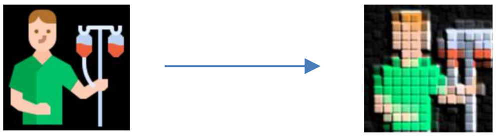
Individual and digital identity

Any individual registered in an information system is recognised there via that person's digital identity. This includes at least:

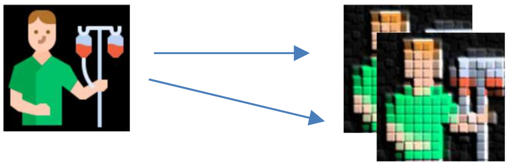
- an identification domain (DI) which identifies the identity database used
- the local identifier (I) used in that database to identify the patient
- a set of identity traits (T) characterising that patient (name, address, etc.;
- a status (S) which specifies the level of confidence in this identification.

Identification domain (DI)

An identification domain contains all the computer applications where the patient is recognised by the same digital identity, through a common database of identities.



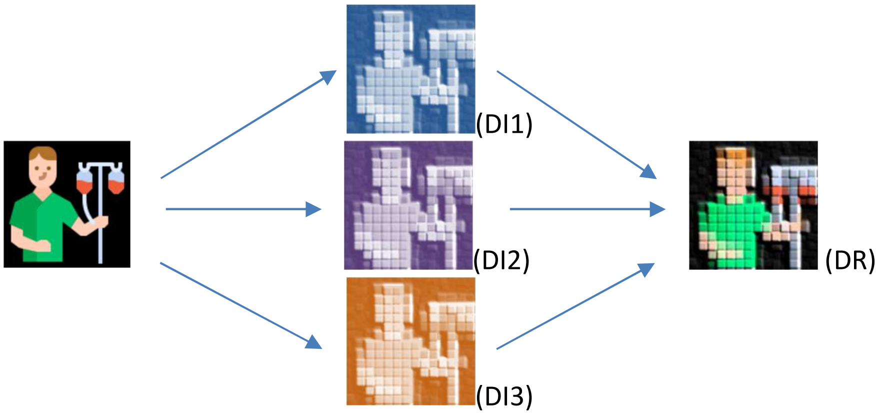
In a DI, a duplicate is when the same individual is identified with more than one digital identity (I1, I2, etc.).



In a DI, a collision is when two different physical persons are identified with the same digital identity.

Matching domain (DR)

A matching domain assigns a common digital identity (known as a federation identity) to multiple identification domains, which can then exchange data securely. It serves as a unique repository of identities.



ANNEX II – Terminology and definitions

This annex defines a number of terms used by identity security professionals.

Healthcare provider

This term is used generically in this document to identify the professionals involved in the health care or social care of a patient.

Alias = pseudonym

Entitled person

A patient who is not insured in their own right but who is entitled to social benefits because of a link, which is often family-related, with the insured person who is the entitlement holder.

Code officiel géographique (COG: Official Geographical Code)

This is the coding method used to record the place of birth for people born in France, based on tables provided by INSEE, the national statistics agency. As the COG of the municipality is likely to change over time, the COG retrieved from the INS is used in case of discrepancies related to the coding history of the municipality (*commune*).

Collision

This is an anomaly that occurs when the same identifier has been assigned to two or more different physical persons, particularly in the following cases: Erroneous selection of a computer file, identity theft targeting a third party who is already registered, error in the merging of files that do not belong to the same patient, etc. When this occurs, it becomes very difficult to distinguish after the fact which medical information belongs to each patient. There is a risk that medical and care decisions could be made based on another person's health data.

Date of birth

This is one of the mandatory identity traits and must be entered in DD/MM/YYYY format, which requires that dates in a lunisolar calendar be converted into this format for patients born abroad.

Identification domain

This domain contains all applications within a healthcare organisation that use the same identifier for one patient.

Examples:

- a medical practice with a unique way of identifying its patients is considered an identification domain
- a healthcare facility whose software all uses the same identifier is an identification domain

Matching domain

This domain contains at least two identification domains that exchange or share information with each other. A distinction is made between intra-facility and extra-facility matching domains.

Examples:

- a healthcare facility with a Permanent Patient Identifier (IPP) where some of the software uses one identifier while other software uses another identifier is a matching domain. In this example, there are two groups of software and each group uses its own identifier. Each group therefore constitutes a different identification domain. The institution also has an IPP that allows it to exchange information between the two identification domains. This matching domain is an intra-facility matching domain
- if healthcare facilities populate a regional identity and matching server, then this server constitutes a matching domain.

Health data

Personal data relating to physical or mental health which reveal information about the state of that person's health. They include information that is:

- collected for the purpose of receiving health benefits (identifiers, identity traits)
- obtained during care (history, test results, information exchanged between professionals, etc.)
- from which it is possible to deduce information about the state of the person's health (care provided, hospital ward, etc.).

Duplicate

Duplicate identities occur when the same person is recorded under two (or more) different identifiers in the same identification domain. The patient then has multiple different medical and administrative files that do not communicate with each other. Not having all the medical information about the patient creates a risk due to the professional being unaware of data that would be useful for decision-making.

Duplicate flow: A duplicate detected in the active queue at the time of a patient's visit

Duplicate stocks: All duplicates present in the identity repository Duplicate stocks can be identified when analysing the quality of the patient database.

Civil status

Under French law, civil status is made up of the elements that allow a person to be identified, such as surname, given name(s), sex, date and place of birth, parentage, nationality, home address, marital status, and date and place of death. Any person who normally lives in France, even if born abroad and holding a foreign nationality, must have a civil status.

Merger

This refers to the transfer, into a single identifier, of all the information concerning the same patient that is spread out across multiple identifiers (duplicates) of the same identification domain.

Identical traits

Identical traits are when there is an exact match between multiple mandatory traits shared by multiple different people. These trait-sharing patients must therefore be differentiated by other traits.

Compare this notion of identical identities to the notion of close or similar identities where the traits are different but can potentially be confused (e.g.: Dupond and Dupont).

Identifier (technical)

A sequence of alphanumeric characters used by one or more information systems to represent an individual. For example: permanent patient identifier (IPP), INS number, etc.

National eHealth ID (INS, for "Identité nationale de santé")

This is a unique, unambiguous, permanent digital identity that allows a patient's health information to be listed, stored and transmitted. Its use is mandatory effective 01/01/2021 for all healthcare professionals. Today it corresponds to the *INS* (see this term).

Note: A calculated identifier (INS-C), assigned through an algorithm based on information read from the insured person's Carte Vitale, was initially used, but the results were found to cause duplicates or collisions.

Primary identification

This is the set of operations intended to unambiguously assign an individual a digital identity of their own. Primary identification includes the steps of searching for a patient in the database, creating or modifying an identity, validating this identity, and retrieving the INS by querying the INSi teleservice.

Secondary identification

This corresponds to the verification, by any healthcare professional, of the identity of the physical patient throughout their care before carrying out a procedure concerning that person (sampling, care, transport, technical procedure, etc.). It also includes identifying the patient's samples or documents and selecting the right file in an application used within a care service (prescription, care file, test results, etc.).

Identity

A set of data, or identity traits, that constitute a representation of an individual.

Questionable identity

An attribute of a digital identity used to indicate that the identification procedure is not secure, either because of a doubt about the identification document presented (suspicion of fraud) or because the identity is based on the statements of a confused patient or a third party who does not know that person well. This is an attribute that can only be associated with provisional identity status.

Fictitious identity

An attribute of a digital identity used to indicate that the identity traits do not relate to the patient's real identity. It results from applying an identification procedure used in sensitive identity situations (anonymisation of care). This attribute can also be used for IT testing or training purposes. This is an attribute that can only be associated with provisional identity status.

Fraudulent identity

Identity fraud takes place when a patient uses the identity of another in order to receive social benefits to which the fraud perpetrator is not entitled. This situation can lead to very serious risks for the health of the perpetrator as well as for the rights-holder during a future stay in the healthcare facility because of the combined information (collision) found in the same patient file. When it is suspected, the “questionable identity” attribute must be used.

Similar identity

Attribute used to indicate a high degree of similarity between digital identities and to alert professionals when dealing with these patients with similar identities.

INS

The INS contains all the digital information provided by the INSi teleservice and is made up of:

- the INS number: identification number in the register of natural persons (NIR or NIA)
- INS traits (surname at birth, list of given names from civil status, date of birth, sex, commune code of place of birth or country code for persons born abroad)
- the OID *(object identifier*) which identifies the origin and type of information (INSEE, NIR/NIA, etc.).

Digital identity

Digital identity is the representation of a physical individual in an information system (see Annex I). The same patient can have several digital identities: in the identification or matching domain(s) used by the facility, in their Shared Medical Record (DMP), in the health insurance billing database, etc. On the other hand, when the patient has several digital identities in the same identification domain, they are duplicates.

Provisional identity

Status of a local digital identity that has not been retrieved from the INSi teleservice and has not yet been checked for consistency with the traits shown by a highly-trusted identity scheme. This status can, if necessary, be associated with a *questionable identity* or *fictitious identity s*attribute.

Qualified identity

Status of a local digital identity that has been retrieved from the INSi teleservice, and successfully checked for consistency with individual's traits shown by a highly-trusted identity scheme.

Retrieved identity

Status of a local digital identity that has been retrieved from the INSi teleservice after being successfully matched against the individual's traits but which could not yet be checked against a highly-trusted identity document.

Sensitive identity

The term "sensitive identity" is used generically to cover all cases where there is a legally-enforced right to confidentiality, particularly in terms of anonymity of care.

Validated identity

Status of a digital identity that has not been retrieved from the INSi teleservice but has been checked for consistency with the set of traits shown by a highly-trusted identity scheme, thus ensuring that there are no errors in the recording of a patient's identity traits.

Test identity

A fictitious identity created to evaluate the functioning of an information system in the context of a creation, modification, or update. In a real identity database, it must be subject to the use of the attribute “questionable identity”.

Identity security

Policy, arrangements, and means implemented to ensure the reliability of a patient's identification at all stages of their care.

INSi

Online service of the CNAM to search and download the INS.

Sets of traits

A group of characteristics (or traits) of a patient which allow that person to be uniquely described.

Place of birth

Identification of the place of birth which includes several parameters filled out in the mandatory and additional traits: Name of the municipality (commune), postal code, and official INSEE geographical code for persons born in France; country and INSEE code of the country for persons born abroad.

INS number

INS identifier, represented by the patient's personal NIR or NIA.

Electronic identification means

A tangible and/or intangible element containing personal identification data and used to authenticate oneself for an online service.

NIA

This is the *numéro d’immatriculation d’attente* (NIA, “temporary registration number”) allocated by the CNAV to persons born abroad on the basis of civil status data (Article R.114-26 of the Social Security Code). The NIA becomes the NIR once the identity of the person has been confirmed and no duplication with another NIR is possible. In the absence of a NIR, the NIA is the INS number for persons receiving care in the health and social care sectors (Articles L.1111-8-1, R.1111-8-1 et seq. of the Public Health Code).

NIR

The *numéro d'inscription au répertoire des personnes physiques* (NIRPP or NIR, "national Individual Registration number") is used to identify a person in the national identification register of natural persons (the RNIPP) managed by INSEE.

The personal NIR is the INS number for persons receiving care in the health and social care sectors (Articles L.1111-8-1, R.1111-8-1 et seq. of the Public Health Code).

The NIR is assigned:

- either by INSEE when registering someone in the RNIPP; registration generally takes place no later than eight days after birth, on the basis of the civil status transmitted by a town hall (sex, year and month of birth, department and commune of birth, civil status register number)
- or by the CNAV when registering someone in the national identity management system (SNGI) at the request of a social security organisation, when steps are taken either by the person on their own or by their employer.

The two systems are synchronised on a daily basis.

Family name

The term *family name* has officially replaced the terms *patronymic name*, *surname at birth*, and *maiden name*. It is transmitted according to rules set by parentage. It is always included in the birth certificate.

The ability to change one's family name is provided for in Articles 60 to 62-4 of the Civil Code. It may be linked to the procedure for the "francization" of surnames and/or given names for persons acquiring or regaining French nationality.

Note: For better understanding, it was decided to continue to use the term *surname at birth* in the RNIV, as patients tend to confuse *family name* and *customary name*.

Maiden name (obsolete) = family name = surname at birth

Married name (obsolete): See "customary name"

Surname at birth = family name

Patronymic name (obsolete) = family name = surname at birth

Customary name

The *customary name* is a surname drawn from a civil status document (marriage or birth certificate, etc.). It is normally specified on an official identity document after the phrase "Nom d'usage" (Customary Name).

It may change based on civil status documents (divorce, remarriage). If identity documents are not kept up to date, it is sometimes inconsistent with the name actually used by the patient, which makes it an unreliable identity trait, especially as the patient may decide not to use it in all or some of their activities.

Note: It is recommended that the term *customary name* be preferred to the outdated term *married name*.

Usual name = customary name

Surname used

In place of the *customary name*, which has a legal definition, the RNIV has created the term *surname used* to allow the recording of the name actually used in everyday life, whether it is the *surname at birth* or the *customary name*, or even, under certain conditions, the name used in the *pseudonym* or *nickname* of the patient. This additional trait is intended to facilitate dialogue between the caregiver and the patient.

Entitlement holder

A person affiliated with a compulsory health insurance scheme. This affiliation allows that person to "give rights" to other persons called "entitled persons" (e.g. their minor children).

Given name(s) at birth

The assignment of a given name is compulsory: It is indicated on the birth certificate. It may include several given names, as well as compound names.

First given name at birth

The distinction of the *first given name* in the list of names given at birth is necessary for communication between software that has not yet been made compliant with RNIV requirements. It can be compound (with or without hyphens between the given names).

Usual given name

Any given name recorded in the birth certificate may be chosen as the usual given name (Art. 57 of the Civil Code). This choice can be made after the words "Prénom usuel" under the heading "Prénom(s)" on the identity document. However, sometimes the given name used in everyday life is different from the first given name at birth, and has never been made official.

Customary given name = Usual given name

Given name used

Instead of the *usual given name*, which has a legal definition, the RNIV has created the term *given name used* to enable the recording of the given name actually used in everyday life. This may be one of the *given names at birth*, the *customary name* or, under certain conditions, another unofficial name – as may be customary in some regions – or one used in the patient's *pseudonym* or *nickname*. This additional trait is intended to facilitate dialogue between the caregiver and the patient.

Data controller

According to the General Data Protection Regulation (GDPR), the controller is the legal person (facility) or natural person (professional) who determines the purposes and means of a processing operation, i.e. the objective and the way in which it is carried out. In practice and in general, it is the artificial person as embodied by its legal representative.

Pseudonym

An assumed identity or "alias" freely chosen by a person to conceal their real identity in the course of a particular activity, especially in the literary or artistic world. It is not subject to any particular regulation and cannot be mentioned on civil status documents. A pseudonym may, however, appear on the identity card if its reputation is confirmed by constant uninterrupted use (e.g.: "Johnny Halliday"). It is preceded by the words "Pseudonyme" (Pseudonym) or the adjective "Dit" (alias) on a specific line[25].

It can be mentioned in the fields *surname used* and *given name used* if all three of these conditions are met: (1) it is at the patient's express request, (2) it is a trait that is not likely to change with each visit, (3) it is compatible with the facility's identity security policy.

Identity reconciliation

Assigning a common digital identity (known as a federation identity) to multiple digital identities belonging to different identification domains (at the territorial or regional level) which nonetheless refer to the same patient.

Single identity repository

Set of components (technical and organisational) of the information system that guarantees the consistency of identity data for all the business software that manages personal information about the patients receiving care.

[25] To be distinguished from the word "dit" in the surname line which is an integral part of the person's surname at birth

Sex

Sex is coded as M (male), F (female) or I (indeterminate). The INS can only contain F or M values.

Healthcare facility

This term is used generically in this document to identify the establishments, private practices, services, and organisations involved in the health care or social care of a patient.

Nickname

This is an identity trait that may be mentioned on the birth certificate if there is a fear of confusion between several namesakes; in such a case, it is preceded by the adjective "Dit" (alias) on a separate line from the surname.

It can be mentioned in the fields *surname used* and *given name used* if all three of these conditions are met: (1) it is at the patient's express request, (2) it is a trait that is not likely to change with each visit, (3) it is compatible with the facility's identity security policy.

(Identity) traits

These are patient-specific identification elements of varying importance: A distinction is made between strict and additional traits (see also: Set of traits).

Mandatory traits

These are reference identity traits that allow an individual to be officially identified without risk of error: surname at birth, given name(s) at birth, first given name at name, date of birth, sex, country of birth (for patients born abroad) or place of birth (for patients born in France, including the overseas areas known as DOM, COM, and POM), INS number.

Additional traits

This is personal information, which may change over time, and provides additional information for the proper management of the patient. For example: given name used, surname used, address, etc.

Patient

This term is used generically in this document to identify the people cared for by the healthcare facilities, including residents as well as patients.

Identity theft

According to Article 226-4-1 of the Criminal Code, this is an offence consisting of using the identity of a third party for malicious purposes. In health care, these situations involve fraudulently using an identity in order to benefit from the social security coverage of another patient, often with the latter's complicity.

ANNEX III – Requirements and recommendations

Common requirements and recommendations for information systems

Exi SI 01	The information system must, at a minimum, allow a search for a digital identity to be carried out on the basis of: - all or part of the INS retrieved after the INSi teleservice query; - the entry of the date of birth, possibly supplemented by the first characters of the surname or given name.
Exi SI 02	The use of the INS number for the existing identity search must be secured to avoid any risk of input error. If the INS number is not retrieved electronically, the entry of the 15 characters of the NIR and their validation by the control key is mandatory for any search on the basis of the INS number.”
Exi SI 03	When searching for a patient in the identity database, it is necessary for the information system to query without distinction, with the corresponding data but without taking into account hyphens or apostrophes, the fields *Surname at birth* and *Surname used*, as well as the fields *Given name(s) at birth, First given name at birth and Given name used*.
Exi SI 04	Identification traits must be the subject of specific fields in the information system.
Exi SI 05	The information system must allow for the entry of the additional traits *Surname used* and *Given name used*.
Exi SI 06	The information retrieved from the INSi teleservice is stored and tracked in the health information system.
Exi SI 07	Any health information system must be able to assign one of four trust statuses to each stored digital identity.
Exi SI 08	The information system must ensure that only *qualified identity* status allows the listing of health data exchanged with the INS number, in compliance with the applicable regulations.
Exi SI 09	For digital identities with a *questionable identity* or *fictitious identity* attribute, it must be made impossible for the software: - to assign a status other than provisional identity - to make a query to the INSi teleservice.
Exi SI 10	The type of identity scheme used to collect the identity must be recorded. Only a highly-trusted document, or its digital equivalent, shall allow the status of *validated identity* or *qualified identity* to be assigned.
Exi SI 11	It is important that the nature of each identity trait displayed on documents and human-machine interfaces are easily recognised, without risk of misunderstanding, by all healthcare providers involved.
Exi SI 12	After the qualified identity or retrieved identity status has been assigned, the INS traits shall replace, if not already present, the local mandatory traits in the corresponding fields.
Exi SI 13	Facilities must have a single identity repository ensuring data consistency for all software that manages patients' personal information.
Exi SI 14	It is essential that accesses and modifications to identities are logged (date, time, type of modification and professional who carried out the action). Successive retrievals of the INS must also be recorded.
Exi SI 15	Information systems may allow dates of birth in a lunisolar calendar to be translated into DD/MM/YYYY format for patients born abroad.

Reco SI 01	"It is recommended that health information systems allow the use of additional attributes to enable professionals to characterise digital identities requiring special treatment.
Reco SI 02	It is recommended that the information system must have dedicated functionalities to search for anomalies in the recording of identity traits.

Common requirements for professional practices

Exi PP 01	Querying the INSi teleservice is mandatory to verify a received INS when the digital identity does not exist or does not have Retrieved or Qualified status.
Exi PP 02	The creation of a digital identity requires the capture of information in at least five mandatory traits: surname at birth, first given name at birth, date of birth, sex, and place of birth.
Exi PP 03	The fields relating to the list of given names at birth and the INS number are filled in as soon as it is possible to access this information: Presentation of an identity document and/or query to the INSi teleservice (in cases where use of the INS number is required and authorised).
Exi PP 04	It is necessary to fill in as many additional traits as possible, according to the instructions that each facility defines according to their needs.
Exi PP 05	Before any integration of the INS into the local digital identity, it is necessary to validate the consistency between the INS traits returned by the INSi teleservice and the traits of the individual receiving care.
Exi PP 06	Whenever possible, querying the INSi teleservice via the Carte Vitale is the preferred method of querying whenever possible.
Exi PP 07	The assignment of a trust level to any digital identity is mandatory.
Exi PP 08	In order to use a trusted digital identity, it is essential to ensure, at least when the patient first makes physical contact with a facility, that the identity documents presented correspond to the person being cared for.
Exi PP 09	Validating a digital identity without being able to check its consistency against a highly trusted identity credential, or its digital equivalent, the type of which is duly recorded in the information system, is strictly prohibited.
Exi PP 10	At a minimum, the following mandatory traits must be displayed: surname at birth, first given name at birth, date of birth, sex and, on documents containing health information data, the INS number followed by its nature (NIR or NIA) when this information is available and its sharing is authorised.
Exi PP 11	Once the identity has been upgraded to *qualified identity* status, the INS number and the INS traits must be used to identify the patient, particularly when exchanging health data concerning that person.
Exi PP 12	The organisations must have an application map detailing in particular the identity-related flows. Non-interfaced tools that require human intervention to update identities must be identified.
Exi PP 13	An IT charter formalising the rules of access and use of the information system, and in particular for applications managing personal health data, must be drawn up within each group practice.
Exi PP 14	Healthcare providers affected by the dissemination of an INS-related error must be alerted without delay, using a specific procedure formalised by the facility.
Exi PP 15	Group medical practices must formalise the institutional patient identification policy in an identity security charter.

Exi PP 16	As with other mandatory traits, the date of birth to be recorded is the date of birth from an official identity document or scheme, not the date of birth read on a health insurance document, which may be different.
Exi PP 17	Recording the *surname used* is mandatory when it is different from the *surname at birth*.
Exi PP 18	Recording the *given name used* is mandatory when it is different from the *first given name at birth*.
Reco PP 01	In order to obtain relevant results, it is strongly recommended to limit the number of characters entered when searching for a record.
Reco PP 02	It is important that any difficulty encountered in retrieving the INS or qualifying the digital identity, due to a non-minor inconsistency, is reported as an adverse event, including at the regional and national level[26].

The requirements of the RNIV supplement those of the INS Reference Document.

[26] The methods for reporting at the regional and national levels will be specified later

ANNEX IV – Rules for recording identity traits

The following general rules apply to the manual recording of identity traits.

Surname at birth (family name)

This mandatory trait must be recorded (see Exi PP 02). It must be entered as it appears on the *nom* ("surname") line of the identity document, in unaccented capital letters, without diacritical marks and without abbreviation**.** For patients who do not have a surname at birth (e.g. an empty field on their identity document or a series of X's), the name will be entered as SANSNOM ("NO SURNAME"). As with the INS, hyphens and apostrophes must be retained. However, other characters such as "/" must be replaced by a space.

Note: For some patients of foreign origin, the identity document does not specify the surname at birth. In this case, the trait is recorded "on the basis of the patient's own statements". But, as this is a mandatory trait, the digital identity will have to remain at "provisional identity" status until this information is proven with an identity document from the country that distinguishes the different identity traits.

Individual cases must be decided on a case-by-case basis and reported to the regional or even national level. They are also the subject of practical information sheets formalised by the network of regional identity security contacts (3RIV).

An internal procedure must describe how an approximate or fictitious surname at birth can be given in situations where an unaccompanied and unidentifiable patient (comatose, non-communicative, delirious) is admitted or asserts their rights to anonymity.

First given name at birth

This mandatory trait must be recorded (see Exi PP 02).

Civil status allows a compound given name (e.g.: Jean-Pierre) but, as it is not mandatory to link the two parts of the compound name by a hyphen (e.g.: Jean Pierre), this can make it difficult for the person responsible for recording the digital identity. In this situation, it is possible to rely on:

- either the identity document presented, if it uses a comma to separate the first names, by recording the given names before the first comma, as they appear
- or the instructions given by the patient (or their representative).

The consideration of special cases (e.g. compound names without hyphens) must be decided on a case-by-case basis.

For patients who do not have a given name at birth (e.g. an empty field on their identity document or a series of X's), the name will be entered as SANSPRENOM ("NO GIVEN NAME").

An internal procedure must describe how an approximate or fictitious first given name at birth can be given in situations where an unaccompanied and unidentifiable patient (unconscious, non-communicative, delirious) is admitted or asserts their rights to anonymity.

Given name(s) at birth

This field is one of the mandatory traits to be filled in as soon as an identity document can be accessed (see Exi PP 03). It must be entered as it appears on the *prénom* ("given name") line of the identity document, in unaccented capital letters, without diacritical marks and without abbreviation. For patients who do not have a given name at birth (e.g. an empty field on their identity document or a series of X's or SP), the name will be entered as

SANSPRENOM (“NO GIVEN NAME”). As with the INS, hyphens and apostrophes must be retained, but if there are commas separating the given names on the identity document, these must not be recorded.

Note: The INS list of given names may include compound given names, with or without a hyphen, but it does not use a comma to separate the given names (see First given name at birth).

Individual cases must be decided on a case-by-case basis and reported to the regional or even national level. They are also the subject of practical information sheets formalised by the network of regional identity security contacts (3RIV).

Date of birth

This mandatory trait must be recorded (see Exi PP 02). It is entered and displayed locally in DD/MM/YYYY format.

As with other mandatory traits, the date of birth to be recorded is the date of birth from an official identity document or scheme, not the date of birth read on a health insurance document, which may be different[27]. [Exi PP 16]

Information systems may allow dates of birth in a lunisolar calendar to be translated into DD/MM/YYYY format for patients born abroad. [Exi SI 15]

Where the date of birth provided by the identity document or digital identification scheme is incomplete, the following guidelines must be applied:

- if only *the day* is unknown, it is replaced by the first day of the month (01/MM/YYYY)
- if only *the month* is unknown, it is replaced by the first month of the year (DD/01/YYYY)
  if both *the day AND the month* are unknown, the date of 31 December of the year of birth (31/12/YYYY)[28] must be entered
- if *the year* is not known precisely, the estimated year or decade is used
- if the date of birth is unknown, 31/12 and a year or decade consistent with the announced or estimated age is recorded, e.g. 31/12/1970.

Note: If the information system allows it, a specific marker like "Dummy date", "Provisional date", "Uncertain date” etc. must be used to differentiate real dates of birth from cases where the date is interpreted with the above rules. This marker can be transmitted by computer.”

Sex

This mandatory trait must be recorded (see Exi PP 02). The sex code (M or F), as shown on the identity document when presented, is entered; it is also possible, on a provisional basis, to use the code 'I' for *indeterminate*[29].

Note: In a gender reassignment procedure, the consideration of the change of identity may be decided locally according to an internal protocol. It may be based, for example, on the judgment of the administrative court showing the old and new identities. Whatever the case, the identity must be reset to ***provisional identity*** status to allow for the modification of mandatory traits (with the deletion or invalidation of the INS number if it was recorded). It will then be necessary to wait for the presentation of a highly-trusted identity document with the new identity (see 3.3.3.2) to assign the status of ***validated identity*** and then, after retrieving the new INS via the dedicated teleservice, that of ***qualified identity***.

[27] The use of Assurance Maladie (Health Insurance Fund) data for billing is not within the scope of the RNIV (see 1.2)

[28] This instruction is not applicable for a child < 1 year old in hospital (date of entry into care is prior to the date of birth). In such a case, it is recommended to estimate the month of birth approximately (01/mm/YYYY).

[29] This may be the case especially for children under 2 years of age where gender may temporarily be difficult to determine. The INS returned by the INSI teleservice can only contain F or M values.

Place of birth

This mandatory trait must be recorded (see Exi PP 02).

For persons born in France, the official INSEE geographical code (COG)[30] corresponding to the municipality (*commune*) of birth must be recorded. For persons born abroad, the INSEE code of the country (starting with 99) must be recorded[31] and, if desired by the facility, the city of birth.

Note: The name of the commune of birth (for all) and the postcode (for French communes) are not part of the mandatory traits but can be recorded in ad hoc fields of the additional traits. In this case, for persons born in France, it is desirable that the information system be able to suggest the INSEE code from either of these data, if entered manually. As the INSEE code of the commune of birth is the one that was valid on the patient's date of birth, there may be a discrepancy between the code entered manually and the code returned by the INSi teleservice. When this occurs, the INS code prevails: It must replace the previous one (see Annex VI).

If the place of birth is unknown, code 99999 must be used.

The surname used

Recording the *surname used* is mandatory when it is different from the surname at birth. [Exi PP 17]

This field is intended to record the surname used by the patient in their everyday life. As with the surname at birth, it must be entered in unaccented capital letters, without diacritical marks or abbreviations but with hyphens and apostrophes.

As this is an additional trait, it does not affect the status of the digital identity. Each healthcare facility defines the rules for inputting this field into its information system, depending on its identity security policy, its activities, its patient base and even the contractual obligations it may have with other facilities. The choice can be made to limit its use to recording only the civil status information mentioned on an identity document or to agree to record any surname actually used by the patient (see 3.1.3.3). The facility may also decide to make the entry of this trait mandatory, even when the surname used is identical to the surname at birth.

- Where the surname used is the *customary name* (see Annex II), it corresponds to the name entered on the *nom d'usage* ("customary name") line of the identity document presented, without the preceding reference such as: "époux/se de", "divorcé/e de", "veuf/ve" ("spouse of", "divorced with", "widow/er of") or the abbreviations for them in French titles ("Ep.", "Div.", "Vve") or their equivalent on foreign documents.

  Note: the actual use of the surname mentioned on the identity document may change on the occasion of civil status events (marriage, divorce, etc.). It is up to the facility to assess the relevance of taking into account unofficial changes and/or to invite the patient to have their identity document updated by the civil status registries[32].

- When the surname used is the *surname at birth* – if the facility has chosen to populate the field in this situation – the information system can usefully facilitate the user voluntarily copying that name from the *surname at birth* field.

- For persons who do not use their full surname at birth in everyday life, recording may be limited to the part of the surname actually used (fictitious example: for Mr SAINT JOUAN DE LA FRAIRIE, who uses only the first part of his surname (SAINT JOUAN) in everyday life, only that part will be recorded).

[30] https://www.INSee.fr/fr/information/2560452
[31] https://www.insee.fr/fr/information/2028273
[32] https://www.service-public.fr/particuliers/vosdroits/R19902

- This field can also be used to record the name part of the *pseudonym* or *nickname* (see Annex II), provided that it is: (1) at the patient's express request; (2) a constant trait, used at each visit; (3) compatible with the facility's identity security policy.

The given name used

Recording the *given name used* is mandatory when it is different from the *first given name at birth*. [Exi PP 18]

This field is intended to record the given name used by the patient in their everyday life. As with the given name at birth, it must be entered in unaccented capital letters, without diacritical marks or abbreviations but with hyphens and apostrophes.

As this is an additional trait, it does not affect the status of the digital identity. Each healthcare facility defines the rules for inputting this field into its information system, depending on its identity security policy, its activities, its patient base and even the contractual obligations it may have with other facilities. The choice can be made to limit its use to recording only the civil status information mentioned on an identity document or to agree to record any given name actually used by the patient (see 3.1.3.3). The facility may also decide to make the entry of this trait mandatory, even when the given name used is identical to the first given name at birth.

- When the given name used is one of the *given names at birth*[33]*,* the information system can usefully facilitate the populating of this field by suggesting that the user voluntarily copy all or some of the *given name(s) at birth* or the *first given name at birth* field.
- Where the given name used is the *usual given name* (see Annex II) officially declared to the civil status authorities, it corresponds to what is entered on the ad hoc line of the identity document presented.
- This field can also be used to record any given name commonly used by the patient without having been formalised or forming part of their *pseudonym* or official *nickname* (see Annex II), provided that it is: (1) at the patient's express request, (2) a constant trait, used at each visit, (3) compatible with the facility's identity security policy.

[33] Article 57 of the Civil Code

ANNEX V – Primary identification without the patient's physical presence

The development of telemedicine, the use of remote registration tools and applications facilitating the coordination of patient care by multiple healthcare professionals increases the number of unique identification situations. The transmission of health information by computer and the application of rules concerning the use of the INS number require the implementation of special conditions for securing primary identification by facilities carrying out procedures without the patient's physical presence.

Carrying out procedures on behalf of a third party that has no direct link with the patient

When a service provider is responsible for carrying out procedures at the request of another professional ("prescriber") without being able to verify the identity of the patient for whom it is carrying out the service, due to the patient's absence, the responsibility for primary identification rests with the facility issuing the request (see 3.1.2.3). This is the case, for example, for:

- medical biology and pathological anatomy and cytology laboratories
- the French Blood Establishment (EFS) and the Armed Forces Blood Transfusion Centre (CTSA)
- carrying out professional assessments such as multidisciplinary consultation meetings (RCPs) when the patient is not known to the organising facility
- a request for care pathway coordination made by a healthcare provider

There are several different cases, depending on the existence of a previous record of the patient, their status, and the confidence that the provider has in the quality of the identity addressed.

The provider has full confidence in the quality of the identity addressed

The prescriber and the provider are normally bound by a contract that guarantees, among other things, the quality of the prescriber's identity security procedures. In this case, the provider who receives a digital identity may, as an exemption to the general rule, consider it as a:

- *Qualified identity* when it is transmitted with the INS number and the qualifier "validated" in the interoperability message, even if there is no chance of verification by the INSi teleservice (an exception to the rule, which remains the preferred procedure)
- *Validated identity* when transmitted without the INS number with the qualifier "validated" in the interoperability message
- *Provisional identity* in other cases.

In a case where the identity is not received in digital format, the query to the teleservice is mandatory if the identity is not known to the provider or does not have a retrieved or qualified status (see 4.2.3.2 and Exi PP 01).

If the patient is not yet known to the provider, the provider creates a digital identity using the traits and status deduced from the transmission by the prescriber.

If a corresponding local digital identity is already recorded with a status of *validated identity* or *qualified identity*:

- the receipt of a *validated* or *qualified identity* authorises the direct populating of the patient's local file
- in the case where the identity is transmitted with a lower level of trust and the provider is not in a position to clear up the doubt (by contacting the prescriber, for example), rather than risk creating a collision the provider must create a new digital identity as would be done for a patient with a similar identity (using the *similar identity* attribute if it is available).

The provider shall not spread the INS number transmitted by the prescriber to other correspondents except in the case where the local digital identity has qualified identity status.

The provider cannot guarantee the quality of the identity addressed

When the prescriber is unknown to the provider or when the quality of its identity security practices is not contractually guaranteed, the special instructions in the previous section cannot be applied. The transmitted identity must be taken into account using the common rules in force, which prohibit validating the traits without the opportunity to check consistency from an identity scheme and recording the INS number without querying the teleservice for verification (see 3.1.2.3).

As the provider is not able to qualify the digital identity, it must not spread the INS number transmitted by the prescriber to other correspondents.

Carrying out a procedure with a patient remotely present (telemedicine)

The use of telemedicine tools is set to become more frequent as a result of the development of eHealth. Telemedicine involves carrying out procedures at a distance:

- carrying out a clinical or technical examination (teleconsultation, telediagnosis, teleimaging, telemonitoring, etc.)
- exchanging opinions between healthcare professionals (tele-expertise)

Collecting and validating the identity remotely, when no professional is physically with the patient, requires several conditions:

- the collection and recording of their digital identity (possibly through a substantial eIDAS-certified digital identification scheme, see 3.3.3.2)
- checking for consistency between the digital identity and that of the physical patient on the day of the consultation

When the patient is accompanied by a professional carer, that carer is responsible for certifying the patient’s real identity. If none is present, it may be necessary to use dedicated authentication tools or, where possible, to ask the patient to present their identity document to the camera.

When a digital identity creation is required for an unknown patient, a query to the INSi teleservice can be made by the facility in order to retrieve an INS and to assign a corresponding level of trust.

It is essential to use best practice when searching for existing records (see 3.1.1). This is particularly the case in situations where access to images and reports is authorised via a portal to healthcare professionals involved in the care of a patient (general practitioner, specialist, team participating in a multidisciplinary consultation meeting, etc.). These practices are governed by an ad hoc procedure.

Example of teleimaging

Teleimaging (in radiology and nuclear medicine) is a telemedicine procedure that allows a specialist to consult images remotely[34] with the aim of:

- either interpreting an examination carried out at another site, in conjunction with professionals in direct contact with the patient (requesting doctor, medical electroradiology technician in charge of the technical procedure, etc.)
- or exchanging an opinion with a colleague in the same speciality who requests it on a particular case

Direct dialogue between professionals, which is mandatory in this type of activity, is supposed to facilitate the patient identification stage. Whatever the urgency, it rests with the facility that initiated the request. The

[34] HAS. Tele-imaging memo sheet, May 2019 (https://www.has-sante.fr/upload/docs/application/pdf/2019-07/fiche_memo_teleimagerie.pdf)

stakeholders must ensure that the examination – interpretation and archiving of images – is properly identified with the known traits of the person being examined.

Whether it is for creating a new file or in the case where the patient already has a digital identity in the information system – subject to the traits provided being consistent with the previously recorded data – the status of the local digital identity is assigned according to several parameters:

- *Qualified identity* if the INS is provided OR this status was already assigned locally OR the consistency check shows that the identity matches a local identity previously recorded as a *retrieved identity*
- *Validated identity* if the consistency check between the identity sets has been carried out or if this status was already present
- *Retrieved identity* if this status existed before and the consistency check has not been carried out
- *Provisional identity* in other cases.

In all cases, this practice must be governed by a partnership agreement that specifies the technical details of digital exchanges in order to guarantee their security. In particular, it must specify the case where:

- the provider is authorised to connect to the requesting facility's imaging information system (PACS[35]), which allows the provider to interpret the images directly in the system after ensuring that they are connected to the right file
- the connection is not direct or involves shared iconography (e.g. use of a dedicated territorial or regional platform), which requires strict application of the rules for searching existing files in order to avoid the risk of an error (see 3.1.1).

Remote registration of a patient

There are more and more situations where the primary identification of the patient is achieved through an upstream appointment/pre-consultation/pre-admission solution within an online patient portal involving the patient in the management of their own digital identity. This type of solution is similar to an identity repository based on an identification domain different from that of the facility/professional, since the identities it contains are created/updated on the patient's own initiative.

In these appointment/pre-consultation/pre-admission solutions within an online patient portal, an identity can acquire the status of qualified identity, if the patient's registration has been accompanied by a verification of their identity through a substantial eIDAS-certified electronic identification scheme and the query to the INSi teleservice. In this case, the entire INS (including the INS number and its OID) can be transmitted to the HIS. Re-qualification of this identity in the facility's identification domain is not necessary when the two identification domains (upstream and facility patient repository) are held by the same legal entity.

In the absence of qualified identity status, the INS number (and its OID) are not transmitted to the HIS: only the traits are transmitted (possibly retrieved via the INSi teleservice).

Registration via a substantial eIDAS-certified digital identification scheme (see 3.3.3.2) makes it possible to secure the digital identity created, provided that the traits expected by the information system are actually filled in during the procedure, but it does not make it possible to ensure that the person recorded is actually the person who will be cared for. It is therefore not possible to validate a digital identity created remotely before ensuring that the registered patient is the one who is benefiting from the service. The digital identity collected, which is very incomplete, can therefore only have the status of *provisional identity*[36].

[35] Picture Archiving and Communication System

[36] Or from an identity with *retrieved identity* status if the tools evolve, allowing the INSi teleservice to be queried for retrieval.

It is the responsibility of the facility to implement identity security best practices when the patient actually comes to the facility, in order to complete the data, to link it to an existing file if the patient was already known, and to change the status of the digital identity accordingly (see 3.3.1).

ANNEX VI – Assessing the consistency of the INS

- **When is it necessary to assess this consistency?**

  The different situations where it is necessary to assess the consistency between the INS and the locally identified traits are the following:
  - an identity is being created via the teleservice (see 3.1.2.1)
  - querying the teleservice for retrieval when a digital identity has already been created locally (see 3.1.2.2 and 3.1.2.3)
  - a qualified identity verification operation has failed (see 4.2.3.2 and 4.2.3.4)
  - health data transmitted by a healthcare provider outside the facility has been received (see 3.1.2.3).

- **Why is this assessment necessary?**

  In the case of INS retrieval, the aim is to check that the traits proposed by the INSi teleservice correspond to those of the identity sought before agreeing to record them in the local information system.

  In the case of INS verification, the objective is not to transmit an invalid INS before investigating the cause of the verification failure.

  In the case of receiving health data, the aim is not to include information that could belong to another patient (collision).

- **What are the potential sources of divergence?**

  The lack of consistency between the reference traits shown by the INS and the local information can have different sources:
  - a local origin, which may be linked to an error in the manual input of the lines (letters swapped, etc.), the use of old input rules, or even an error in selecting the file before querying the teleservice or the beneficiary listed on the Carte Vitale, when the query is made by this means
  - the differences that may exist between the identity document and the identity in the *Répertoire national d'identification des personnes physiques* (national identification register of natural persons, *RNIPP*), due to civil status rules specific to each domain or the use of commas to separate given names
  - patient identification error prior to the transmission of health data by a healthcare provider.

- **What should I do if I find a problem?**

  Depending on the nature of the discrepancy, it may be decided to:
  - validate the acceptable differences: the set of traits in the INS then become those to be used as mandatory traits (see Exi SI 12 and Exi PP 11)
  - reject the identity presented by the teleservice and thus to keep the locally entered traits[37]
  - investigate the origin of the problem, especially when significant differences between the identity retrieved through the teleservice and the highly trusted identity document presented to validate the digital identity are found afterwards
  - update the status of the digital identity accordingly (see Annex VII)
  - not automatically integrate health data transmitted by another healthcare provider if there is any doubt about the associated identity (risk of collision).

[37] The identity on a highly trusted identity scheme takes precedence over all others

- **How can this search for consistency be organised?**

The consistency check is carried out when the patient visits the centre, preferably in their presence, or when data concerning that person is received (identity document for updating data, health data transmitted by a third party).

When the INS traits from the teleservice are accepted, the recorded identity is then given the status of *qualified identity* (excluding the *fictitious identity* and *questionable identity* attributes) – when the validation of the identity is feasible at the time – or *retrieved identity* otherwise.

The qualification process may have to be postponed. This is the case, for example, when the flow of patients to be received is too great or when task overload does not allow the necessary level of vigilance to be ensured. It can then be carried out "in the back office" by dedicated professionals of the facility, provided that the identity of the patient has been verified during the physical reception and that the procedure provides for being able to rely on the identity document that was used to create or modify the patient's file; this requires that it be saved by photocopying or scanning[38].

It is up to the local identity security bodies to formalise in the form of procedure(s) – applicable to all or part of the facility – how the assessment of consistency (between the traits of the local identity document or digital identity and those returned by the INSi teleservice and/or transmitted with health data) is carried out, and by whom. An ad hoc quality document must also provide for the action to be taken according to the results of the periodic verification of qualified identities in the identity repository (see 4.2.3).

- **How to manage discrepancies between sets of traits**

The main sources of inconsistencies known to date, in relation to the nature of the information returned by the INSi teleservice, relate to:

- the existence of empty data in the fields of some patients, mainly those born abroad (see 3.2.1.1)
- the date of birth, which may be in an unusual format by returning null values instead of days and/or months (see 3.2.1.1)
- the place of birth, which uses the INSEE code of the commune that existed at the time of registration with the RNIPP but which may have changed in the meantime (which is not really an inconsistency).

When the inconsistency between the transmitted traits and the local data is considered too large, it justifies not retrieving the INS and/or not integrating the received health data into the patient's file. It is not possible to list all situations exhaustively: They are usually managed on a case-by-case basis and validated collectively, taking into account the procedures applicable locally.

Examples:

- If the discrepancy is found to be related to a local input error[39], the INS is accepted as either a *retrieved identity* or – after identity validation – *qualified identity*.
- If the differences are minor and considered acceptable, priority should be given to the INS. Examples: Different INSEE code of the commune of birth but related to the same commune; given names displayed separately but consistent with the identity document; anomaly related to the presence of hyphens and

[38] Subject to compliance with applicable data retention rules

[39] In this case, the discrepancies can be highlighted by the information system

apostrophes in only one of the two sets of traits; transmitted date of birth different from an interpreted local date of birth (see Annex IV), etc.

- When the inconsistency is related to an error on the identity document, confirmed by the patient, the patient (or their relatives) must be invited to have it corrected by the civil status authorities[40].
- When the differences are more significant and seem to reveal an error in the national reference database (e.g. date of birth inconsistent with the highly-trusted identity document presented locally, error in writing the surname or a given name, etc.), it is preferable not to retrieve the INS; the patient (or a relative) must then be asked to send a request for a correction of civil status to INSEE[41], enclosing a full copy of the birth certificate.
- When the identity transmitted by another healthcare provider is in doubt, the person who transmitted the information must be contacted directly to carry out the necessary checks.

Note: Even in cases where the digital identity has been created with the retrieved INS, the identification of non-minor discrepancies with the highly-trusted identity document after the fact must prevent qualification. It may even be necessary, since the INS is not changeable, to downgrade the digital identity to *provisional identity* (see Annex VII) so that the traits are manually corrected to match those of the highly-trusted identity document – which must automatically result in the deletion (or invalidation) of the originally associated INS number.

- **How to report anomalies**

It is important that any difficulty encountered in retrieving the INS or qualifying the digital identity, due to a non-minor inconsistency, is reported as an adverse event, including at the regional and national level. [Reco PP 02]

[40] https://www.service-public.fr/particuliers/vosdroits/R19902

[41] https://psl.service-public.fr/mademarche/rnipp/demarche?execution=e1s1

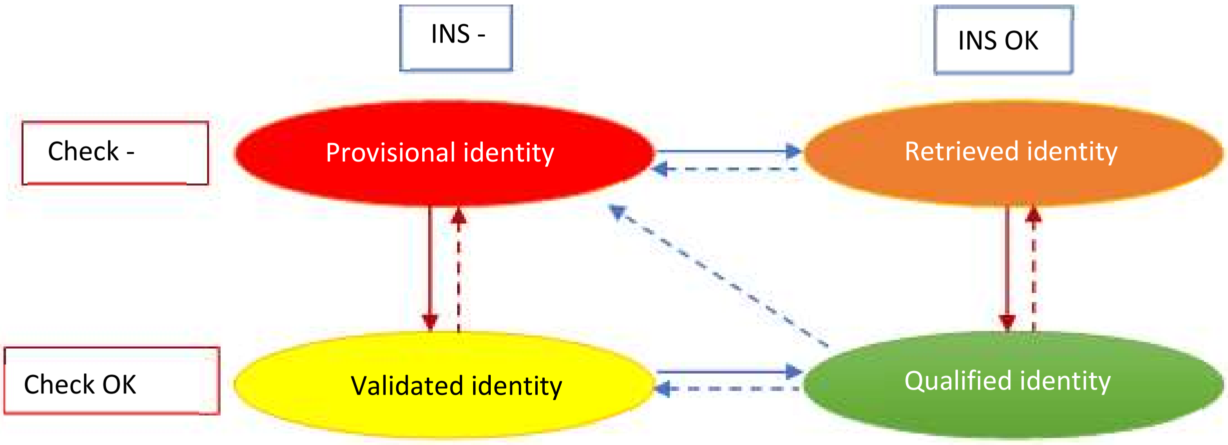
ANNEX VII – Local digital identity statuses

- **Terms for granting a status based on how the digital identity was created**

Step 1	Existing digital identity?	Trusted identity document?	Initial trust status	Step 2	Identity returned by INSi?	Consistent, accepted traits ?	Final trust status	Mandatory traits recorded	Use of INS number?
Patient intake	No	No		INSi TLS query	No		Provisional identity	Those input locally	No
					Yes	Yes	Retrieved identity	Those from the INS	Local
		Yes			No		Validated identity	Those input locally	No
					Yes	Yes	Qualified identity	Those from the INS	Yes
	Yes	No	Provisional identity		No		Provisional identity	Those input locally	No
					Yes	No			
						Yes	Retrieved identity	Those from the INS	Local
		Yes	Validated identity		No		Validated identity	Those input locally	No
					Yes	No	Validated identity or Provisional identity*	Inconsistency to be managed by the facility (see Annex 4)	No
						Yes	Qualified identity	Those from the INS	Yes

**per the facility's choice.*

- **Possible changes to the statuses**



It is possible to upgrade the trust status positively:

- from *provisional* to *validated* or from *retrieved* to *qualified* after a satisfactory consistency check between the digital identity and the patient's identity, as determined by a highly-trusted identity scheme (see 3.3.3.2);
- from *provisional* to *retrieved* or from *validated* to *qualified* after retrieval of the INSi teleservice traits, attesting to their consistency with the local digital identity (see 3.2.1).

Conversely, trust is likely to be degraded in certain circumstances:

- a *retrieved* or *validated* or *qualified* identity that is subsequently found to be related to the fraudulent use of a Carte Vitale must be downgraded to *provisional* Identity with the use of the attribute *questionable identity* (see 3.3.2)

- an inconsistency with the INS returned by the INSi teleservice when retrieving a previously *validated* identity may, if the facility so chooses, result in the downgrading to *provisional* identity status, until the cause of the anomaly is identified and corrected (see Annex VI)
- if a verification operation from the INSi teleservice fails, the digital identity concerned cannot remain in *qualified* identity status, and the INS number must be deleted or invalidated (see 4.2.3.4), adding it to a list of anomalies reported to the operational identity security body.

ANNEX VIII – Displaying identity traits

- **Principles**

The identity traits displayed in accordance with the regulations must be easily distinguishable, without risk of ambiguity, by those concerned (Exi SI 11).

At least the following mandatory traits must be found on documents containing health information data: surname at birth, first given name at birth, date of birth, sex and – if the identity is qualified – INS number followed by its type (NIR or NIA) (Exi PP 10).

On a Human Machine Interface (HMI) or a label, they can be limited to the traits: Surname at birth, first given name at birth, date of birth and sex (Exi PP 10).

It is recommended to add the information on the given name used and surname used if any, and, if necessary, the local reference identifier (e.g. IPP).

It is possible to display the nature of each trait explicitly or abbreviated using the following examples:

Trait	*Explicit nature*	*Abbreviated nature*
Surname at birth	Surname birth:	S.Birth:
Date of birth	Date birth:	DOB:
Place of birth code	Place birth code	INSEE.Birth. :
Sex	Sex:	S:
Given names at birth	Given name(s):	Giv.Nam. :
First given name at birth	First name:	Giv.N.1:
Surname used	Surname used:	S.Us:
Given name used	Given name used:	Giv.N.Us. :
INS number	INS no.:	INS:
Patient identifier	Patient ID:	IPP:

Other alternatives can be used by the facilities, provided that there can be no doubt in the interpretation of the data displayed by different correspondents. For example:

- use a different case for the display of given names and surnames (e.g.: DARK Jeanne)
- separate the first name from the other given names at birth by square brackets or parentheses
- display additional traits, such as given name used and surname used, in parentheses
- precede the surname at birth by *né(e)*
- use a table-based display (see examples)
- etc.

When the INS number is printed, it is not relevant to print the OID, but the nature of the trait (NIR or NIA) must be specified so that the recipient's IT tool can query the INSi teleservice for verification.

Note: If not all characters of the surname and given names at birth can be displayed, it is necessary to indicate this with an asterisk (*) at the end of the displayed character string.

In addition to the "plain text" INS, the display of a datamatrix is planned.

- **Display examples**

The following examples are given for illustrative purposes by taking the traits of the fictitious person cited in § 3.1.3.1 and 3.1.3.3 – Mrs JEANNE, MARIE, CECILE DARK widow LOUIS – and adding the internal identifier of the facility (IPP = 165487).

- **Labels**
  - *Example 1:* S.Birth: DARK Giv.Nam.: JEANNE MARIE CECILE *S*: F *DOB*: 30/05/1960 *IPP*: 165487
  - Example 2: Mrs Jeanne [Marie Cecile] DARK, born on 30/05/1960, called DARK MARIE-CECILE, *IPP*: 165487
  - Example 3:

S. Birth	*Given name(s)*	*S*	*DOB*	*Place of birth*	*Identity used*	*IPP*
DARK	JEANNE (MARIE CECILE)	F	1960-05-30	88154	DARK Marie-Cecile	165487

For the exemption involving identification of biological samples, if a system enabling an identifier to be reliably linked to the identity of the sampled patient is used by the collector, the identity traits might not appear on the label on the tube.

More generally, in addition to a "plain text" display, INS identities are also presented as a datamatrix.

- **Request for exam:**

  Surname at birth: DARK
  Given name(s): JEANNE MARIE CECILE
  First given name at birth: JEANNE
  Sex: F
  Date of birth: 30/05/1960 (INSEE: 88154)
  PID: 165487
  INS: *260058815400233 (NIR)*

- **Referral letter:**

  Surname at birth: DARK
  Given name(s): JEANNE [MARIE CECILE]
  Born on 30/05/1960 in Domrémy-la Pucelle (INSEE: 88154)
  Sex: F
  INS: *260058815400233 (NIR)*
  Surname/given name used: DARK Marie-Cecile

- **Computer screen** *(banner at the top or bottom of each page of the patient's file)*

DARK JEANNE MARIE CECILE *born on* 30/05/1960 (F) – **(qualified)** – *Id. used: DARK Marie-Cecile*

ANNEX IX – Glossary of acronyms used

CNAM:	Caisse nationale d’assurance maladie (National Health Insurance Fund)
CNAV:	Caisse Nationale d'Assurance Vieillesse (National Ageing Insurance Fund)
COG:	Code officiel géographique (Official geographical code: INSEE coding of French communes)
COM:	Collectivité d’Outre-mer (Overseas Collectivity)
CPx:	Health professional card (CPS) or facility card (CPE)
CTSA:	Centre de transfusion sanguine des armées (Armed Forces Blood Transfusion Centre)
DI:	Identification domain
DMP:	Dossier médical partagé (Shared Medical Record)
DOM:	Département d’Outre-mer (Overseas Department)
DP:	Dossier pharmaceutique (Pharmaceutical Record)
DR:	Matching domain
EFS:	Établissement français du sang (French Blood Establishment)
eIDAS:	*Electronic Identification, Authentication and Trust Services* (European regulation to increase trust in electronic transactions)
Exi:	Requirements made enforceable by the RNIV (short for *Exigences*)
RM:	Risk management
GHT:	Groupement hospitalier de territoire (regional healthcare coordination network)
HAS:	Haute Autorité de Santé (France's National Health Authority)
HMI:	Human Machine Interface
INS:	National eHealth ID (“Identité Nationale de Santé” or INS)
INS-C	Calculated INS
INSi:	INS search and verification teleservice
INSEE:	Institut National de la Statistique et des Études Économiques (French National Statistics Agency)
PID:	Identifiant permanent du patient (Permanent patient identifier used in HoISs)
NIA:	Numéro d’immatriculation d’Attente (temporary registration number)
NIR:	Numéro d’Identification au Répertoire des personnes physiques (identification number in the register of natural persons)
OID:	Object identifier (universal identifiers used to ensure interoperability between software)
PACS:	Picture Archiving and Communication System
POM:	Pays d’Outre-mer (Overseas countries: New Caledonia, French Polynesia)
PP:	Professional practices
Reco:	RNIV recommendations for best practices
RCP:	Réunion de concertation pluri professionnelle (multi-professional consultation meeting)
REX:	Retour d’expérience (feedback)
GDPR:	General Data Protection Regulation
RNIPP:	Répertoire national d’identification des personnes physiques (national register of identification of natural persons)
RNIV:	National Identity Security Standard
SNGI:	National Identity Management Service
IS:	Information system
HoIS:	Hospital information systems
HIS:	Health information system

ANNEX X – Regulatory references

- Circular of 28 June 1986 on the implementation of Article 43 of Law 65-1372 of 23 December 1985.
- Law no. 2002-304 of 4 March 2002 on family names
- General Instruction on Civil Status of 2 November 2004
- Article 57 of the Civil Code (amended by Order No. 2005-759 of 4 July 2005)
- Decree No. 2006-6 of 4 January 2006 on the hosting of personal health data and amending the Public Health Code (regulatory provisions).
- Decree No. 2007-960 of 15 May 2007 on the confidentiality of medical information stored on computer media or transmitted electronically and amending the Public Health Code (regulatory provisions).
- Circular No. INT/D/00/00001/C of 10 January 2009 on the preparation and issue of national identity cards.
- Circular of 28 October 2011 on the specific rules for various civil status records relating to birth and parentage
- Circular No. 5575/SG of 21 February 2012 on the civil status Mademoiselle, maiden name, patronymic name and married name
- Law no. 2012-410 of 27 March 2012 on the protection of identity
- Law no. 2013-404 of 17 May 2013 opening marriage to same-sex couples.
- Regulation 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
- Implementing Regulation 2015/1502 of 8 September 2015 setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation 910/2014
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation [GDPR])
- Decree no. 2017-412 of 27 March 2017 on the use of the NIR
- Methodological guide to implementing patient identity within regional healthcare coordination networks (ASIP Santé, 2018)
- Law No. 2019- 774 of 24 July 2019 on the organisation and transformation of the health system (articles L110-4-1 and L110-4-2 of the Public Health Code)
- Ministerial order of 24 December 2019 approving changes to the "National eHealth ID" Reference Document
- Methodological guide for the production of information relating to medical activity and its billing in medicine, surgery, obstetrics, and dentistry. ATIH (annual update).
- Handbook for the certification of healthcare facilities (version 2014 or 2020)
- INSEE nomenclature of municipalities and of foreign countries and territories
- ISO standards (9001, 15189, etc.)
- CI-SIS (https://esante.gouv.fr/interoperabilite/ci-sis)
- https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-reglement-eidas/referentiel-documentaire-lie-au-reglement-eidas/

MINISTÈRE
DE LA SANTÉ
ET DE LA PRÉVENTION
Liberté
Égalité
Fraternité

Direction générale
de l'offre de soins