Resource: Reference Framework MR-008

Deliberation No. 2023-083 of 20 July 2023 approving a reference methodology for the processing of data from the main database of the National Health Data System implemented for the purposes of research, study or evaluation in the field of health by organisations acting in their legitimate interests (MR-008)

Title I: DEFINITIONS, DATA CONTROLLERS CONCERNED, SCOPE AND PUBLIC INTEREST

1.1. Definitions

For the purposes of this methodology, the following terms are defined as follows:
Review: a summary, sent to the CNIL every three years by the data controller, reporting on the uses of the reference methodology observed during that period;
French Scientific and Ethical Committee for Research, Studies and Evaluations in the Health Sector (CESREES): committee that issues a reasoned opinion on the research methodology, the need to use personal health data, the relevance of such data in relation to the purpose of the processing and, where applicable, on the scientific and ethical relevance of the project as well as on the public interest of the research, study or evaluation;
Personal data: any information relating to an identified or identifiable natural person (“data subject”); an “identifiable natural person” is deemed to be a natural person who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier, or to one or more factors specific to his or her physical, physiological, genetic, mental, economic, cultural or social

identity (see. Art. 4 of the GDPR). As such, SNDS data, although pseudonymised, constitutes personal data;
Controlled environment: set of resources (hardware, software, personnel, data) to which the manager of a National Health Data System (SNDS) system applies the requirements of the SNDS security standard;
Secure processing environment : workspace dedicated to a study, secured and controlled by the system manager providing access to SNDS;
Study: research or study in the field of health that does not meet the definition of research involving the human subject as defined in Article L. 1121-1 of the Public Health Code (CSP). It may also be an evaluation or analysis of healthcare or prevention practices or activities, within the meaning of Article 72 of the Data Protection Act. This processing must be in the public interest within the meaning of Article 66 of the same Act. A study may require several queries to be made using SNDS data;
Expression of needs: document indicating the components of the main SNDS database concerned by the request for access, the target population, the target period, the data or categories of data required, the historical depth of the data and the duration of access requested, for which a model developed in collaboration with the HDH and the French National Health Insurance Fund (CNAM) is made available;
Study office: organisation responsible, where applicable, for implementing data processing and in charge of analysing the data, having made a commitment to the CNIL to comply with the decree of 17 July 2017 relating to the guidelines determining the criteria of confidentiality, expertise and independence for design offices and contract research organizations. This is a subcontractor within the meaning of the GDPR which, under this reference methodology, is the only entity authorised to access SNDS data in place of the data controller(s);
The Health Data Hub (*Plateforme des données de santé* - HDH): a public interest group formed by the French government, organisations representing patients and users of the healthcare system, health data producers, and public and private users of health data, including health research organisations, responsible for implementing the main strategic guidelines relating to the SNDS and thus facilitating the sharing of health data from various sources in order to promote research;
Historical depth of data: years of data production required to carry out the study;
Protocol: document specifying, in particular, the research methodology, the purpose of processing personal data, the categories of individuals concerned by the data processing, the origin, nature and list of personal data used and the list of the justification for their use, the duration and organisational methods of the research, study or evaluation, the data analysis method and, when required by the characteristics of the study, research or evaluation, the justification for the number of individuals to include and the chosen method of observation or investigation chosen;
Scientific officer or data processing manager: the person appointed by the data controller, acting under their responsibility, to ensure the quality, integrity and security of the information and processing thereof, as well as compliance with the purpose of the processing;
Data controller: the natural or legal person who, alone or jointly with others, is responsible for a research, study or evaluation not involving human persons, ensures its management, verifies that its funding is secured and determines the purposes and means of the processing necessary for it;
Subcontractor: a natural or legal person, public authority, service or other body that

processes personal data on behalf of the data controller;
National Health Data System (*Système national des données de santé* - SNDS): health database comprising a main database, covering the entire population, as well as other databases integrated into a “catalogue”;
Processing: any operation or set of operations which may or may not be performed using automated processes and applied to personal data or sets of personal data, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
User: a natural person who accesses individual data from the SNDS made available in a project area.

1.2. Data controllers concerned

1.2.1. The only persons who may make a declaration certifying compliance with this reference methodology are data controllers for whom the implementation of research, studies or evaluations in the field of health is necessary for the pursuit of a legitimate interest within the meaning of Article 6.1.f of the GDPR, with the exception of the organisations mentioned in Paragraph 1 of A and Paragraphs 1, 2, 3, 5 and 6 of B of I of Article L. 612-2 of the Monetary and Financial Code and insurance intermediaries mentioned in Article L. 511-1 of the Insurance Code.
1.2.2. In the case of joint responsibility for processing, the data controllers must define, in a transparent manner, their respective obligations in accordance with Article 26 of the GDPR.

1.3. Processing of personal data included in the scope of this methodology

1.2.1. Only the processing of personal data for the purpose of conducting research, studies or evaluations in the field of health, which is in the public interest within the meaning of Article 66 of the Data Protection Act and which complies with the following security, organisational and transparency requirements, may be subject to a declaration of compliance with this reference methodology:

- a protocol and an expression of requirements must be drawn up by or under the responsibility of the data controller before the data processing operation begins. These documents must be submitted to the CESREES;
- the processing operations covered by this reference methodology must obtain an expressly favourable opinion from the CESREES prior to their implementation. When this opinion is accompanied by recommendations, the data controller undertakes to take them into account and to amend the file accordingly, prior to processing the data;
- the data processed must come exclusively from the CNAM, which alone is competent, within the framework of this methodology, to extract and transmit SNDS data, in strict compliance with the expression of needs;
- the data processed must also come directly from the CNAM. No re-use of data is

permitted under this reference methodology;
- data processing may only be carried out by a study office or contract research organization, whether public or private, that has made a commitment to the CNIL to comply with the Decree of 17 July 2017 relating to the guidelines determining the criteria of confidentiality, expertise and independence for design offices and contract research organizations;
- the data is made available to the study office or contract research organization in a project area within a controlled environment, as defined in point 1.1 (definitions), and which meets the following cumulative conditions:
- has been approved in accordance with the security standard applicable to the SNDS. This approval, which must not have expired, is subject to regular monitoring and is regularly renewed within the time limits specified in the approval decision;
- has been assessed by the CNIL in the context of data processing that has been expressly authorised by the CNIL. This authorisation must be less than three years old;
- complies with Title V of this Deliberation concerning data hosting methods and the absence of transfers outside the European Union;

- the data controller does not have access to individual data in the SNDS. Therefore, they cannot themselves be the manager of the controlled environment used in the studies covered by this reference methodology;
- the data controller undertakes not to pursue any of the prohibited purposes described in Article L. 1461-1 V of the Public Health Code;
- the data controller and, where applicable, the data processor, must first sign a data access agreement with the manager of the controlled environment providing the SNDS data. They must also have each authorised user sign an individual commitment to comply with the conditions of use defined by the controlled environment. Finally, the data controller must send the manager of the controlled environment an updatable list of the design offices or contract research organizations it uses;
- the data controller undertakes to send the CNIL and the CESREES, every three years, a report summarising the uses of the reference methodology observed during that period. If they deem it relevant, the CNIL or the CESREES may share this report with the CNAM and/or the HDH;
- the data controller must register each study carried out within the framework of the reference methodology in the public directory maintained by the HDH. The method and the results obtained are published by the HDH at the end of the processing, in accordance with the procedures set out in paragraph 6.3: “Principle of transparency”.

1.3.2. In particular, this reference methodology does not apply to the following processing operations:

- hosted outside a controlled environment that meets the cumulative conditions mentioned above;
- requiring the matching of SNDS data with personal data from other sources (for example: medical records);

- requiring the reuse of data made available in a previous study or from a health data warehouse containing SNDS data.

1.3.3. The processing operations mentioned in Paragraph 1.3.2 may only be implemented after authorisation from the CNIL.

1.4. Public interest and prohibited purposes

1.4.1. Processing carried out within the framework of this reference methodology must:

- be in the public interest, justified by the data controller in the protocol, which will be sent to the HDH when it is recorded in the public directory;
- comply with all the legislative and regulatory provisions relating to the SNDS (Articles L. 1461-1 to L. 1461-7 of the Public Health Code), in particular the prohibition on using this data for the purposes described in Article L. 1461-1 V of the Public Health Code:

1. the promotion of the products mentioned in Paragraph II of Article L. 5311-1 to healthcare professionals or healthcare institutions;
2. the exclusion of cover under insurance contracts and the modification of insurance contributions or premiums for an individual or a group of individuals presenting the same risk.

Title II: PROCESSING OF DATA RELATING TO INDIVIDUALS CONCERNED BY STUDIES

2.1. Purpose of processing

1.4.1. Only data processing for the purposes of research, studies or evaluations in the field of health, as detailed below, may be carried out under the reference methodology:

- comparative assessment of healthcare provision;
- changes in care practices;
- comparative analyses of healthcare activities;
- description and analysis of pathologies and patient care pathways;
- epidemiological and/or medico-economic studies, including studies to prepare cases for discussions and meetings with the competent authorities and committees, or studies for monitoring purposes;
- feasibility studies or targeting of centres for carrying out research involving or not involving the human person.

1.4.2. The main or secondary purpose or effect of the proposed processing of personal data of data subjects must not be to enable one or more of the prohibited purposes described in Article L. 1461-1 V of the Public Health Code to be achieved.

2.2. Origin and nature of data
2.2.1. Origin of personal data

2.2.1.1. The data must come exclusively and directly from the databases made available by the CNAM.

2.2.2. Nature of personal data

2.2.2.1. Pursuant to Article 5, Paragraph 1, point c of the GDPR, the data processed must be relevant, adequate and limited to what is necessary for the purposes for which it is processed (principle of data minimisation). In this respect, the data controller undertakes to only process data that is strictly necessary and relevant to the study objectives. Consequently, each category of data may only be processed if its processing is justified in the protocol.
2.2.2.2. The following categories of personal data may be processed within the framework of this methodology:
For data subjects:
2.2.2.3. Only data from the main SNDS database, as defined in Article R. 1461-2 of the Public Health Code, may be processed. This database currently comprises:

- data from the information systems mentioned in Article L. 6113-7 of the Public Health Code (PMSI database);
- data from the French National Health Insurance Inter-Schemes Information System referred to in Article L. 161-28-1 of the Social Security Code (SNIIRAM database);
- data on causes of death referred to in Article L. 2223-42 of the General Local Authorities Code (INSERM CépiDC database);
- medico-social data from the information system mentioned in Article L. 247-2 of the Social Action and Family Code (data relating to disability);
- data from the “Vaccin-Covid” and “SI-DEP” (screening information system) databases.

2.2.2.4. The processing included in this reference methodology covers data with a maximum historical depth of nine years in addition to the current year, provided that it can be disseminated by the CNAM.
2.2.2.5. In particular, the following must be justified in the protocol with regard to the purpose of the processing: the categories of data processed, the period for targeting data subjects, the components of the SNDS and the historical depth of the data consulted, the access duration, the geographical area and the number of data subjects.

For users:
2.2.2.6. The following categories of personal data relating to users may be processed:

- surname, first names, job title, access profiles;
- if relevant:
- professional telephone, postal and/or electronic contact details, employer;
- training, qualifications;
- elements needed to evaluate the knowledge to carry out the study.

2.2.2.7. Users' data is must only be processed for the sole purpose of carrying out the study and complying with the data controller's legal obligations.
2.2.2.8. In particular, the purpose of the data processed is to manage declarations of interest, to send them to the HDH, where necessary, and to manage internal authorisation procedures.

2.3. Those who access and receive processed data (users)

2.3.1. The data is made available to the study office or the contract research organization within a controlled environment. The data controller does not have access to individual data in the SNDS.
2.3.2. The data processor shall keep up-to-date and make available to the data controller documents specifying those responsible within the company for issuing authorisation to access data, the list of those authorised to access data, their respective access profiles and the procedures for granting, managing and checking authorisations.
2.3.3. Only authorised persons from the study office and contract research organization may access the data, in compliance with the provisions set out in Article 3 of the standards determining the criteria of confidentiality, expertise and independence for design offices and contract research organizations.
2.3.4. These categories of people are subject to professional secrecy under the conditions defined by Articles 226-13 and 226-14 of the French Criminal Code.
2.3.5. The classification of authorised people and their access rights must be regularly reassessed, by the study office or contract research organization, in accordance with the procedures described in the authorisation procedure drawn up by the data processor, in compliance with any instructions given by the data controller.

2.4. Information and rights of individuals concerned by the study
2.4.1. Informing individuals

2.4.1.1. In the case of data originating exclusively from the SNDS, the persons concerned are informed of the possible reuse of their personal health data in accordance with the terms defined in Article R. 1461-9 of the Public Health Code.
2.4.1.2. The provisions of Article 69 of the Data Protection Act, which establish the principle of individual notification of persons whose data is processed, are applicable to all

processing carried out using SNDS data.
2.4.1.3. However, pursuant to the provisions of Article 14.5.b of the GDPR, the data controller may invoke an exception to the obligation to provide individual information for the implementation of processing involving exclusively data from the main SNDS database.
2.4.1.4. In this case, they must take appropriate measures to protect the rights and freedoms and legitimate interests of the data subjects, including by making the information publicly available.
2.4.1.5. In this regard, the information provided to the data subjects cannot be limited to the registration of the study in the HDH public directory.
2.4.1.6. Within the framework of this reference methodology, the public must be informed of the implementation of each research project, study or evaluation in the field of health.
2.4.1.7. As a minimum, the following measures must be implemented to ensure that information is publicly available:

- publication of the information note on the data controller's website and, where applicable, the study office or contract research organization's website;
- implementation of a transparency portal when the data controller carries out several studies using SNDS data. This transparency portal includes general information on the SNDS and a specific information note for each study carried out.

2.4.1.8. Other collective information methods may also be used, depending on the characteristics of the studies carried out (social networks, patient associations, press releases, etc.).
2.4.1.9. These documents must contain all the information required by Article 14 of the GDPR.

2.4.2. Exercising individual rights

2.4.2.1. The data subject shall exercise their rights to access, rectify, remove, restrict and object to processing carried out within the framework of this methodology, directly with the data protection officer of the body responsible for data processing.
2.4.2.2. The information provided to users, as well as the procedures for exercising their rights, must comply with the principle of transparency set out in Chapter III of the GDPR.

2.5. Data access and storage duration

2.5.1. This period must be limited to the time strictly necessary for the processing and must not exceed the duration of the study. In any event, this duration of access or storage may not exceed five years from the last time the data is made available. In exceptional cases, this period may be extended for a maximum of two years, upon substantiated request by the data controller to the CESREES, which will then issue a new opinion. No data may be archived.
2.5.2. Personal data processed within the framework of this methodology may not be

stored outside the controlled environment used by the study office or contract research organization.
2.5.3. Only anonymous results, within the meaning of Article 29 Data Protection Working Party (G29) Opinion No. 05/ 2014 2014 or any subsequent EDPS opinion on anonymisation, may be exported.
2.5.4. The personal data of users responsible for carrying out the study may not be kept any longer than five years after the end of the study.

2.6. Publication of results

2.6.1. In accordance with the provisions of the Data Protection Act, the presentation of the results of the data processing will under no circumstances allow direct or indirect identification of the individuals concerned.

Title III: SECURITY

3.1. The processing of data from the National Health Data System and its components must be carried out in accordance with the provisions of Articles L. 1461-1 to L. 1461-7 of the Public Health Code.
3.2. The security measures must comply with the security standard applicable to the National Health Data System, provided for in the Decree of 22 March 2017 and subsequent updates.
3.3. The design offices and contract research organizations must comply with the Decree of 17 July 2017 relating to the guidelines determining the criteria of confidentiality, expertise and independence for design offices and contract research organizations.
3.4. Systems providing access to the data referred to in this methodology must therefore comply with the aforementioned SNDS security standard.
3.5. In accordance with the aforementioned standard, the data controller must ensure that the agreement concluded with the study office or contract research organization specifies the security measures and conditions relating to compliance with the aforementioned standard. In particular, the controlled environment must be approved prior to the implementation of the data processing required for the study.
3.6. The data controller or, where applicable, the data processor, must adopt the following technical and organisational measures:

Division of roles and responsibilities

SEC-REP-1	The division of roles and responsibilities between the data controller(s), the data processor and the manager of the controlled environment must be set out in an agreement. This agreement must cover, in particular, awareness-raising among study users, trace monitoring, alert and incident management, and the management of anonymous data exports. This agreement must comply with Article 28 of the GDPR.
Management of authorisations and logical access to data	
SEC-HAB-1	Different authorisation profiles must be provided to manage access to data on an as-needed and exclusive basis.
SEC-HAB-2	Individuals authorised to access personal data must be individually authorised according to a procedure involving validation by their supervisor.
SEC-HAB-3	Authorisations must be reviewed regularly, at least annually, and at the end of each study.
SEC-HAB-4	Access permissions must be withdrawn as soon as authorisations are withdrawn, for example after the departure of an authorised user or a change in their roles and responsibilities.
User identification and authentication	
SEC-IDE-1	Access to personal data must be subject to local or national identification for any natural or legal person, in accordance with the requirements of level 2 of the PGSSI-S identification guidelines.
SEC-IDE-2	Access to personal data must be subject to strong authentication involving at least two distinct authentication factors, in accordance with the requirements of level 2 of the PGSSI-S authentication guidelines. If one of these factors is a password, it must comply with the CNIL's recommendations on passwords on the date of drafting of this methodology (Deliberation No. 2022-100 of 21 July 2022).
Project area	

SEC-ESP-1	Data from a study must only be handled by authorised users in a project area specific to this study, which is sealed with data from the central SNDS and with the project areas of other studies conducted in the same controlled environment.
SEC-ESP-2	Data sets imported into a project area specific to a study must be kept to a minimum and limited to only the data required for the study. A unique number specific to each project area must be generated under the same pseudonymisation conditions as those defined by the aforementioned security standard applicable to the SNDS. For example, this unique number could be generated by a cryptographic hash function able to withstand brute force attacks or a cryptographically secure pseudorandom number generator.
Data transmission	
SEC-TRA-1	All data transmissions from or to the controlled environment or project areas must be encrypted in accordance with Appendix B1 of the General Security Reference System (RGS) in order to guarantee confidentiality. These encryption measures apply to data in transit and to its storage after reception in the controlled environment or project areas.
Exporting anonymous data beyond workspaces	
SEC-EXP-1	Only anonymous data sets may be exported outside the controlled environment or a project area. The anonymisation process must produce a data set that complies with the three criteria set out in G29 Opinion 05/2014 or any subsequent EDPS opinion on anonymisation. This compliance must be documented. Otherwise, if the three criteria cannot be met, a study of the risks of re-identification must be carried out and documented prior to each export.
SEC-EXP-2	Data exports must be subject to prior validation by a manager in order to endorse the principle, particularly with regard to the SEC-EXP-1 requirement.
SEC-EXP-3	Exports must be monitored automatically or manually by a specialist operator to ensure that are anonymous. If this monitoring is automatic, any export identified as non-compliant must be subject to an alert and quarantined in a dedicated partitioned area, before being checked manually by a specifically trained and authorised manager.

User awareness and work station security	
SEC-SEN-1	All individuals authorised to access the controlled environment must be trained to respect professional secrecy and regularly informed of the risks and obligations related to processing health data.
SEC-SEN-2	All individuals authorised to access the controlled environment must sign a privacy policy. This policy must set out the obligations with regard to both the protection of personal health data and the security measures implemented in the controlled environment, as well as the penalties for non-compliance with these obligations.
SEC-SEN-3	The work stations of individuals authorised to access the controlled environment, including external users accessing project areas only, must be subject to specific security measures, for example by setting up personal accounts, appropriate authentication, automatic session locking, hard disk encryption and filtering measures. If the work stations are not under the control of the data controller, the security measures to be implemented at the work stations must be governed by an agreement between the parties concerned.
Logging	
SEC-JOU-1	The actions of users in project areas and those of users in the controlled environment must be subject to logging measures, in accordance with the requirements of level 3 of the PGSSI-S accountability guidelines. In particular, connections (login details, date and time), requests and operations carried out must be logged.
SEC-JOU-2	Traces must be monitored regularly, at least once a month, and at the end of each authorisation period linked to a study. This monitoring must be carried out by: - an automatic monitoring solution with alerts dealt with manually by an authorised operator; - or by a semi-automatic control by running programmes to select abnormal traces, followed by manual rereading by an authorised operator.

SEC-JOU-3	The logging traces defined in the SEC-JOU-1 requirements must be kept for a period of six months to one year from the time they are collected, unless an exception is justified by the extent of the risk to individuals in the event of misapplication of the processing purposes and the frequency of such practices. In case of the latter, the maximum storage duration for logging traces can be extended to three years.
Management of security incidents and personal data breaches	
SEC-INC-1	The parties concerned by the agreement must establish a procedure for managing and handling security incidents and personal data breaches, specifying the roles and responsibilities and the actions to be taken in the event of such incidents.
SEC-INC-2	Any security incident, whether malicious or not and whether intentional or not, which has the effect, even temporarily, of compromising the integrity, confidentiality or availability of personal data must be documented internally in a register of breaches.
SEC-INC-3	Any data breach must be notified to the CNIL under the conditions set out in Article 33 of the GDPR.
SEC-INC-4	In the event that the breach is likely to result in a high risk to the rights and freedoms of an individual, the data controller must inform the data subjects of the data breach as soon as possible, in accordance with Article 34 of the GDPR.

3.7. These measures are not exhaustive and will have to be completed depending on the risks weighing on the processing implemented.
3.8. Furthermore, Articles 5.1.f and 32 of the GDPR require security measures to be updated with regard to the regular reassessment of risks and to ensure ‘state of the art’ measures.

Title IV: SUBCONTRACTORS

4.1. The data controller never has access to individual data in the SNDS and must use, for all processing, an independent study office or contract research organization, a subcontractor that has declared itself to the CNIL in accordance with the guidelines determining the criteria of confidentiality, expertise and independence for design offices and contract research organizations, as per Order of 17 July 2017.

4.2. This obligation to use a study office or contract research organization does not apply to the latter when it is acting as data controller.
4.3. In accordance with this decree and Article 28 of the GDPR, the respective commitments of the data controller and the study office or contract research organization are set out in an agreement, the content of which is defined by these texts.
4.4. In addition, subcontractors:

- must appoint, where necessary, a data protection officer in accordance with Article 37 of the GDPR;
- must keep a register of the categories of processing operations carried out on behalf of the data controller, in accordance with Article 30 of the GDPR.

The data controller(s) undertake(s) to:

- have no connections with the study office or contract research organization and the purpose of the processing operation that might constitute a conflict of interest;
- not seek access to personal data made available to the study office or contract research organization;
- not use the results provided for any of the prohibited purposes.

Title V: HOSTING OF SNDS DATA AND ABSENCE OF DATA TRANSFERS OUTSIDE THE EUROPEAN UNION

5.1. Within the framework of this reference methodology, the study data controller(s) shall ensure:

- that data from the SNDS main database is hosted exclusively in member countries of the European Economic Area, with no possibility of data being transferred outside the European Union;
- the absence of remote access to data from outside the European Union.

5.2. In addition, organisations and, where applicable, their subcontractors, accessing SNDS data in the context of hosting operations for the controlled environment technical infrastructure, as well as the administration and operation associated with this storage, must be subject exclusively to the laws of the European Union.

Title VI: IMPLEMENTATION OF THE PRINCIPLE OF RESPONSIBILITY

6.1. Data protection impact assessment

6.1.1. The data controller shall carry out a data protection impact assessment in

accordance with the provisions of Article 35 of the GDPR, which must cover in particular the risks to the rights and freedoms of data subjects.
6.1.2. This impact assessment must be reviewed and updated regularly, particularly if significant changes are planned to the processing carried out under this methodology, or if the risks to data subjects have changed.
6.1.3. One single analysis may cover a set of similar processing operations presenting similar risks.

6.2. Formalities

6.2.1. Each data controller appoints a data protection officer in accordance with Article 37 of the GDPR. The data protection officer's main role will be to check the compliance of the processing carried out in accordance with this methodology.
6.2.2. The data controller shall submit a single declaration of compliance with this methodology to the CNIL for all the processing operations implemented, provided that they are and will be carried out in compliance with all the provisions of the methodology.
6.2.3. In the case of shared responsibility, each data controller makes a declaration of compliance with the reference methodology on their own behalf.
6.2.4. The processing operations covered by this reference methodology must obtain an expressly favourable opinion from the CESREES prior to their implementation. To obtain this opinion, a request must be submitted to the HDH single secretariat and must include the information listed in this methodology.
6.2.5. In accordance with Article 30 of the GDPR, the data controller shall keep an up-to-date list of the processing operations carried out under this methodology in the register of processing operations. They regularly check the compliance of processing operations underway with the requirements of the reference methodology and shall document this analysis.

6.3. Principle of transparency

6.3.1. The legal framework governing the provision of SNDS data is designed to ensure that the public is informed about how the data is used. To this end, Article L. 1461-3 of the Public Health Code makes access to SNDS data and its components conditional upon the data controller providing the HDH with certain information before and after the study.
6.3.2. Accordingly, the data controller undertakes to record each study carried out using this methodology in the public directory held by the HDH.
6.3.3. This record must be made before the start of each study by the data controller or the person acting on their behalf. Simultaneously, a file containing the following is sent to the HDH:

- the protocol, including justification of the public interest, as well as a summary, according to the model made available by the HDH. In the event of a favourable opinion with recommendations from the CESREES, the protocol and the summary, which clearly take

account of the recommendations, must be recorded;
- the declaration of interests, in relation to the subject of the study, of the data controller, as well as that of the study office or contract research organization, as provided for in Article 5 of the aforementioned Decree of 17 July 2017.

6.3.4. At the end of the study, the method and results obtained must be communicated to the HDH with a view to publication, in compliance with trade secrecy and intellectual property rights.
6.3.5. The recording of the processing and transmission of the results are carried out in accordance with the procedures defined by the HDH.

6.4. Review

6.4.1. The data controller, where applicable after consulting the subcontractor(s), sends the CNIL a report summarising their observed uses of this reference methodology every three years, indicating in particular:

- the number of studies implemented over the period analysed;
- the types of purpose pursued;
- the methods of financing projects and partners (in particular public funding, etc.);
- on the data processed:
- the SNDS components mostly frequently called upon;
- the overall compliance of the expression of needs with the objectives of the study;
- the average historical depth called upon and whether or not it is sufficient;
- the average number of people concerned by the studies;
- the average duration of access to or storage of the data requested and whether or not it was sufficient;

- collective information media used;
- the status of individuals authorised to access SNDS data;
- on data security:
- security incidents, likely to impact the rights of individuals, possibly revealed or avoided;
- any substantial modification to the architecture of the controlled environment;

- the number of scientific publications resulting from the research, studies and evaluations carried out within the framework of the methodology;
- the benefits, scientific contributions observed and/or measured.

Title VII: ENTRY INTO FORCE

7.1. This reference methodology enters into force upon its publication in the Official Journal.

7.2. Where research, studies or evaluations in the field of health, previously authorised by the CNIL, undergo substantial modification and comply with this methodology, no new authorisation from the CNIL is required.
7.3. This decision will be published in the Official Journal of the French Republic.

The Chair,
M.-L. Denis