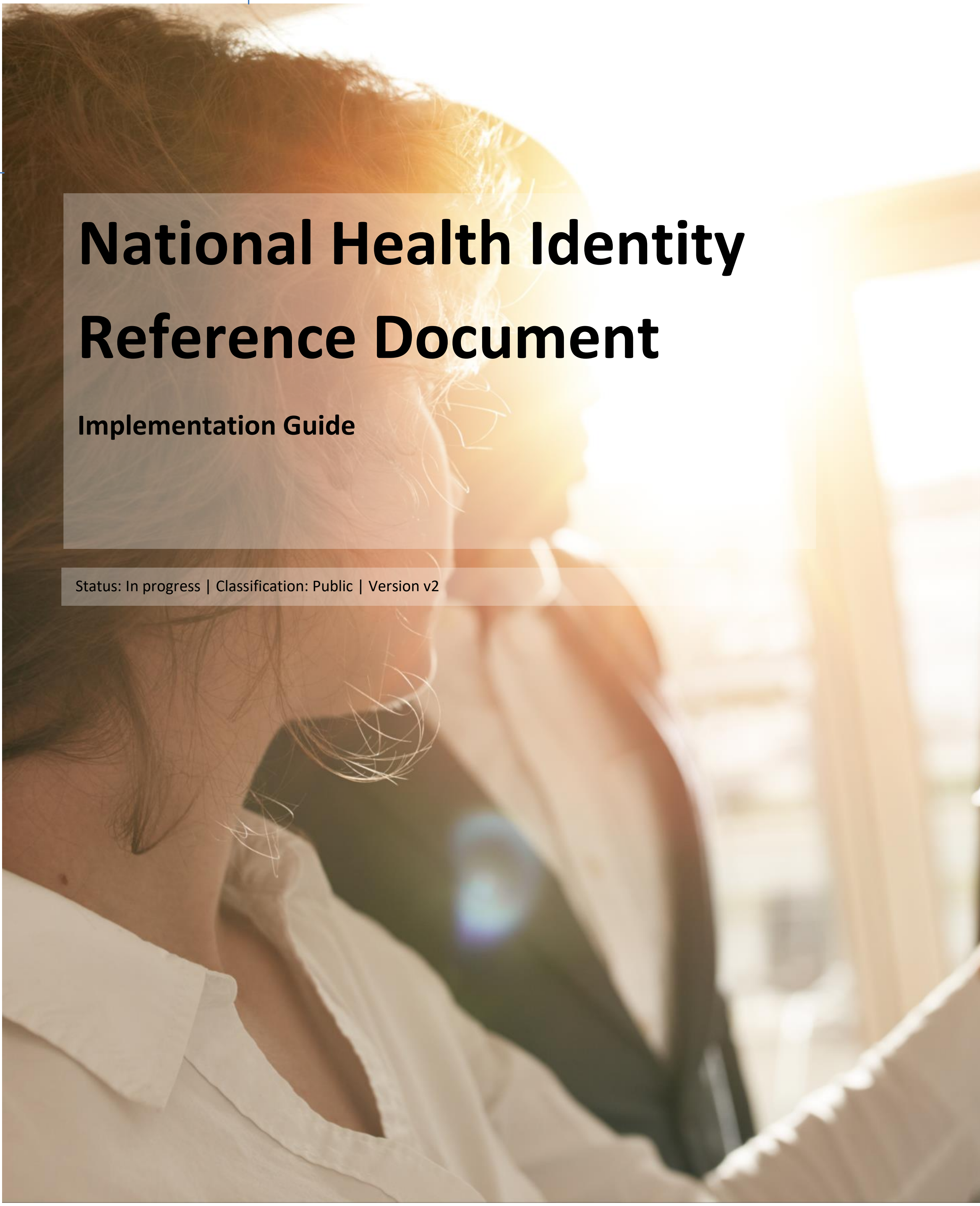
MINISTÈRE
DES SOLIDARITÉS
ET DE LA SANTÉ
*Liberté
Égalité
Fraternité*

AGENCE
DU NUMÉRIQUE
EN SANTÉ



National Health Identity Reference Document

Implementation Guide

Status: In progress | Classification: Public | Version v2

SUMMARY

1. Background and objectives of this document 3

1.1. Background 3

1.2. Objectives of the document 3

1.3. Scope of the document 4

1.4. Texts and reference documents 5

1.5. Document outline 5

2. Components of the INS 6

2.1. Identity traits 6

2.2. Identity status and attributes 11

2.2.1. Identity status and attributes in identity repository software 11

2.2.2. Status in software that does not log identities 13

2.2.3. The business rules associated with the status of the identity 13

3. Distributing an identity – all software 15

3.1. Distributing an identity via paper flows 15

3.2. Distributing an identity via computerised flows 16

3.3. Distributing an identity to populate the DMP 16

4. Retrieving the INS in identity repository software 17

4.1. Use cases of the INSi retrieval operation (non-exhaustive list) 17

4.2. Implementation steps of the INSi retrieval operation. 18

4.2.1. Call to the INSi retrieval operation 18

4.2.2. Traceability of the INSi return 18

4.2.3. Displaying the INSi return and comparing it to any pre-existing traits 19

4.2.4. The populating of identity fields (only if response is "00": A unique identity has been found from INSi). 20

5. Verifying the INS in identity repository software 22

5.1. Use cases of the INSi verification operation (non-exhaustive list) 22

5.2. Implementation steps of the INSi verification operation. 23

5.2.1. Call to the INSi verification operation. 23

5.2.2. The traceability of the return from the INSi verification operation call. 23

5.2.3. Managing the INSi return 23

6. Verifying the INS in the software 25

6.1. Use cases of the INSi verification operation (non-exhaustive list) 25

6.2. Implementation steps of the INSi verification operation. 25

6.2.1. Call to the INSi verification operation. 25

6.2.2. *The traceability of the return from the INSi verification operation call.* 26

6.2.3. *Managing the INSi return* 26

7. Monitoring **27**

1. BACKGROUND AND OBJECTIVES OF THIS DOCUMENT

1.1. Background

The National Health ID (INS) initiative is one of the flagship projects of the eHealth roadmap. This project is intended to **have all actors use the same ID: the INS**.

This INS is composed of:

- **the INS number (which corresponds to the individual's social security number: National Individual Registration number (NIR) or Temporary Individual Registration number (NIA))**
- **the identifier of the structure that assigned the INS in the form of an OID[1] associated with this number,**
- **the five essential components (surname at birth, given name(s) at birth, date of birth, sex, place of birth code).**

This INS is regularly checked, to enable the sharing of medical information in a secure and trustworthy manner. This sharing of medical information is particularly important in the context of complex care pathways or public emergencies such as COVID 19, involving the coordination of many professionals working in the health system.

The use of the INS is meant to enable reliable, unambiguous referencing of patients' health data, prior to any sharing within the circle of trust, avoiding incorrect indexing and the spread of misidentification. Its national scope makes it possible to go beyond regional administrative limits or the borders of the new health territorial divisions, and justifies the use of a single reference database, queried via the INSi teleservice implemented by the national health insurance fund (CNAM).

Locally speaking, universal INS registration contributes to better management of identity security procedures, reducing duplication, facilitating a search for a patient who is already known, and automating the integration of external medical data into the corresponding record.

1.2. Objectives of the document

This document, drawn up with the participation of business and information system referents from health structures and regions (ARS and GRADeS), is intended for software suppliers affected by the listing of health data with the INS. It sets out for them the rules defined in the French National Health ID Reference Document, to which it is annexed, and in the National Identity Security Standard (RNIV).

The objective of this document is therefore to harmonise the implementation of the INS throughout France, by defining common business rules, in compliance with the RNIV.

The business rules may concern:

- all types of software,
- or only identity repository software.

[1] OID: Object Identifier. The NIR and the NIA each have their own assignment body. The OID allows them to be told apart. OIDs are universal identifiers, represented as a sequence of integers. They are organised in a hierarchical form with nodes.

An identity repository is a software that allows the creation or modification of identities. These are often patient administrative management systems (PAM) in healthcare facilities, practice management software (PMS) for self-employed professionals, the laboratory management system (LMS) for laboratories, the radiology information system (RIS) in imaging practices, etc.
The software to which each rule applies is specified.

Please note: Solutions used at an earlier stage in the care pathway for making appointments, pre-consultation, or pre-admission, which directly involve the patient in the management of their own digital identity, are also considered identity repository software.

Please note: The degree of criticality of each business rule has been specified:

- criticality *** : A business rule essential for the proper implementation of the INS, in compliance with the rules of the French National Health ID Reference Document and the RNIV
- criticality **: An important business rule to facilitate the work of future users
- criticality *: A business rule that provides a benefit to future users.

1.3. Scope of the document

This document focuses on the business rules necessary for the proper referencing of health data with the INS in software. **It does not therefore describe the actions to be taken to ensure that the patient being cared for (physically or remotely) corresponds to the digital identity in use (during administrative or medical care). These actions are described in the RNIV.**

1.4. Texts and reference documents

This guide should be read in the light of the following additional documents:

- The provisions of the French Public Health Code relating to the INS articles L. 1111-8-1 and R. 1111-8-1 et seq
- The French National Health ID Reference Document, published on the website of the Agence du numérique en santé (ANS) https://esante.gouv.fr/securite/identifiant-national-de-sante, to which it is annexed
- The INSi teleservice integration guide to retrieve and verify the INS https://www.sesam-vitale.fr/web/sesam-vitale/insi
- The National Identity Security Standard (RNIV) developed by the network of regional identity security authorities (3RIV) under the aegis of the DGOS, DGS and HAS https://solidarites-sante.gouv.fr/soins-et-maladies/qualite-des-soins-et-pratiques/securite/securite-des-soins-securite-des-patients/article/identitovigilance,
- the Health Information Systems Interoperability Framework (CI-SIS) annex: Support for the National Health ID (INS) in the CI-SIS interoperability standards and components, published on the ANS website https://esante.gouv.fr/securite/identifiant-national-de-sante. This CI-SIS annex covers both the CI-SIS standards and the standards maintained by InteropSanté,
- all the documents published on the ANS website (the " understanding the INS kit", the "INS implementation guide", etc.) https://esante.gouv.fr/securite/identifiant-national-de-sante.

1.5. Document outline

This guide covers:

- the components of the INS (Chapter 2),
- the principles of disseminating the INS (Chapter 3),
- the methods for retrieving the INS in identity repository software **(Chapter 4),**
- the methods for verifying the INS in identity repository software **(Chapter 5),**
- the methods for verifying the INS in non-identity-log software **(Chapter 6),**
- the steering indicators (Chapter 7).

2. COMPONENTS OF THE INS

2.1. Identity traits

Rule 1 (criticality *) – valid for all software.**
The RNIV provides for the following 2 requirements [EXI SI 04, EXI SI 05]:
"Identification traits should be the subject of specific fields in the information system."
"The information system must allow for the entry of the additional traits Surname used and Given name used".
The table below lists all the fields that must be included in the software, in accordance with the French National Health ID Reference Document [EXI 15] and the RNIV requirements above.

Rule 2 (criticality *) – valid for all software.
The RNIV includes the following requirement [EXI SI 11]:
"It is important that the nature of each identity feature displayed on documents and human-machine interfaces is easily recognised, without risk of misunderstanding, by all health actors involved."
The wordings (full or abbreviated) recommended for use in the RNIV are specified in the table below.

Rule 3 (criticality *) – valid for all software**
The RNIV includes the following requirement [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."
Therefore, the software must offer the possibility to display in the GUI (graphical user interface) all the fields listed in the table below, but, if for ergonomic reasons, not all these fields can be displayed, the software must allow the users to configure which fields are to be displayed or not displayed (though the fields surname at birth, first given name at birth, date of birth and sex must be displayed, according to the RNIV).

Rule 4 (criticality *) – valid for all software**
In accordance with the French National Health ID Reference Document (requirements [EXI 24], [EXI 25], [EXI 26], [EXI 27], [EXI 28], [EXI 29], [EXI 30] and [EXI 31] relating to access control, traceability, communication security and INSi teleservice self-certification):

- The software must allow the data controller to manage sufficiently fine-grained permissions so that only authorised persons can access the INS and the INSi teleservice,
- Access to the INS and the INSi teleservice must be logged. The traceability procedures to be implemented are the same as those already implemented for access to personal data under the GDPR.

Field name [Short]	Details	Size	Comments (format)	Is it mandatory or optional	technical tag associated with the INSi return
Mandatory identity traits					

INS number [INS]	This field contains the NIR or NIA (concatenated with the key) of the patient receiving care. As a reminder, the INS number must be a separate field from the national insurance number used for the reimbursement of care.	15 characters.		Existence of the mandatory field Optionally populated for the creation of an identity *(but filled in for patients likely to have one, as soon as the call to the teleservice can be made, in use cases where its search is required and authorised – see EXI PP 03 of the RNIV and EXI 16 of the French National Health ID Reference Document)*	*NumIdentifiant* (EF_INS23_01) *Cle* (EF_INS23_02)
OID [OID]	Identifier of the structure that assigned the NIR or NIA, in the form of an OID (Object IDentifier).	20 characters.	List of OIDs available on the ANS website here.	Existence of the mandatory field Optionally populated for the creation of an identity	*OID* (EF_INS22_01)
Surname at birth [N.Nais.]	Also called family name.	100 characters.	Baseline: Capital letters, no accents, no diacritical marks, with the ability to use hyphens and apostrophes.	Existence of the mandatory field Must be populated for the creation of an identity	*NomNaissance* (EF_INS25_01)
Given name(s)[Pr. Nais.]	All given names at birth.	100 characters.	Baseline: Capital letters, no accents, no diacritical marks, with the ability to use hyphens and apostrophes. **Please note:** If the given name(s) at birth are stored in uppercase in the database, it is possible to display them in lowercase if this makes them easier to read for users. **Please note:** The list of given names at birth does not exceed 54 characters at present. The field size of 100 characters has been set as a safe margin, consistent with the size of the surname at birth field.	Existence of the mandatory field Optionally populated for the creation of an identity *(but filled in as soon as it is possible to access this information: Presentation of an identity document and/or call to the INSi teleservice - see EXI PP 03 of the RNIV).*	*ListePrenom* (EF_INS25_03) Warning, do not use the *Prenom* tag (EF_INS25_02)
First given name [Pr.1]	First given name at birth	100 characters.	**Please note:** The field size of 100 characters has been set as a safe margin, consistent with the size of the surname at birth field. **Please note:** If the first given name at birth is stored in uppercase in the database, it is possible to display it in lowercase if this makes it easier to read for users.	Existence of the mandatory field Must be populated for the creation of an identity	Not applicable: Data not returned by INSi
Date of birth[DDN]		YYYY-MM-DD	The date of birth is returned in the format YYYY-MM-DD by INSi but should be reversed in the user display for ease of reading. **Please note**: INSi can return dates of birth containing a day and possibly a month set to 00 when the day and/or month are not known.	Existence of the mandatory field Must be populated for the creation of an identity	*DateNaissance* (EF_INS25_05)
Sex [S]		1 character.	3 possible values: F (Female), M (Male), I (Indeterminate), where INSi will only return F or M values.	Existence of the mandatory field Must be populated for the creation of an identity	*Sexe* (EF_INS25_04)
Place of birth code - INSEE Code [INSEE Nais.]	This is the commune of birth for people born in France and the country of birth for people born abroad.	5 characters (for the INSEE code).	Use of the INSEE code (different from the postal code), with the name of the	Existence of the mandatory field Must be populated for the creation of an identity	*LieuNaissance* (EF_INS25_06)

			corresponding municipality or country[2].		
Additional identity-related traits (non-exhaustive list)					
Surname used [N.Ut]	Surname used in everyday life. The name used can be similar to the surname at birth.	100 characters.	Baseline: Capital letters, no accents, no diacritical marks, with the ability to use hyphens and apostrophes.	Existence of the mandatory field Optionally populated for the creation of an identity *(but filled in when different from the surname at birth [Exi PP 17] of the RNIV)*	Not applicable: Data not returned by INSi
Given name used[Pr.Ut.]	Given name used in everyday life. The given name used may be one of the given names at birth or any other name chosen by the patient.	100 characters.	Baseline: Capital letters, no accents, no diacritical marks, with the ability to use hyphens and apostrophes. **Please note:** If the given name used is stored in uppercase in the database, it is possible to display it in lowercase if this makes it easier to read for users.	Existence of the mandatory field Optionally populated for the creation of an identity *(but filled in when it is different from the first given name at birth. [Exi PP 18])*	Not applicable: Data not returned by INSi Warning, do not use the *Prenom* tag (EF_INS25_02)

Rule 5 (criticality *) – valid for identity repository software.**

The software must not allow the creation of an identity if the fields that must be filled in are not completed. As indicated in the table above, the following fields must be filled in to create an identity: Surname at birth, first given name at birth, date of birth, sex and place of birth code (INSEE code).

Please note: Fields that are optional do not have to be made mandatory in order to create an identity.

Rule 6 (criticality *) – valid for identity repository software.**

The RNIV provides for the following requirement [EXI SI 12], consistent with the French National Health ID Reference Document [EXI 17]:

"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". Therefore, the fields surname at birth, given name(s) at birth, date of birth, sex and place of birth code (INSEE code) must be populated with the data returned by INSi as soon as the identity has the status "qualified identity" or "retrieved identity" (using the methods described in chapter 4).

For identities with the status "provisional identity" or "validated identity", all these fields are populated with data collected locally.

Please note: Even if the first given name at birth field is not directly populated by the INSi return, it must be consistent with the beginning of the list of given names at birth returned by INSi.

Rule 7 (criticality *) – valid for identity repository software.

The software can offer several ways of filling in the first given name at birth field to make it easier for users. For example:

- The first given name can be extracted from the list of given names at birth,
- The first given name can be manually input, but with a consistency check against the beginning of the list of given names at birth.

Rule 8 (criticality *) – valid for identity repository software.

[2] The active list of commune and country codes, as well as the history of changes to communes, are available at https://www.data.gouv.fr/fr/datasets/code-officiel-geographique-cog/# .

The software can offer several ways of filling in the given name used field to make it easier for users. For example, the first given name at birth can be voluntarily copied by the user if it is identical to the given name used.

Rule 9 (criticality *) – valid for identity repository software.
The RNIV includes the following requirement [EXI SI 15]:
"Information systems may allow dates of birth in a lunar-solar calendar to be translated into DD/MM/YYYY format for patients born abroad".

Rule 10 (criticality *) – valid for identity repository software
For unusual dates of birth[3], the RNIV states:
"Where the date of birth provided by the identity document or digital identification device 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) 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.

If the information system allows it, a specific marker like "Dummy date", "Provisional date", "Uncertain date" etc. should 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."

Rule 11 (criticality *) – valid for identity repository software.**
Software should not retrieve an INS if it contains a date of birth with "00" as the day and/or month of birth.

Rule 12 (criticality *) – valid for identity repository software.**
Software should not retrieve an INS if it contains an empty surname at birth and/or given name(s) at birth and/or sex field.

Rule 13 (criticality *) – valid for identity repository software.
The software may offer a field "Place of birth – postal code" in addition to the field "Place of birth code (INSEE code)". The presence of this field is optional.

Rule 14 (criticality *) – valid for identity repository software.
The software may offer a field "Country of birth" in addition to the field "Place of birth code (INSEE code)", so that the country of birth (France or a foreign country) can be made more explicitly visible to users. The presence of this field is optional.
Similarly, software may offer a "City of birth" field for patients born abroad, in addition. The presence of this field is optional.

Rule 15 (criticality **) – valid for identity repository software
When the field "Place of birth code (INSEE code)" is filled in not from INSi but from user input, the software should:

- both allow the user to enter the name of the commune/country of birth,

[3] Unusual dates of birth are dates of birth with a day not between 1 and 31 and/or a month not between 1 and 12. In the social security context, these birth dates are referred to as lunar dates of birth.

- and offer the appropriate INSEE code, taking into account the INSEE code assigned to the commune or country of birth in force at the time of patient's date of birth (for example, the software should offer the INSEE code 75073 if the patient was born in Suresnes before 01/01/1968, and 92073 if the patient was born after).

Rule 16 (criticality *) – valid for identity repository software.**
The RNIV includes the following requirement [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 should also be recorded.”

Rule 17 (criticality *) – valid for all software**

The RNIV provides for the following requirements [EXI SI 01, EXI SI 02 and EXI SI 03] when searching for an existing identity:

"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."

"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."

"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."

Rule 18 (criticality **) – valid for all software performing identity mergers

The RNIV includes the following requirement [RECO SI 02]:

"It is recommended that the information system should have dedicated functionalities to search for anomalies in the recording of identity traits." Therefore, software should display warning messages in particular in the following cases:

- An attempt to merge two identities with separate INS numbers
- An attempt to merge a provisional identity with a validated identity if the identity selected as the master is the provisional identity
- An attempt to merge two identities if the identity selected as the master does not have the status "retrieved identity" or "qualified identity" and has the status "provisional identity" or "validated identity"
- There are two identities with the same INS number (a work list is populated in addition to the alert message).

2.2. Identity status and attributes

2.2.1. Identity status and attributes in identity repository software

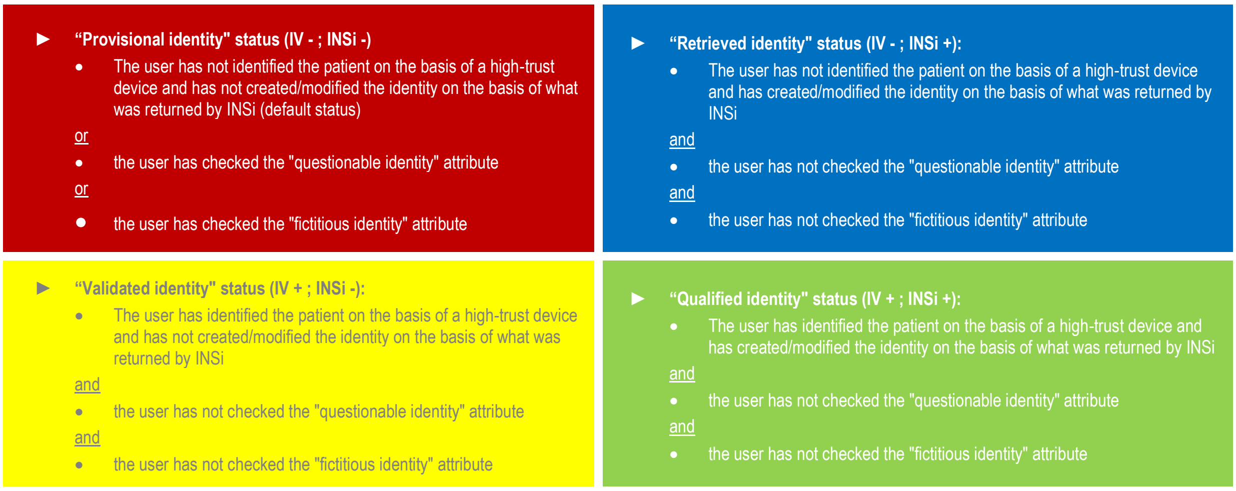
The RNIV requires that identity repository software manage the following 4 functional statuses:

- "provisional identity"
- "retrieved identity"
- "validated identity"
- "qualified identity".

These functional statuses are mutually exclusive. The French National Health ID Reference Document [EXI 18] further specifies that the INS number and OID must be accompanied by information confirming that they have been qualified.

The RNIV recommends that identity repository software manage at least the following three attributes:

- similar identity
- questionable identity
- fictitious identity



► **"Provisional identity" status (IV - ; INSi -)**
- The user has not identified the patient on the basis of a high-trust device and has not created/modified the identity on the basis of what was returned by INSi (default status)

or
- the user has checked the "questionable identity" attribute

or
- the user has checked the "fictitious identity" attribute

► **"Retrieved identity" status (IV - ; INSi +):**
- The user has not identified the patient on the basis of a high-trust device and has created/modified the identity on the basis of what was returned by INSi

and
- the user has not checked the "questionable identity" attribute

and
- the user has not checked the "fictitious identity" attribute

► **"Validated identity" status (IV + ; INSi -):**
- The user has identified the patient on the basis of a high-trust device and has not created/modified the identity on the basis of what was returned by INSi

and
- the user has not checked the "questionable identity" attribute

and
- the user has not checked the "fictitious identity" attribute

► **"Qualified identity" status (IV + ; INSi +):**
- The user has identified the patient on the basis of a high-trust device and has created/modified the identity on the basis of what was returned by INSi

and
- the user has not checked the "questionable identity" attribute

and
- the user has not checked the "fictitious identity" attribute

Rule 19 (criticality **) – valid for identity repository software

The RNIV includes the following requirement [EXI SI 10]:

"The type of identity device used to collect the identity should be recorded. Only a high-trust document, or its digital equivalent, shall allow the status of Validated Identity or Qualified Identity."

Consequently, identity repository software must include a field allowing the user to indicate the nature of the credential (supporting document or electronic identification device) that was used to create/verify the patient's identity. The user must be able to set up in the software the list of the different possible credentials and the degree of trust associated with each credential (the management of this list must remain in the hands of the users as it can be modified). The list of high-trust credentials is specified in the RNIV.

Please note: Validating an identity ("validated identity" status) must at least be possible through voluntary action by the user (e.g. a checkbox). However, identity repository software can offer the chance to automatically assign the status "validated identity" when a highly trusted credential is submitted by the user. If the software offers this feature, it must be possible to deactivate it by configuring the settings.

After consulting with the National Commission for Information Technology and Civil Liberties (CNIL), it is permitted to keep a copy of the patient's identity document for a maximum of 5 years from the last time the patient visited the facility, subject to:
- the encryption of the digitised identity documents
- limiting access to this copy to specifically authorised professionals.

Rule 20 (criticality **) – valid for identity repository software

The RNIV includes the following requirement [EXI SI 07]:

"Any health information system must be able to assign one of four trust statuses to each stored digital identity." The RNIV describes functional statuses: The identity repository software can choose to implement :
- a set of values corresponding to the functional status of the identity (with the 4 possible values: provisional, retrieved, validated, or qualified identity),
- or 2 sets of values (one set of values related to whether or not the identity is validated, and one set of values related to whether or not the INSi return was used to create/modify the identity), the combination of which makes it possible to reach the four functional statuses described above.

Rule 21 (criticality **) – valid for identity repository software

Any change in status must be logged (previous status, date of status update and person responsible for the update).

Rule 22 (criticality **) – valid for identity repository software
The RNIV includes the following requirement [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."

Rule 23 (criticality *) – valid for identity repository software
Software may allow a time limit to be set after which any identity with a "qualified identity" status remains qualified but is subject to an alert message / flag inviting the user to redo an identity security procedure and a new call to INSi. These identities are also included in a dedicated work list.

Rule 24 (criticality **) – valid for identity repository software
Software should display the status of the identity to the user, highlighting their category (e.g. a red dot for an identity with the status "provisional identity", blue for an identity with the status "retrieved identity", yellow for an identity with the status "validated identity", and green for an identity with the status "qualified identity"). This display should allow the user to see what remains to be done to move, if applicable, towards a "qualified identity" status.

2.2.2. Status in software that does not log identities

identity repository software must manage the four functional statuses mentioned above. However, in order to minimise the impact on interoperability, only the technical statuses "provisional identity" or "validated identity" are transmitted in IHE PAM flows.

The statutes "retrieved identity" and "qualified identity" are therefore not transmitted.

- The status "qualified identity" is deduced, by non-identity repository software, by filling in the field relating to the INS number or its OID, associated with an identity with the status "validated identity".
- The status "retrieved identity" cannot be deduced and therefore managed.

2.2.3. The business rules associated with the status of the identity

The following business rules are associated with the identity status:

Rule 25 (criticality **) – valid for identity repository software
The RNIV includes the following requirement [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 call to the INSi teleservice."

Therefore,

- if the attribute "questionable identity" or "fictitious identity" is selected by the user for identity with the status "retrieved identity", "validated identity", or "qualified identity" the immediate consequence is that the status of the identity is downgraded to "provisional identity",
- the call to INSi must be expressly blocked for digital identities with a questionable identity or fictitious identity attribute.

Rule 26 (criticality **) – valid for identity repository software

In line with requirement [EXI 13] of the French National Health ID Reference Document, the INS number, its OID and the 5 mandatory reference traits must not be modifiable when the identity has the status "retrieved identity" or "qualified identity", unless specific permission is granted to a "super user" (for example, when an identity error is detected). The non-editable nature of these fields should be made clear to the user (e.g. lock or greyed-out area). On the other hand, additional traits (surname used, given name used, contact details etc.) must be modifiable even if the identity has the status "retrieved identity" or "qualified identity".

Rule 27 (criticality **) – valid for identity repository software

Downgrading of status. Any downgrading of an identity to the status of "retrieved identity" or "qualified identity" to an identity with the status of "provisional identity" or "validated identity" must entail:

- Automatically deleting (invalidate) the fields relating to the INS number and its OID,
- Propagating the changes to be made, in accordance with requirement [EXI 22] of the French National Health ID Reference Document.

Modifying mandatory traits. Any change to the mandatory reference traits of an identity with the status of "retrieved identity" or "qualified identity" must entail:

- Automatically deleting (invalidate) the fields relating to the INS number and its OID,
- Downgrading the status of the identity to a lower level (an identity with the status of "retrieved identity" is downgraded to "provisional identity" status; an identity with the status of "qualified identity" is downgraded to "validated identity" status),
- Propagating the changes to be made, in accordance with requirement [EXI 22] of the French National Health ID Reference Document.

On the other hand, modifying one or more additional traits (surname used, given name used, contact details etc.) should not entail the above actions.

Rule 28 (criticality *) – valid for all software.**

This is one of the fundamental rules of this guide.

The RNIV includes the following requirement [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".

This requirement is also present in the French National Health ID Reference Document [EXI 12].

Therefore, the software should only transmit the INS number and its OID if the identity has the status "qualified identity". If the identity does not have "qualified identity" status, the INS number and its OID are not transmitted (even if they have been retrieved); only the traits are transmitted.

Rule 29 (criticality *) – valid for all software**

The status "qualified identity" is transitive within the same identification domain. The receiver does not need to requalify an INS transmitted by other software belonging to the same identification domain (no new identity security procedure to validate the patient's identity and no new call to INSi).

Exception: If the INS has to be manually re-entered in the receiver's software (no computerised flow between the sender's and receiver's software, despite their belonging to the same identification domain), the receiver must make a new INSi call (to avoid potential re-entry errors).

Rule 30 (criticality *) – valid for all software**

The status "qualified identity" is not transitive between two different identification domains. The receiver must therefore requalify an INS transmitted by software belonging to a different identification domain (another identity security procedure to validate the patient's identity and another call to INSi).

Exception #1 (see Annex V of RNIV 1 - Performing acts on behalf of a third party, with no direct link to the patient) if the receiver performs a procedure on behalf of a third party, with no direct link to the patient (e.g. subcontracted examinations, professional expertise such as multidisciplinary consultation meetings (RCPs), etc.), then the receiver is not obliged to requalify the INS, provided that the following two conditions are met:

- the receiver has full confidence in the quality of the identity transmitted (the contract between the parties explicitly provides this guarantee),
- the INS is transmitted as a computerised flow (no manual re-entry of the identity into the receiver's software).

In this case, the receiver can assign the status "qualified identity" to this identity; it will be able to broadcast this identity (including the INS number and the OID) to any actor.
Concerning the transmission of a paper prescription, the RNIV states:
"In a case where the identity is not received in digital format, the call to the verification 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)."

Exception #2 (see Annex V of the RNIV 1 - Remote patient registration): The status "qualified identity" can be transitive between different identification domains under the responsibility of the same data controller.

3. DISTRIBUTING AN IDENTITY – ALL SOFTWARE

As a reminder, requirement [EXI 14] of the French National Health ID Reference Document states that the INS, once qualified, should be used to reference health data, in the context of exchanging and sharing health data.

Reminder of Rule **28 (criticality ***) - valid for all software**
identity repository software may only transmit the INS number and its OID if the identity has the status "qualified identity".
If the identity does not have "qualified identity" status, the INS number and its OID are not transmitted (even if they have been retrieved); only the traits are transmitted.

Rule 31 (criticality *) – valid for all software**
In accordance with requirement [EXI 21] of the French National Health ID Reference Document, the software must be able to log partners with whom health data containing the INS have been exchanged or shared.

3.1. Distributing an identity via paper flows

Rule 32 (criticality *) – valid for all software**
The RNIV provides [EXI PP 10] that at a minimum, the following information 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. The OID is not intended to be displayed in plain text on a paper document. However, the nature of the INS number (NIR or NIA) must be indicated.

This information should be displayed in plain text on the health data. A text block template will be put online by the NSA on its website, as an example.

This information must also be shown in the form of a datamatrix. The specifications to be followed for printing the INS datamatrix will also be published by the ANS on its website.
Please note: This printing is optional if another signed 2D-DOC barcode containing the mandatory data of the national health ID is also present on the physical medium.

However, the software must allow the user to display any other field that the user finds useful.

3.2. Distributing an identity via computerised flows

Rule 33 (criticality *) – valid for all software**
All the fields listed in Chapter 2 must appear in the output data stream of all software. For this purpose, refer to the interoperability standards described in Annex INS of the Health Information Systems Interoperability Framework (CI-SIS) (which also lists the standards maintained by InteropSanté).
Please note: Distributing the INS history is not mandatory.

3.3. Distributing an identity to populate the DMP

A qualified INS will be required to populate the DMP (Shared Medical Record). Otherwise, the DMP cannot be populated.

For more information, please refer to the DMP integration guide published by GIE SESAM-Vitale.

4. RETRIEVING THE INS IN IDENTITY REPOSITORY SOFTWARE

The INSi retrieval operation collects the INS (INS number, its OID and the 5 mandatory INS traits) as it appears in the national reference databases.

The INSi retrieval operation can be called either via the patient's Carte Vitale card or via their identity traits.

In return, the retrieval operation returns three possible responses:
- "00": A unique identity has been found,
- "01": No identity was found,
- "02": Several identities have been found.

This chapter describes the use cases and the implementation steps of the INSi retrieval operation.

4.1. Use cases of the INSi retrieval operation (non-exhaustive list)

The retrieval operation is called:
- when creating an identity in the software for a new patient,
- or when updating the identity of a known patient (for whom the INS number, OID and mandatory reference traits have not yet been retrieved).

The call for the retrieval operation can occur in different contexts:
- prior to the patient's visit, during the treatments carried out to prepare for scheduled visits (online pre-admission, online appointment booking),
- when the patient visits a reception desk (administrative or decentralised reception desk in the departments) of a structure (e.g. healthcare facility),
- during the patient's care (e.g. at the doctor's office),
- from information transmitted by a third party, in paper format or via interfaces (performing a telemedicine procedure at the request of a requesting professional, performing a subcontracted examination, etc.),
- with a view to populating its identity repository(s) with INS identities, in particular in order to more rapidly acquire a common identity between several actors in the same territory (regional health coordination network called a GHT, for example),
- etc.

Please note: This call is not necessary if the INS has already been obtained via INSi (i.e. if the identity already has the status "retrieved identity" or "qualified identity").

4.2. Implementation steps of the INSi retrieval operation.

The INSi retrieval operation is carried out in four steps:

- call to the INSi retrieval operation
- traceability of the INSi return
- displaying the INSi return and comparing it to any pre-existing traits
- using the INSi return to populate the fields corresponding to the mandatory identity traits

4.2.1. Call to the INSi retrieval operation

As a reminder, there are two possible ways to call the INSi retrieval operation: Searching by Carte Vitale or searching by traits.

Rule 34 (criticality **) – valid for identity repository software
According to the RNIV [EXI PP 06], "Querying the INSi teleservice via the Carte Vitale is the preferred method of querying whenever possible.” Searching based on the Carte Vitale card should be preferred from the moment it is inserted in the reader. Otherwise, searching based on the traits available in the software is used.

Rule 35 (criticality *) – valid for identity repository software
For a feature-based search, the minimum fields to be filled in to call INSi can be clearly identified (e.g. star, colour, bold).

Rule 36 (criticality **) – valid for identity repository software
The call for the retrieval operation (feature-based search) should be launched:

- after a user action (click), or automatically, without user action,
- for a file or for a set of files from a work list prepared by the software (sequential searches, in particular to adapt to the use case of pre-admission, for example, or the populating of the database).

For an automatic call to INSi, the software should ensure that a call to INSi is only made if it is legitimate (no recent failure, INS not yet retrieved, fields needed to call INSi not empty, etc.)

4.2.2. Traceability of the INSi return

As a reminder, the INSi retrieval operation can return three responses:

- "00": A unique identity has been found,
- "01": No identity was found,
- "02": Several identities have been found.

Rule 37 (criticality **) – valid for identity repository software
Any call to INSi must be logged (regardless of whether the response is "00", "01” or "02").

Rule 38 (criticality *) – valid for identity repository software
The log of the call to INSi can also include the call method used (search by Carte Vitale or by traits).

Rule 39 (criticality **) – valid for identity repository software
The RNIV includes the following requirement [EXI SI 06]:
"The information retrieved from the INSi teleservice is stored and tracked in the health information system.”

Furthermore, the French National Health ID Reference Document [EXI 20] specifies that the history of a person's INS numbers must be preserved. This requirement of the French National Health ID Reference Document only applies to identity repository software.
Therefore, in case of a "00” response, the information returned by INSi (INS number, OID, INS history and mandatory reference traits returned by INSi) must be preserved unchanged in the software.

4.2.3. Displaying the INSi return and comparing it to any pre-existing traits

Rule 40 (criticality **) – valid for identity repository software
In the case of a "01" response: No identity has been found, and the user should be informed by an appropriate message (e.g. if the different call methods have not been exhausted: "No identity found, change your search").

Rule 41 (criticality **) – valid for identity repository software
In the case of a "02"response: Multiple identities found, the user should be informed (and asked, if justified, to add e.g. the place of birth code or the list of given names in order to attempt a new call).

Rule 42 (criticality **) – valid for identity repository software
In the case of a "00" response: A unique identity has been found, and the software should offer to show the user, for example in a pop-up or insert, the mandatory reference traits returned by INSi. The software also informs the user of any discrepancies between the mandatory traits returned by INSi and any pre-existing traits in the software (e.g. by colour-coding, highlighting, etc.).
It is recommended to display this window no matter what (but whether or not it is displayed can be made configurable).

Rule 43 (criticality *) – valid for identity repository software
In the case of a "00" response: A unique identity has been found, the software can calculate a similarity rate between the mandatory traits returned by INSi and any pre-existing traits in the software.
This calculation means that for each identity feature, the weight given to it and the accepted deviation rate (similarity threshold) can be configured.
The calculation of this rate must involve:

- **For alphabetical characters**: Recognised methods such as Jaro-Winkler distance or Levenshtein distance.
  Please note: The presence or absence of a hyphen or apostrophe should not be considered a difference.
- **For dates of birth**: Recognised methods such as Hamming distance.
- **For places of birth**: Comparing the postcode, if any, in the field "place of birth” and the INSEE code returned by INSi (from a transcoding table).
  Note: *It is also possible for the place of birth to calculate a similarity rate for the name of the town rather than on the basis of the INSEE code-postcode comparison.*

Spotlight on the response "00": A unique identity has been found.

Clarification: What can be the differences between the local traits (patient already known) and the mandatory reference traits returned by INSi?

Name of the field	**Historical data entry rules promoted by the 2013 DGOS instruction**	**Information returned by INSi**
Surname at birth	In capital letters, with no accents, no diacritical marks, **no** ability to use hyphens and apostrophes (replaced by a space), in line with the 2013 DGOS instruction.	In capital letters, with no accents or diacritical marks, but **with** the ability to use hyphens and apostrophes.
Given name at birth	In capital letters, with no accents, no diacritical marks, **no** ability to use hyphens and apostrophes (replaced by a space), in line with the 2013 DGOS instruction. Entry of **First given name at birth** only.	In capital letters, with no accents or diacritical marks, but **with** the ability to use hyphens and apostrophes. **List of given names, separated by spaces**. Some people have compound names without hyphens, so it may not be possible to detect the given name because of the space separator.
Date of birth	**Unusual values not accepted.**	**Could have some unusual values**[4]
Sexe	**Value "I" allowed.**	**Value "I" not transmitted.**
Place of birth	**Postcode**	**INSEE code**, different from the postcode Need to accept obsolete INSEE codes (from when communes were merged, etc.).

4.2.4. The populating of identity fields (only if response is "00": A unique identity has been found from INSi).

Reminder of Rule 6 (criticality *) – valid for identity repository software**
The RNIV provides for the following requirement [EXI SI 12], consistent with INS [EXI 17]:
"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". Therefore, the fields surname at birth, given name(s) at birth, date of birth, sex and place of birth code (INSEE code) must be populated with the data

[4] Unusual dates of birth are dates of birth with a day not between 1 and 31 and/or a month not between 1 and 12. In the social security context, these birth dates are referred to as lunar dates of birth.

returned by INSi as soon as the identity has the status "qualified identity" or "retrieved identity" (using the methods described in chapter 4).

For identities with the status "provisional identity" or "validated identity", all these fields are populated with data collected locally.

Please note: Even if the first given name at birth field is not directly populated by the INSi return, it must be consistent with the beginning of the list of given names returned by INSi.

Rule 44 (criticality **) – valid for identity repository software

In case of response " 00 – a unique identity was found" from INSi, the software should populate the following fields with the information returned by INSi: INS number, OID, surname at birth, first given name(s) at birth, date of birth, place of birth (INSEE code) and sex. All these fields can be populated:

- upon express validation by the user,
- or automatically, if the software has calculated a similarity rate which is higher than the similarity threshold defined by the user (see Rule 43).

The status of the identity must also be updated in accordance with Rule 19.

Changes to fields and statuses must be logged, in accordance with Rules 14 and 20.

Rule 45 (criticality **) – valid for identity repository software

If INSi returns a "00 – A unique identity was found" response, when the INS number, OID, surname at birth, given name(s) at birth, date of birth and sex fields have not been filled in with the information returned by INSi (abandoned by the user), the software should automatically generate a work list, particularly for the identity security unit.

5. VERIFYING THE INS IN IDENTITY REPOSITORY SOFTWARE

This chapter describes the use cases and the implementation steps of the INSi verification operation in identity repository software.

The INSi verification operation ensures that an INS present in the software or transmitted by a third party is identical to the one existing in the civil status databases.

In return, the verification operation returns two possible responses:

- OK,
- KO.

5.1. Use cases of the INSi verification operation (non-exhaustive list)

Use cases of this verification operation (non-exhaustive list) for identity repository software:

- **Verification of identities with the status "retrieved identity" and "qualified identity" existing in the identity repository:**
    - **Bulk verification:** The identities in the patient database must be reviewed within 5 years from their date of acquisition (in accordance with the French National Health ID Reference Document [EXI 19]. The verification operation is queried to identify the identities to be analysed and possibly rectified.
    - **Individual verification of the patient's NSI prior to or during their care** (e.g. when managing pre-admissions).

      Please note: In view of the low probability of a change in the INS number and/or one of the mandatory reference traits over time, it is not recommended to automate the INSi verification operation each time the patient enters care (in the interests of digital sobriety).

      Examples of situations in which a call to the verification operation may be useful before/during the patient's care:
        - an INS number of the NIA type, its OID, and the associated mandatory reference traits were retrieved during a previous visit by the patient (or at the beginning of a long stay). The verification operation is queried before/during the patient's next visit or during their stay to identify if they have not been registered in the meantime (change from NIA INS to NIR INS and associated OID change),
        - a patient is undergoing a sex reassignment protocol. The verification operation is queried before/during the patient's next visit to identify whether the sex change has been reflected in the civil status,
        - periodic verification of the INS after a user-definable period of time.

- **Individual verification of the INS transmitted by an actor belonging to a different identification domain.** As a reminder, requirement [EXI 11] of the French National Health ID Reference Document provides for the need to qualify an INS that has not been previously qualified by the recipient (unless expressly contracted for by the sender).

  Please note: This verification is only useful if the receiver does not already have the patient's INS with the status "qualified identity".

Examples of situations in which a call to the verification operation may be useful following the receipt of an identity transmitted by an actor belonging to a different identification domain:

- an identity is transmitted as part of a telemedicine procedure,
- a patient appears with their INS number (for example on a prescription, possibly in the form of a barcode/datamatrix). The user enters/scans the INS number and enters the mandatory reference traits, which triggers a call to the verification operation (note: This may imply that the software has pre-filled the OID).

5.2. Implementation steps of the INSi verification operation.

5.2.1. Call to the INSi verification operation.

As a reminder, the INSi verification operation requires the following input data:

- INS number
- OID
- surname at birth
- at least one of the given names at birth
- sex
- date of birth
- place of birth (in INSEE code) (optional).

Rule 46 (criticality **) – valid for identity repository software
Software should allow the user to schedule bulk verification operation calls, allowing the user to set their frequency (e.g. verification every x months) and scope (e.g. to spread processing over x days, taking identities in the database by alphabetical order of surname at birth, or taking identities in the database by the date the identity was created).

Rule 47 (criticality **) – valid for identity repository software
The call to the verification operation should be initiated automatically by the software as long as an identity with the status "retrieved identity” or “qualified identity” has an INS number of the NIA type. How frequently the verification operation is called in this context should be configurable.

5.2.2. The traceability of the return from the INSi verification operation call.

Rule 48 (criticality *) – valid for all software**
The RNIV includes the following requirement [EXI SI 06]:
"The information retrieved from the INSi teleservice is stored and tracked in the health information system.”
Therefore, any call to INSi, as well as the return ("OK” or "KO") must be logged.

5.2.3. Managing the INSi return

Rule 49 (criticality **) – valid for identity repository software

When an INS contained in the identity repository is verified through the INSi verification operation and receives a "KO" response:

- the status of the identity must be downgraded (an identity with the status of "retrieved identity" must be downgraded to “provisional identity"; an identity with the status "qualified identity” must be downgraded to "validated identity" status - if the identity can be rechecked for consistency against a scanned high-trust document - or to "provisional identity” otherwise)
- the INS number and its OID must be deleted (invalidated).

Rule 50 (criticality *) – valid for identity repository software

When an INS is transmitted by an actor belonging to a different identification domain and the call to the INSi verification operation results in an "OK" response, all the transmitted identity traits can be integrated into the receiving software (including the INS number and its OID).

The receiver will then have to identify whether this transmitted identity does or doesn’t correspond to a patient already known in its identity repository.

- If the receiver detects that the patient is not known in the identity repository, it will be able to create an identity in its identity repository by reusing all the traits communicated by the sender (including the INS number and its OID). The status of the identity is necessarily “retrieved identity” (it will change to the status of “qualified identity” once an identity security procedure has been carried out).
- If the receiver detects that the patient is known in the identity repository, it will be able to update an identity in its identity repository by reusing all the traits communicated by the sender (including the INS number and its OID). The status of identity becomes "retrieved identity” if the identity initially had the status of “provisional identity" in the receiver software and becomes "qualified identity" if it initially had the status "validated identity".

Rule 51 (criticality **) – valid for identity repository software

When an INS is transmitted by an actor belonging to a different identification domain and the call to the INSi verification operation results in a "KO” response, the transmitted identity traits are still integrated in the receiving software (so as not to impede care), except for the INS number and its OID.

The receiver will then have to identify whether this transmitted identity does or doesn’t correspond to a patient already known in the identity repository.

- If the receiver detects that the patient is not known in the identity repository, it will be able to create an identity in its identity repository by reusing the traits communicated by the sender, except for the INS number and its OID. The status of the identity is necessarily “provisional identity”.
- If the receiver detects that it is a known patient in the identity repository, the identity traits communicated by the sender are not integrated in the receiver software. The status of the identity remains as the receiver originally had it ("provisional identity" or "validated identity").

6. VERIFYING THE INS IN THE SOFTWARE

This chapter describes the use cases and the implementation steps of the INSi verification operation in any software that integrates health data referenced with the INS (including EAI).

The INSi verification operation ensures that an INS transmitted by a third party is identical to the one existing in the civil status databases.

Please note: Applications that store health data transmitted by health care providers by juxtaposing them, without the logic of integrating them into a patient file, and without the ability to modify these data (examples: PACS-type image warehouses) are not affected. This type of application is not intended to call for the verification operation prior to the integration of health data referenced by the INS.

In return, the verification operation returns two possible responses:

- OK,
- KO.

6.1. Use cases of the INSi verification operation (non-exhaustive list)

Use case of an operation: Individual verification of the INS transmitted by an actor belonging to a different identification domain, in the context of exchanging or sharing health data referenced with this INS

As a reminder, requirement [EXI 11] of the French National Health ID Reference Document provides for verifying the consistency of the INS with the identity traits upon receipt of health data (unless they have already been retrieved or verified by the INS teleservice at the health data receiver).

Please note: This verification is only useful if the receiver does not already have the patient's INS with the status “qualified identity”.

6.2. Implementation steps of the INSi verification operation.

6.2.1. Call to the INSi verification operation.

As a reminder, the INSi verification operation requires the following input data:

- INS number
- OID
- surname at birth
- at least one of the given names at birth
- sex
- date of birth
- place of birth (in INSEE code) (optional).

Rule 52 (criticality *) – valid for all software**
The call to the verification operation must be launched automatically by the software as soon as an INS is transmitted by an actor belonging to a different identification domain, unless this INS already exists at the receiver with the status "qualified identity” or "retrieved identity”.

As a reminder, in some exceptional cases the call to the verification operation is not mandatory (see exceptions mentioned in Rule 30 of the INS Implementation Guide). This principle also applies to Rules 53, 54 and 55 of that Guide.

6.2.2. The traceability of the return from the INSi verification operation call.

Rule 53 (criticality *) – valid for all software**

The RNIV includes the following requirement [EXI SI 06]:
"The information retrieved from the INSi teleservice is stored and tracked in the health information system."
Therefore, any call to INSi, as well as the return ("OK" or "KO") must be logged.

6.2.3. Managing the INSi return

Rule 54 (criticality *) – valid for all software
When health data referenced with the INS is transmitted by an actor belonging to a different identification domain and the call to the INSi verification operation results in an "OK" response, the health data can be integrated automatically.

Rule 55 (criticality *) – valid for all software**
When health data referenced with the INS is transmitted by an actor belonging to a different identification domain and the call to the INSi verification operation results in a "KO" response, the health data must not be integrated automatically. This should be flagged and placed on a work list for analysis.

7. MONITORING

Rule 56 (criticality **) – valid for identity repository software
At a minimum, the following monitoring indicators must be implemented in the identity repository software in order to monitor the deployment of the INS:

- Share of identities with the status "provisional identity”
- Share of identities with the status "retrieved identity”
- Share of identities with the status "validated identity”
- Share of identities with the status "qualified identity”

The detailed method for calculating these indicators will be specified elsewhere.

Rule 57 (criticality *) – valid for identity repository software
The following monitoring indicators can be implemented in identity repository software in order to monitor calls to INSi:

- total number of calls to INSi per period, distinguishing between calls to the retrieval operation (one category for Carte Vitale, and another for traits) and calls to the verification operation (one category for individual, and another for bulk) and indicating the % of calls for which the response was "00", "01” or “02” for the retrieval operation and the % of calls with a return of "OK” or "KO” for the verification operation).
- average number of successive calls per identity.

These indicators must be available in the form of exports and will serve as a basis the controls carried out by the identity security unit.

Please note: To monitor the deployment of the INS, an indicator will also be calculated by the MSSanté operators to quantify the % of messages containing health documents referenced with the INS.

MINISTÈRE
DES SOLIDARITÉS
ET DE LA SANTÉ

Liberté
Égalité
Fraternité