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

Direction générale
de l'offre de soins

NATIONAL IDENTITY SECURITY FRAMEWORK

HIGHLIGHTS: WHAT EVERY HEALTHCARE PROVIDER SHOULD KNOW

3RIV
RÉSEAU DES
RÉFÉRENTS RÉGIONAUX
D'IDENTITOVIGILANCE

RNIV 00 Highlights • version 1.3 | June 2022

CONTENTS

CONTRIBUTORS

Ms Céline Descamps, CRIV NA

Mr Thierry Dubreu (SESAN)

Mr Marc Fumey (HAS)

Dr Gilles Hebbrecht, DGOS

Ms Bérénice Le Coustumer, DGOS

Mr Mikaël Le Moal, DGOS

Ms Christelle Nozière, CRIV NA

Dr Manuela Oliver, GRIVES

Mr Bertrand Pineau (SESAN)

Dr Sylvie Renard-Dubois, DGOS

Mr Michel Raux, DGOS

Dr Bernard Tabuteau, CRIV NA

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	2020-12-18	1st release of the document
1.1	2021-05-20	Update following CNIL opinion
1.2	2022-06-03	Correction of typos
1.3	2022-06-24	Updated systems to validate or qualify an identity

1 Introduction

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.

The purpose of this document is to summarise the essential concepts that all health actors need to know in this field. To deepen their knowledge, they can consult the best practices detailed further in the various sections of the *National Identity Security Standard*, or RNIV in French (see 2).

It is annexed to the "National eHealth ID" Reference Document, which it complements.

2 National Identity Security Standard (RNIV)

2.1 General description

The RNIV formalises the best practices to be adopted by all health actors for:

- *primary identification* (search, create, or edit a digital identity)
- *secondary identification* (verify the link between the patient, their file, and the care provided)
- *risk management* (RM) relating to identification (preventive and corrective actions)
- *policy and organisation* to shape the fight against misidentification (management)
- *INS management* (secure listing of health data).

It consists of six further parts detailing:

- the principles of patient identification common to all health care providers (RNIV 1)
- Implementation of identity security in health care facilities (RNIV 2)
- Implementation of identity security in non-hospital settings (RNIV 3)
- Implementation of identity security by providers in private practice (RNIV 4)
- regional identity surveillance policy and organisation (not finalised)
- national identity surveillance policy and organisation (not finalised)

2.2 Which component goes with which actor?

Where it's used	*RNIV*	*Comments*
In a healthcare facility (HCF)	1 + 2	Except in cases where RNIV 3 is applied by a regional decision (ARS)
In a social care facility or service (ESMS)	1 + 3	
In a coordinated private practice with more than 10 full-time equivalents	1 + 3	Except where RNIV 2 applies - by regional decision (ARS) - by voluntary choice of the practice - during an intervention in a facility covered by another component
In a coordinated private practice with no more than 10 full-time equivalents	1 + 4	Unless a voluntary choice is made to apply the RNIV 3, or in the event of involvement in a practice covered by another component (HCF, ESMS)
As a sole practitioner	1 + 4	Except in the case of involvement in a practice covered by another component (HCF, ESMS)
In support of care pathway coordination	1 + 3	
Service provider performing procedures without direct contact with patients	1 + 3	

3 Basic concepts

3.1 Identity security vocabulary

Identity: The set of civil status *traits* that characterise a person.

Digital identity: Representation of a physical individual in an information system.

Identifier: A unique code associated with the digital identity of an individual.

INS (National eHealth ID): A reference digital identity used in the health sector, extracted from a query to the INSi teleservice of the national reference identity base (INSEE).

Identification: Operation allowing the identity of an individual to be established with regard to civil status.

Primary identification: Operation to assign a specific digital identity to a patient.

Secondary identification: Consistency checks applied to patient identification or to the documents concerning that person, implemented to ensure that the right care is provided to the right patient.

Identity security: Arrangements made to ensure the reliability of patient identification and that person's health data.

Validation of digital identity: Consistency check with the official identity of the individual attested by a highly trusted scheme.

INS retrieval: Searching for a patient's INS through the INSi teleservice and recording the results in the mandatory traits of their digital identity, after checking for consistency with the traits of the person receiving care.

INS verification: Checking the consistency of the INS traits record or transmitted during a query to the INSi teleservice against the traits already present in the health information system or on a reference identity document.

3.2 INS

The INS is the reference digital identity for the healthcare and social care sector. It is formed of:

- the *INS number*, associated with an *object identifier* (OID) which specifies the nature of the number (NIR or NIA number, see 3.3);
- *INS* identity *traits* as recorded in the national reference databases (surname at birth, given name(s) at birth, date of birth, sex and INSEE code of place of birth).

The INS can be retrieved and/or verified by healthcare professionals through a dedicated teleservice called INSi, managed by the Health Insurance Fund.

Fictitious example of the set of INS traits returned by the INSi teleservice:

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

3.3 NIR, NIA, NSS, INS number

People born in France and foreigners working in France are registered in the *Répertoire national d'identification des personnes physiques (RNIPP* directory). Each individual listed has a unique identifier in this directory which is called the NIR (registration number). An NIA (temporary registration number) is allocated for persons not born in France before an NIR is permanently associated with the reference identity traits from public records.

The NIR is the *social security number* (NSS) of 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). In this case, the "entitled person" can be identified via their own NIR or via the trio: NIR of the entitled person, date of birth of the entitled person, and their order of birth. **The term *social security number* should be used in particular when referring to health costs or cash benefits paid by a compulsory health insurance organisation.**

The NIR is also the *INS number*. Unlike the NSS, it is unique for each individual**. The term *INS number* is to be used when talking about health data listed with the INS.**

4 Primary identification traits of a patient

4.1 Definitions

Primary identification involves the steps of searching for, creating, and/or modifying the digital identity assigned to a patient in the information system of the facility or professional tasked with that person's care. It includes the assignment of a trust status to the recorded data.

Digital identity is made up of a set of identification factors *(identity traits* or set of traits), which are specific to the patient to whom it refers. They are of varying importance and can be divided into strict and complementary traits.

4.2 Mandatory traits = official health identity

These are the traits that define the official identity of a healthcare user. They include five mandatory traits to create an identity (with fictitious data if necessary): surname at birth, first given name at birth, date of birth[1], sex, INSEE code of the place of birth[2]; they must be completed as soon as possible by the list of first names at birth and the INS number, for patients who have one. The individualisation of the first given name at birth is necessary for reasons of compatibility with many health software packages that are not yet adapted to the new identity security rules.

4.2.1 Collection of mandatory traits by querying the teleservice

The patient's national health identity (INS) is searched, retrieved and/or verified by querying the INSi teleservice[3]. When it is required, the query to this teleservice is made via the health information system (HIS) and entails the authentication of the patient (e.g. physical CPx card or digital authentication procedure) or of the institution (server certificate which may be issued subject to the institution's self-accreditation), in accordance with the requirements of the INS Reference Document.

The teleservice can be queried by a professional to search for the INS of a registered patient (see 3.3) in order to:

- either directly create their local digital identity with the recovered traits, when they are brought in for the first time
- or update their digital identity by registering the INS traits as mandatory traits, which is intended to improve the trust status of the digital identity (see 5.1).

Whenever possible, the INSi teleservice should be queried using the traits on the Carte Vitale. **The Carte Vitale is only used to facilitate the retrieval of the reference traits.**

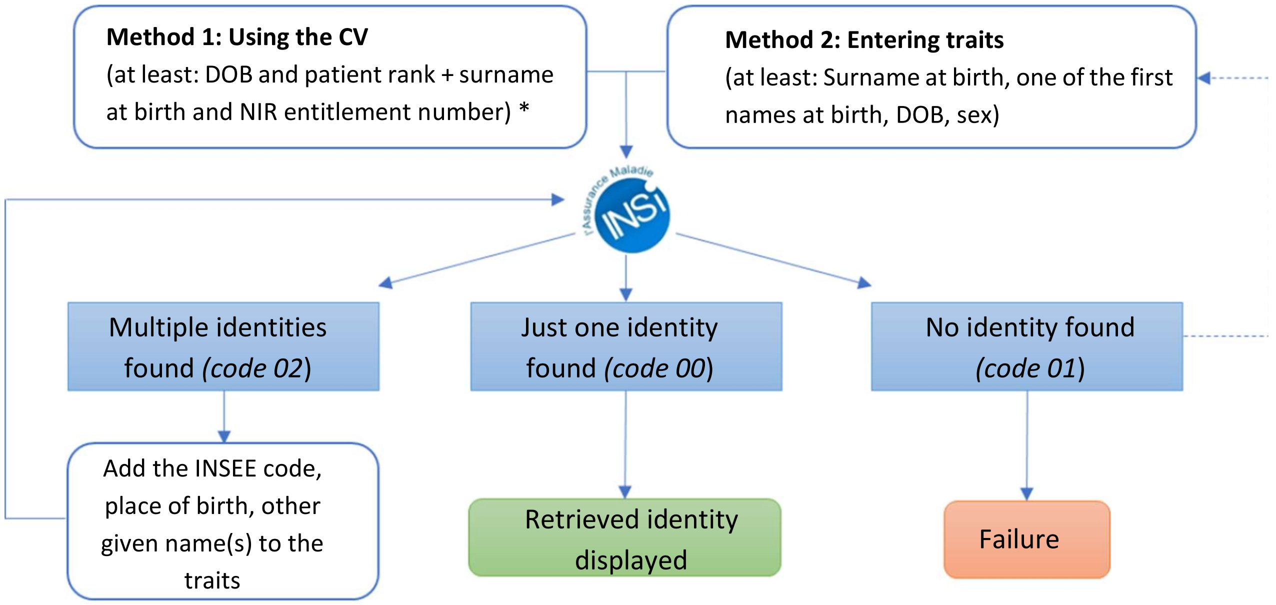
In cases where this method of accessing the teleservice is not possible or where the search based on the traits on the Carte Vitale is unsuccessful, it is possible to query the teleservice by entering the features with, at *a minimum*: the surname at birth, one of the given names at birth, the sex, the date of birth.

As a general rule, a perfect match must be found within the national databases in order to retrieve the INS. If the search is successful, the traits returned by the teleservice should only be accepted into the information system after checking for consistency with local information where the digital identity is known. **The mandatory traits that had previously been recorded are then replaced by those from the INS.**

[1] 31 December of a decade consistent with the age if unknown

[2] 99999 if unknown

[3] Whenever the query to the INSi teleservice is mentioned, the Carte Vitale application can also be used to retrieve the INS


Method 1: Using the CV
(at least: DOB and patient rank + surname at birth and NIR entitlement number) *
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

* Plus, if available, the patient's surname at birth and NIR, and if necessary their surname used.

4.2.2 Use of traits sent by a third party

When the patient is not yet known, it is possible to use the traits that serve to reference the transmission of health data, with or without an INS number, either through digital transmission (recommended method) or, failing that, by manual collection. If it is an INS, it is necessary to query the INSi teleservice to check it (see 5.3).

4.2.3 Manual collection of traits

Where the previous methods have been unsuccessful or where it is not possible to use the INSi teleservice, the remaining option is to enter the identity traits manually. They should be recorded on the most-trusted identity document (or its digital equivalent). Whenever possible, the patient or a relative should check the consistency of the information entered. Input rules are defined and must be adhered to. These rules are identical to those used for the INS.

4.3 Additional traits = useful information

These are other characteristics that are useful in caring for the patient (given name and surname used in everyday life, address and telephone number, people to contact, general practitioner, etc.). They are entered, depending on the nature of the traits according to the instructions established locally, on the basis of either the patient’s (or their relatives') statements or a document providing proof.

4.4 To find out more

- Chapters 3.1 and 3.2 of RNIV 1
- Appendices IV and VI of RNIV 1

5 Digital identity trust levels

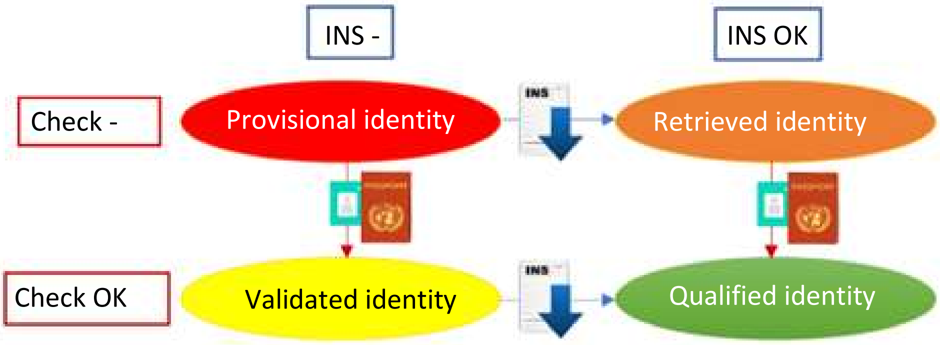
5.1 Digital identity statutes

Trust in the digital identity of a patient in the healthcare and social care fields is based on two major pillars:

- *retrieval* or *verification* of the INS (official mandatory traits) by querying the INSi teleservice;
- *validation* of mandatory traits during a consistency check with the patient's identity carried out using a highly-trusted identification scheme (see 5.2).

Depending on whether either or both of these criteria are met, the digital identity is assigned one of four trust statuses (which should ideally be displayed on the screens):

- *Provisional identity* status is assigned to any digital identity created without using the INSi teleservice and without checking the consistency of the traits through a highly-trusted identification scheme
- *Validated identity* status is assigned after checking the consistency of the traits recorded in *provisional identity* with those shown by a highly-trusted identification scheme
- *Retrieved identity* status corresponds to the registered (or verified) INS after querying the INSi teleservice, without checking the consistency of the traits through a highly-trusted identification scheme
- *Qualified Identity* status combines the retrieval (or verification) of the INS from the INSi teleservice and checking that the registered traits are consistent with those shown by a highly-trusted identification scheme.



Only *Qualified Identity* status, the highest level of trust in a digital identity, allows health data to be referenced and transmitted with the INS number.

5.2 Highly-trusted schemes

Only the following identity documents are considered a "high level of trust" for the *validation* of digital identity in the health sector: A passport, national identity card (for nationals of the EU, Switzerland, Liechtenstein, Norway, Iceland, the Vatican and the Principality of Monaco, San Marino and Andorra[4]), residence permit, the family record book (*livret de famille*) or a birth certificate for children (accompanied by a high level of trust from a parent) or for residents of a home for dependent elderly people who do not have an identity document (accompanied by a high level of trust from a descendant).

[4] 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.

This category also includes electronic identification schemes that provide a "substantial" level of assurance according to the eIDAS standard[5].

5.3 INS verification

Verification is an operation carried out via the INSi teleservice in order to check the consistency of an INS, transmitted by another health actor or registered in the health information system, with the reference traits. This check is indicated in 2 situations:

- when receiving an INS listing transmitted health data, when the corresponding local digital identity does not exist or is registered with a status lower than *Qualified Identity*
- to check the compliance of INS identities registered in the information system during a one-off (unitary) or systematic (mass) verification operation carried out every 3 to 5 years.

5.4 To find out more

- Chapter 3.3 of RNIV 1
- Appendix VII of RNIV 1

6 Secondary identification

6.1 Definition

Secondary identification corresponds to the means implemented, during the care of a physical patient by a professional, to ensure the delivery of "the right care to the right patient". In particular, it consists of checking, at each stage of care, the consistency between the patient's real identity and the one displayed on the documents and care tools (physical or computer file, prescription, label, travel voucher, examination report, etc.).

6.2 Secondary identification techniques

Various means can be used to secure this stage, such as

- seeking the patient's active participation in their own identification, whenever possible ("the patient playing a role in their own security"), by asking that person to declare all or part of their identity
- asking the patient open-ended questions ("What was your surname at birth?" "What is your given name?", etc.) while avoiding closed-ended questions like "Are you Mr/Mrs WHOEVER?"
- taking into account the additional traits *surname used* and the *given name used* where they exist, in order to use the identity traits that the patient uses in everyday life when they are addressed directly
- the use of physical identification schemes such as wristbands, a photograph placed in the patient's file, subject to respecting the patient's rights
- regular verification that the identity of the patient being treated (as stated or verified by the physical identification scheme) matches the one recorded on the documents (prescription, pill box, label, reports, test results, etc.).

[5] The "eIDAS" Regulation No. 910/2014 of 23 July 2014 aims to increase trust in electronic transactions within the internal market. It establishes a common basis for secure electronic interactions between citizens, businesses, and public authorities and is available at https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-reglement-eidas/

6.3 To find out more

- Chapter 4.3 of RNIV 1
- Chapter 3.3 of RNIV 2, 3 and 4

7 Listing of health data

7.1 Basic rules

In order to secure the exchange and sharing of information between professionals, it is essential that all health data be listed with a minimum of identification traits.

At least the following mandatory traits must be found on documents containing health information data: surname at birth, given name(s) at birth, date of birth, sex and - if the identity is *qualified* (see 5.1) - INS number followed by its type (NIR or NIA).

For documents with limited space, such as labels, the following should appear, as a minimum: Surname at birth, given name(s), date of birth and sex.

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

7.2 Transmitting health data

The exchange and sharing of a patient's health data between the professionals who care for that person can be done by computer, secure e-mail, or post.

When exchanged directly between information systems, identity traits are exchanged according to interoperability standards that can tell the type of each trait and inform the receiver what the status of the transmitted identity is.

When the exchanges use printed documents, care must be taken to ensure that the traits cannot be confused with each other.

7.3 To find out more

- Chapter 3.4 of RNIV 1
- Appendix VIII of RNIV 1

8 Organising risk management in identity security

8.1 Policy and governance

All health actors must adhere to good identification practices and participate in the fight against errors in this area. The objectives of the policy conducted and the organisation implemented may differ by healthcare facility or region.

Apart from the professionals in charge of identity security, it is important for every actor to:

- identify who they are speaking with in the field of identification security
- know where to look for information about best practice for the tools they use

8.2 Identity security contacts

Each healthcare facility with more than 10 professionals must designate an *identity security contact* who is the main contact person within the facility in the event of a problem relating to patient identification.

It is also possible for actors who do not have a local contact to call on the expertise of the *regional identity security contact* for any question relating to identity security or for any question relating to patient identification or the transmission of identity traits between facilities.

8.3 Quality documents relating to identity security best practices

The management of risks relating to the misidentification of patients is governed by internal arrangements specific to each healthcare facility. It provides quality documentation that is accessible to any professional working there, either in paper form or through a dedicated electronic application. The documents (policy, procedures, protocols, etc.) describe the best practices to be adopted for primary and secondary identification, the use of IT tools, and the reporting and management of adverse events stemming from an identification error.

8.4 To find out more

- Chapter 4 of RNIV 1
- RNIV 2, 3, 4 (arrangements at the facility level)

MINISTÈRE
DE LA SANTÉ
ET DE LA PRÉVENTION

Liberté
Égalité
Fraternité

Direction générale
de l'offre de soins