Deliberation 2021-123 of November 2, 2021Commission Nationale de l'Informatique et des LibertésLegal status: In force Date of publication on Légifrance: Wednesday November 24, 2021NOR: CNIL2132900XDeliberation no. of a personal nature implemented for the purpose of creating data warehouses in the field of health adopted on October 7, 2021The National Commission for Computing and Liberties,

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (general regulation on the data protection), in particular Article 58 thereof;

Considering the law n° 78-17 of January 6, 1978 modified relating to data processing, files and freedoms, in particular its article 8-I-2°-b);

Having regard to the Commission's rules of procedure, in particular its article 19; The Commission finds material errors in the deliberation as well as in the reference system relating to the processing of personal data implemented for the purposes of creating data warehouses in the field of health appended to deliberation no. 2021-118 of October 7, 2021 adopting it.

The resolution is therefore amended as follows:

In the visa referring to the Data Protection Act, the word: articles is replaced by: article.

The reference is therefore modified as follows:

In point 2.2 of the reference system, the terms: declaration of are replaced by: declaration of;

In point 3.2.2.1 of the reference system, the terms: 5.1 are replaced by: 5.2;

In point 5.1 of the guidelines, the terms: and that their collection are replaced by: and whose collection;

In point 5.6 of the reference system, the terms: 5.3.1.1 are replaced by: 5.2.1.1;

In point 6.2 of the reference system, the terms: must be are replaced by: must be;

In the first sentence of point 7.2 of the reference system, the terms: in points 5.2.1.2 and 5.2.1.3 are replaced by: in point 5.2.1.2;

In the second sentence of point 7.2 of the reference system, the terms: in points 5.2.1.2 and 5.2.1.3 are replaced by: in point 5.2.1.2;

In point 8.2.2.2 of the reference system, the terms: highlighted are replaced by: highlighted;

In point 12.2 of the reference system, the terms: cannot lead to are replaced by: cannot lead to. Who is this reference intended

for? This reference is intended for data controllers who wish, as part of their public interest missions, to collect data with a view to their reuse, for the purposes mentioned in point 3.1.1.1 of such processing is hereinafter referred to as health data warehouses .1.2. The standard also applies to warehouses implemented by joint controllers who define their respective obligations in accordance with Article 26 of the GDPR.1.3. Are not concerned by this standard: the warehouses implemented by a private company on the basis of its legitimate interest; the processing of personal data implemented solely for the purposes of preventive medicine, medical diagnostics, administration of care or treatment, or the management of health services and implemented by health professionals and health care systems or services (e.g.: dematerialized medical records); the processing of personal data staff implemented when the person has given their explicit consent for this purpose; Warehouses matched with the main database of the National Health Data System as defined in Article L. 1461-1 of the Public Health Code.2 . Scope of the standard2.1. This standard specifies the legal framework, resulting from the General Data Protection Regulation (GDPR) and national provisions, applicable to health data warehouses.

2.2. Data controllers who make a declaration of compliance with this standard to the Commission are authorized to implement a health data warehouse when the processing strictly complies with the standard. To declare compliance with the standard: "Declare a file" - section "declaration of conformity"

2.3. Any processing of personal data aimed at implementing a health data warehouse that does not comply with all the requirements defined by these standards must be the subject of a specific authorization request, in accordance with the provisions of Article 66 III of the Data Protection Act. To request authorisation: "Declare a file" - section "health authorization request - purpose of public interest"

2.4. Data controllers must implement all appropriate measures (technical and organizational) to guarantee the protection of the personal data processed, both from the design of the processing and by default, as provided for in Article 25 of the GDPR . They must also demonstrate this compliance throughout the life of the treatments. The warehouses implemented within the framework of the repository must also be registered in the register of processing activities provided for in Article 30 of the GDPR.

2.5. The principles laid down in this reference document also constitute assistance in carrying out the data protection impact analysis (DPIA) that the data controllers concerned must carry out (see point 13 of this reference document).

2.6. Pursuant to Article 65.1 of the Data Protection Act, the warehouses implemented after obtaining consent in accordance

with Article 7 of the GDPR on the basis of Article 9.2.a of the GDPR from each of the persons concerned are not not subject to prior authorization by the Commission or to a declaration of conformity with this standard. However, the Commission recalls that the principles and measures set out in these guidelines can be applied to all processing of health data of the same nature, regardless of their legal framework.

2.7. The processing of personal health data implemented for the purposes of research, studies or evaluation in the field of health, from the data contained in the warehouse, constitutes separate processing which must be the subject of the formalities required under Articles 66 and 72 et seq. of the Data Protection Act .3. Objective(s) pursued by the processing (Purposes) and governance3.1. The purposes covered by the reference system3.1.1. The warehouses governed by this reference system are implemented in order to allow the reuse of the data they contain.

3.1.2. When they are implemented exclusively from the data of the warehouse by the authorized personnel of the data controller and for its exclusive use, the processing operations meeting the following purposes may be implemented within the framework of the declaration of conformity to the this standard:- the production of indicators and the strategic management of the activity, under the responsibility of the doctor responsible for medical information (medical information department - DIM) (e.g.: medico-economic analyzes of the course of care, assessment of the quality and relevance of care);

- improving the quality of medical information or optimizing coding as part of the information systems medicalization program (PMSI);

- the functioning of tools to help with medical diagnosis or treatment;

- carrying out feasibility studies (pre-screening).3.1.3. The data may also be reused for the purposes of research, study or evaluation in the field of health. These processing operations must be subject to the appropriate formalities: if they comply with a reference methodology, they can be implemented on the condition that their manager sends the Commission a declaration attesting to this compliance beforehand. Failing this, they will have to request a research authorization on the basis of article 66.III of the Data Protection Act.

3.1.4. The data contained in the processing carried out within the framework of this reference system may not be used either for the purpose of promoting the products mentioned in II of Article L. 5311-1 of the Public Health Code towards health professionals or establishments, nor for the purpose of excluding guarantees from insurance contracts, nor for modifying contributions or insurance premiums for an individual or a group of individuals presenting the same risk.3.2 . Warehouse

governance3.2.1. In order to verify compliance with the purposes pursued, the data controller implements governance for each warehouse that it sets up. The bodies set up for this purpose can be pooled if the data controller implements several warehouses.

3.2.2. A first body (steering committee or equivalent) determines the strategic and scientific orientations of the repository.

3.2.2.1. It is his responsibility to keep an exhaustive list of data from the warehouse and to justify their necessity, within the limits of the data listed in 5.2 of this reference system.

3.2.2.2. Within the framework of a structure endowed with an IMG, this governance must involve the latter, as well as a representative of the conference or of the medical commission of the establishment.

3.2.3. A second body (scientific and ethics committee, or equivalent) systematically issues a prior and reasoned opinion on project proposals requiring the reuse of data from the warehouse.

3.2.3.1. Only projects that have been reviewed by this body can use the warehouse. The notice must be communicated without delay to the project leader wishing to reuse the data from the warehouse.

3.2.3.2. A list of processing on which this committee has ruled is communicated periodically, at least once a year, to the data protection officer of the controller.

3.2.3.3. For the processing operations covered by point 3.1.3, the committee may choose, for certain files which relate to identical categories of data and recipients, to issue a single opinion. He can also choose not to decide systematically for internal research within the meaning of Article 65.2° of the Data Protection Act.

3.2.3.4. This second body includes in particular:- at least one person involved in health ethics;

- a person independent of the data controller (for example: non-employee);

- health professionals and medico-social professionals;

- researchers ;

- a representative of users or of a patient association.4. Legal basis(s) of processing

4.1. The standard only applies to health data warehouses whose constitution is based on the exercise of a public interest mission, within the meaning of Article 6-1-e of the GDPR. Thus, the warehouse must be necessary for the performance of a task in the public interest or in the exercise of official authority vested in the controller.

4.2. The nature of the public interest of the mission of the data controller must be distinguished from the requirement of public

interest imposed for the purposes of the processing implemented in the field of health, in accordance with Article 66 of Law no. ° 78-17 of January 6, 1978 amended.5. Personal data that may be included in the warehouse

5.1. Only personal data that is adequate, relevant and limited to what is necessary for the purposes of the processing may be collected and processed. As such, the data controller can only collect and process: - data which appear in the medical and administrative file or single computerized file of the person concerned and whose collection is justified by his care; and or

- data from research projects, studies and evaluations in the field of health previously carried out and whose retention period has not expired.

5.2. The data that can be processed includes:

5.2.1. Patient data:

5.2.1.1. Directly identifying and administrative data relating to patients which must be kept in a space separate from other data:

- surname, first names;

- sex, gender, civility;

- marital status ;

- day, month, date and place of birth;

- date, place and cause of death, if present in the medical file;

- telephone and electronic contact details and residence address;

- permanent patient identification number (PPI);

- care episode identification number (IEP);

- identification number in the directory of natural persons - national health identifier (NIR-INS).

5.2.1.2. Other categories of personal data, including sensitive data:- weight, height, reports (medical, CPR, etc.), examination results, results from the analysis of biological samples, medical imaging, data relating to adverse effects and events; requirements; medical and paramedical observations; data from medical devices or measuring devices and any component of the medical file;

- personal or family history, diseases or associated events;

- medico-administrative data from the local PMSI (1);

- genetic data strictly necessary to meet the objectives or purposes of the warehouse and having been interpreted prior to their

transfer to the warehouse, which cannot under any circumstances be used for the purposes of identification or re-identification of persons; they must have been collected as part of the medical care of the person concerned or a research project, provided that the person concerned has not objected to it prior to the carrying out of the examination, in accordance with the provisions of Articles L. 1130-5 of the Public Health Code and that it has been informed on this occasion of the possibility of reusing the results obtained for subsequent research purposes;

- sex life;

- data revealing ethnic origin;

- photography and/or video and/or voice recordings that do not allow the direct identification of the persons concerned (for example, with masking of the face, eyes, distinctive signs) and collected under conditions that comply with the applicable legal provisions image and voice rights;

- data relating to professional life (profession, employment history, unemployment, professional journeys and travel, occupational exposure, socio-professional INSEE category, etc.);

- level of education (eg: primary, secondary, higher);

- social security affiliation scheme, supplementary insurance (mutual insurance, private insurance);

- travel (eg: to the place of care or research: mode, duration, distances or journeys);

- consumption of tobacco, alcohol, drugs;

- lifestyle habits and behaviours, for example: dependency (alone, in an institution, autonomous, bedridden), assistance (housekeeper, family help), physical exercise (intensity, frequency, duration), diet and dietary behaviour, leisure;

- way of life (eg: urban, semi-urban, nomadic, sedentary), habitat (private house, building, floor, elevator, etc.);

- vital status and cause of death;

- quality of life scale or other information on the person's quality of life;

- exposure to known health risks (physical, chemical, biological and environmental, etc.).

5.2.2. Data relating to healthcare professionals - identification data: surname, first name, title;

- function, department and exercise unit;

- professional contact details (professional e-mail address and telephone number);

- ADELI number or RPP number (excluding the matricule number).

5.3. No data can be collected just to feed the warehouse. Thus, the deposit in the warehouse of data whose collection would not be scientifically justified by the health or medico-social care or by the realization of a project of research, study or specific evaluation is prohibited and provided for by protocol.

5.4. The use of each of these data for any reuse must be justified in the request submitted to the governance of the warehouse.

5.5. The directly identifying data mentioned in point 5.2.1.1 may only be collected in the warehouse for the following purposes:

- to contact patients again to suggest that they take part in studies or to inform them regularly of research projects not involving the human person, reusing data from the warehouse concerning them;
- recontact patients following the discovery of genetic characteristics that may be responsible for a condition justifying preventive or care measures for their benefit or for the benefit of their family, with the exception of cases in which the patient is opposed, in accordance with Article L. 1130-5 of the Public Health Code;
- recontact patients following additional discoveries related to the identification of risk factors and/or syndromic identification capable of modifying their management (therapeutic or follow-up);
- warn a person of a health risk to which he is exposed.

5.6. The directly identifying data mentioned in point 5.2.1.1 can only be used if the purposes of the processing justify it. For example, the day of birth can only be used if it is necessary to carry out research involving people under the age of two.

5.7. The relevance of the data included in the warehouse must be re-evaluated regularly by the governance of the warehouse, particularly with regard to the use made of it for the various projects carried out. Data no longer appearing necessary must be deleted.

5.8. In the event that directly identifying data, look-up tables, genetic data or location tracking data are contributed to the warehouse, these must be stored separately from the pseudonymised data, using the methods described in the requirements from SEC-LOG-4 to SEC-LOG-6.6. Access to information

6.1. The data controller of a health data warehouse must pay particular attention to the management of the access rights of persons authorized to access the data contained in the warehouse.

6.2. Access to and use of directly identifying data must be restricted to the purposes listed in point 5.5 and only to the persons responsible for carrying out the operations necessary to achieve these purposes.

6.3. The recipients of pseudonymised data strictly necessary for the achievement of the objectives of their research, study or evaluation projects validated by the governance of the warehouse, the internal research teams (e.g.: composed of employees of the controller) or external (e.g.: made up of partners of the controller) to the controller, authorized for this purpose.

6.4. The internal staff of the data controller authorized for this purpose may be the recipient of pseudonymised data strictly necessary for the accomplishment of their missions corresponding to the purposes of the warehouse.

6.5. When the data is subject to an anonymization process (2) within a project space of the warehouse, the resulting anonymous data may be published or transmitted to any recipient.7. Storage periods

7.1. The retention period of data from the health data warehouse must meet the requirements set out in Article 5.1.e of the GDPR.

7.2. The data mentioned in point 5.2.1.2 may be kept for a maximum of 20 years from their collection in the context of treatment or research. The data mentioned in point 5.2.1.1 must be deleted when the retention period for the data mentioned in point 5.2.1.2 has expired.

7.3. Beyond these durations, all data must be anonymized or destroyed.8. Information of persons8.1. Patient information: Individuals must be informed by the processing manager(s) that the data collected when they are processed are transferred to the warehouse.8.2. Information relating to the constitution of the warehouse for data from medical records

8.2.1. When setting up a warehouse, initial information relating to the setting up of a warehouse must be sent to the persons concerned.8.2.2. Collection of information from patients admitted or readmitted after the constitution of the warehouse

8.2.2.1. New patients as well as those undergoing follow-up are informed individually of the constitution of the warehouse (eg: by mail). The information medium(s) used include all the elements provided for in Article 13 of the GDPR.

8.2.2.2. The reuse of data as well as the procedures for exercising the rights of access and opposition must be particularly highlighted in the information note.8.2.3. Collection of information from patient files admitted prior to the establishment of the warehouse and no longer being followed

8.2.3.1. Patients who are no longer followed are informed individually of the constitution of the warehouse (eg: by mail). The information medium(s) used include all the elements provided for in Article 14 of the GDPR.

8.2.3.2. These information notices must include the data controller's personal data protection policy and be presented in a dedicated section.

8.2.3.3. The reuse of data as well as the procedures for exercising the rights of access and opposition must be the subject of specific highlighting in the information note.

8.2.3.4. The data controller may claim an exception to the obligation of individual information for the constitution of the warehouse, if he justifies in his record of processing activity that the provision of information would require disproportionate efforts, in accordance with the GDPR article 14.5.b.

8.2.3.5. In this regard, the following may in particular be invoked, in view of his situation: - the number of people concerned;

- the age of the data;

- the cost and time of providing the information (3). In most cases, the exception to the obligation to inform will only be justified for one category of data subjects. By way of example, this exception may apply to persons for whom the data controller has a medical file but who are no longer monitored within the establishment or center where prevention, diagnosis and care. The exception could not, however, be invoked in order not to inform the persons who come to consult after the implementation of the warehouse. The DPIA must detail precisely in what way the individual information of the persons concerned would constitute a disproportionate the guarantees implemented by the data controller in order to protect the rights and freedoms as well as the legitimate interests of the persons concerned. 8.2.3.6. In the event of recourse to the exception to the obligation of individual information, the data controller makes the information publicly available, in particular by: - distributing the information note relating to the constitution of the warehouse on its website, in a dedicated section accessible from the home page, supplemented by detailed information on each processing implemented using data from the warehouse;

- communicating about the warehouse on social networks, in the regional media, with patient associations;

- distributing a press release informing of the establishment of the warehouse.8.3. Information about integration into the research data warehouse

8.3.1. If the warehouse integrates research data, the data subjects must be informed individually of the reuse of the research data in order to constitute a warehouse in accordance with the provisions of Article 14 of the GDPR. In this case, recourse to the exception to individual information is possible, under the conditions mentioned in points 8.2.3.4 to 8.2.3.6.

8.3.2. Only data resulting from processing operations whose retention period has not expired may be integrated into the health data warehouse.8.4. Data subjects must also be informed of each re-use of data concerning them for research, study or evaluation purposes, except when the data controllers are unable to provide the information or it would require

disproportionate efforts.8.5. Information from professionals

8.5.1. Concerning the information of professionals working within the establishments of the data controller after the implementation of the warehouse: - the professionals whose data are placed in the warehouse must be informed individually and in writing of the information provided for by the GDPR Article 13;

- if the controller is the employer of the professionals, the information sheet may take the form of a letter or email attached to the payslip or the employment contract. The information should also be disseminated in the establishment's medical committee or conference, on the latter's intranet and by means of posters in the resting places of the personnel.

8.5.2. Concerning the information of professionals who do not or no longer practice within the establishments of the data controller during the implementation of the warehouse:- if the data controller is not the employer of the professionals whose data are collected in the warehouse, he must provide individual information in writing for each of them, including the information provided for in article 14 of the GDPR.9. Rights of persons

9.1. In addition to individual information, the data controller disseminates general information via a public information campaign (e.g.: on social networks, within the establishment and by publishing inserts in the regional press), prior to the establishment of the warehouse in order to ensure that a reasonable period of time (e.g.: one month) elapses between the notification of patients and the start of the processing of their data, so that they can exercise their right of opposition.

9.2. The persons concerned (professionals and patients) whose data appear in the warehouse have the following rights, which they exercise under the conditions provided for by the GDPR:

- permission to access ;
- right of rectification;
- right to erasure;
- right to restriction of processing;
- right of opposition.

9.3. The right of opposition of healthcare professionals is exercised subject to the conditions for exercising this right pursuant to the provisions of Article 21 of the GDPR.

9.4. Patients' right to object must be exercised by any means. In the context of this standard, the data controller must allow people to oppose the processing as soon as they are informed (e.g., by sending a paper document that can be filled in

immediately or by a box to be ticked by the professional, attesting to the exercise of the right of opposition).

9.5. These rights are exercised with any person specifically trained and authorized for this purpose by the data controller, and whose contact details are communicated to the persons concerned. Where appropriate, this may be the data protection officer of the controller.

9.6. The data controller cannot rely on the provisions of Article 11 of the GDPR to limit the exercise of the rights of data subjects. Indeed, when the procedures for setting up the warehouse do not involve the retention of identifying data or means of correspondence with the identity of the persons, the data controller remains in a position to respond to the requests of the persons if they provide additional information allowing the re-identification of their data in the warehouse. To do this, he will have to set up a mechanism guaranteeing the correspondence between the data transmitted by the person exercising his rights and the data in the warehouse concerning him. The data controller will specify in the information notice the information that must be sent to him for the exercise of the rights.

9.7. In any event, the mechanisms for feeding the warehouse must enable individuals to exercise their right of opposition in a sustainable manner and may constitute a means of re-identifying the data of individuals exercising their other rights.10. Security

10.1. In general, the data controller, as well as the subcontractors he uses, must take all necessary precautions with regard to the risks presented by his processing to preserve the security of personal data and, in particular, at the time of their collection, during their transmission and their conservation, to prevent that they are deformed, damaged or that unauthorized third parties have access to them.

10.2. In particular, in the specific context of this standard, the data controller must adopt the following technical and organizational measures:

Requirement Numbers

Security requirements

Network partitioning

SEC-RES-1

The communication network on which the warehouse is hosted or made accessible must be the subject of partitioning measures separating the network flows specific to the warehouse from the rest of the information system flows.

SEC-RES-2

Filtering measures must also restrict the transmission and reception of these network flows to machines specifically identified and authorized for the operation of the warehouse.

SEC-RES-3

All data transmissions from or to the warehouse, as well as all internal data flows to the warehouse, must be subject to encryption measures in accordance with appendix B1 of the general security reference system (RGS) in order to guarantee confidentiality.

Logical and cryptographic partitioning

SEC-LOG-1

The data controller must collect and store the personal data forming part of the warehouse on systems and databases separate from those providing patient care.

SEC-LOG-2

Personal data must be encrypted at rest by algorithms and key sizes compliant with Annex B1 of the RGS. An operational key management procedure must be formalized.

SEC-LOG-3

Backups of this data must also be encrypted in accordance with Annex B1 of the RGS.

SEC-LOG-4

In the event that directly identifying data or correspondence tables are stored in the warehouse, these must be logically separated from the pseudonymised data by cryptographic means. For example, patient administrative data and mapping tables should be encrypted with different keys than those used to encrypt warehouse health data.

SEC-LOG-5

Access to the two categories of separate data defined in requirement SEC-LOG-4 must be made via different user accounts, or via a single user account that must choose one of the different authorization profiles assigned to it when connecting. .

SEC-LOG-6

In the event that genetic or location tracking data is collected, this must be encrypted separately with a specific key from other data in the warehouse.

The key for decrypting genetic data or tracking location must only be mobilized by the authorization profiles responsible for feeding the warehouse and exporting data to a workspace.

Constitution and supply of the warehouse

SEC-ALI-1

The data collection circuits must be subject to appropriate security measures, in particular the regular purging of transit directories and strict access control to the data collected.

SEC-ALI-2

In the case where the warehouse is fed manually via input software that also authorizes the consultation of the data entered, access to this software must be secured via strong authentication in accordance with the SEC-AUT-1 requirement.

Pseudonymization of data

SEC-PSE-1

No internal number, such as a patient file number, can be directly reused as an identifier within the warehouse. Only a unique pseudonymous identifier can be used, allowing, if necessary, the correspondence between the pseudonymised data stored in the warehouse and directly identifying data. This identifier must be dedicated to a single warehouse. It must be generated by a cryptographic hash function resistant to brute force attacks or a cryptographically secure pseudo-random number generator. The data must be pseudonymised prior to their integration into the warehouse.

SEC-PSE-2

In the event that the warehouse integrates existing data sets that have already been pseudonymized, a new unique pseudonymous number respecting the conditions of requirement SEC-PSE-1 must be generated when feeding the warehouse.

SEC-PSE-3

In the event that data relating to healthcare professionals are collected, the data controller must pseudonymize this data.

SEC-PSE-4

Unstructured documents added to the warehouse must be deleted or masked before they are checked into the warehouse. This step consists of deleting the identifying data of patients and healthcare professionals or replacing them with generic terms or fictitious data. For example, the NIR, birth name, first name, postal code, city or telephone number will be replaced by generic terms such as NIR , NAME_OF_BIRTH , FIRST NAME , CODE_POSTAL , CITY or TEL .

This requirement applies in particular to office documents and printed facsimiles (such as medical reports and prescriptions), document scans, medical imaging and any form of biomedical analysis results. It also concerns free-entry comments contained in the databases.

The masking or deletion operation must apply to the visible content of the documents (such as mail headers and image cartridges), to the metadata contained in these files (such as the name of the imaging operator) and to the attributes files (such as their name).

Physical access to data

SEC-PHY-1

Physical access to servers and premises hosting the warehouse infrastructure must be secured by adequate protective measures. In particular, physical access control measures must be put in place.

Management of authorizations and logical access to data

SEC-HAB-1

Different authorization profiles must be provided in order to manage access to data as needed and exclusively.

SEC-HAB-2

A granularity of data access must be provided for each authorization profile, while respecting the SEC-LOG-5 requirement relating to the partitioning of correspondence tables and directly identifying data. For example, a profile may contain either access only to aggregated data and/or access to pseudonymised data, or access only to directly identifying data.

SEC-HAB-3

Persons authorized to access personal data must be individually authorized according to a procedure involving validation by:

- one of the bodies ensuring the governance of the warehouse; Where
- by their line manager in the case of system and network engineers and administrators.

SEC-HAB-4

Privileged access with extended rights, in particular for administration and maintenance, must be reserved for a restricted team and be limited to what is strictly necessary.

SEC-HAB-5

A manual or automatic review of authorizations must be carried out regularly and at least annually, as well as at the end of

each research project using data from the warehouse.

SEC-HAB-6

Access permissions must be withdrawn as soon as authorizations are withdrawn, for example after the departure of an employee or a modification of his assignments.

Authentication for consultation and administration of the warehouse

SEC-AUT-1

Access to personal data must be subject to strong authentication involving at least two distinct authentication factors. If one of these factors is a password, it must comply with the recommendations of the CNIL in terms of passwords (deliberation n° 2017-012 of January 19, 2017 on the date of writing of this reference document).

SEC-AUT-2

This strong authentication must be implemented for both internal and external access to the warehouse.

SEC-AUT-3

All data transmissions from or to the warehouse, as well as all internal flows to the warehouse, carried out automatically without user action, must be carried out by servers mutually authenticated by certificate or equivalent authentication device (4 ).

Workspace

SEC-ESP-1

Warehouse data should be manipulated by researchers only in workspaces internal to the Warehouse and specific to each research project, sealed with the Warehouse database and sealed from each other. Exchange capabilities between workspaces are nevertheless possible for the sharing of data that will have undergone the anonymization process detailed in requirement SEC-EXP-1.

SEC-ESP-2

Datasets imported into a workspace specific to a research project should be minimized and limited to only the data necessary for the project. A unique pseudonym number specific to each workspace must be generated under the same conditions as in requirement SEC-PSE-1.

SEC-ESP-3

In case of cohort follow-up, the same unique pseudonymous number can be reused in several workspaces.

Exporting data out of the warehouse and out of workspaces

SEC-EXP-1

With the exception of data relating to the SEC-REI-1 to SEC-REI-3 re-identification procedures, only anonymous data sets may be exported from the warehouse or from a space of work. The anonymization process should produce a dataset that complies with the three criteria defined by the G29 Opinion No 05/2014 or any subsequent EDPS Opinion on anonymization. This compliance must be documented and demonstrable. Otherwise, if these three criteria cannot be met, a study of the risks of re-identification must be carried out and documented.

SEC-EXP-2

Data exports must be subject to the prior validation of a manager in order to endorse the principle, in particular with regard to the SEC-EXP-1 requirement.

SEC-EXP-3

Exports must be subject to automatic or manual monitoring by a specialized operator in order to verify their anonymity. In the case where this monitoring is automatic, any export identified as non-compliant must be the subject of an alert escalation and quarantine in the warehouse, then must be checked manually by a specifically trained manager and specifically empowered.

SEC-EXP-4

The systems set up in the warehouse relating to the production of indicators and the strategic management of the activity of a health establishment must only allow anonymous restitution, including taking into account the filtering and selection functionalities of these refunds. This feedback process must comply with the three criteria set out in G29 Opinion No 05/2014 or any subsequent EDPS Opinion on anonymisation. This compliance must be documented. Otherwise, if these three criteria cannot be met, a study of the risks of re-identification must be carried out and documented.

SEC-EXP-5

Returns mentioned in SEC-EXP-4 must be exported in accordance with SEC-EXP-2 and SEC-EXP-3.

User awareness and workstation security

SEC-SEN-1

Each person authorized to access the warehouse must be trained in the respect of medical secrecy and regularly made aware

of the risks and obligations inherent in the processing of health data.

SEC-SEN-2

Each person authorized to access the warehouse must sign a confidentiality charter specifying in particular their obligations with regard to the protection of personal health data and with regard to the security measures put in place in the warehouse, as well as the sanctions relating to non-compliance with these obligations.

SEC-SEN-3

The workstations of persons authorized to access the warehouse, including external users accessing only the workspaces, must be subject to specific security measures, for example by setting up nominative accounts, adequate authentication, automatic session locking, encryption of storage media and filtering measures. In the event that the workstations are not under the control of the data controller, the security measures to be put in place on the workstations must be regulated by means of an agreement between the parties concerned.

Logging

SEC-DAY-1

Warehouse workspace user actions should be subject to logging measures. In particular, the connections to the warehouse (identifiers, date and time), the requests and operations carried out must be traced.

SEC-DAY-2

Access by engineers and system and network administrators must be carried out through a specific system ensuring strong authentication as well as detailed traceability of the accesses and actions carried out. For example, an administration bastion can be used to control access and log sessions.

SEC -DAY-3

Traces must be checked regularly and at least every two months, as well as at the end of each authorization period linked to a research project. This control must be carried out by:

- a solution carrying out automatic monitoring with feedback of alerts processed manually by an authorized operator;
- or by a semi-automatic control via the execution of programs allowing a selection of abnormal traces, followed by a manual re-reading by an authorized operator.

SEC-DAY-4

The logging traces defined in requirements SEC-JOU-1 and SEC-JOU-2 must be kept for a period of between 6 months and one year.

Re-identification procedures

SEC-REI-1

The data controller implements a secure operational procedure to ensure the exercise of the rights of individuals and, where applicable, the lifting of the pseudonym and the proper re-identification of the individuals concerned. This procedure makes it possible, from the additional information necessary for the unique identification of the person, to find or calculate the corresponding unique pseudonymous number (5), then to select from the warehouse, with this unique unique pseudonymous number, the data corresponding to the applicant and to carry out the operations necessary for the proper exercise of his rights (deletion of data or extraction for transmission).

SEC-REI-2

If necessary, and in the event of a duly justified and documented need, the data controller implements a secure operational procedure in order to recontact patients to offer them participation in research. This procedure makes it possible, from a list of medical criteria, to select the unique pseudonymous identifiers corresponding to the patients concerned, then, by mobilizing the correspondence table(s) of the warehouse with these pseudonyms alone, to select the identifying data corresponding to these patients in order to export them for this sole purpose.

SEC-REI-3

If necessary, the data controller implements a secure operational procedure to re-identify patients in the event of a medical emergency. This procedure makes it possible, by mobilizing the correspondence table(s) of the warehouse, to select the identifying data of the patients concerned from their unique pseudonymous number, and to export them for this sole purpose.

SEC-REI-4

The authorizations and access relating to the re-identification procedures defined in requirements SEC-EXC-1 to SEC-EXC-3 must be reserved for a restricted team and be limited to what is strictly necessary. The members of this small team must be trained specifically in this procedure.

SEC-REI-5

The data controller implements the appropriate measures to manage the risks inherent in these re-identification procedures

and in particular to guarantee that they can only be used in the event of a request actually emanating from a data subject or a duly authorized health professional.

Management of security incidents and personal data breaches

SEC-INC-1

The data controller provides a procedure for managing and dealing with security incidents and personal data breaches, specifying the roles and responsibilities and the actions to be taken in the event of the occurrence of such incidents.

SEC-INC-2

Any security incident, of malicious origin or not and occurring intentionally or not, having the consequence, even temporary, of compromising the integrity, confidentiality or availability of personal data, must be the subject of internal documentation in a violation register.

SEC-INC-3

When such an incident is likely to create a risk for the rights and freedoms of data subjects, the resulting data breach must be notified to the Commission under the conditions provided for in Article 33 of the GDPR.

SEC-INC-4

In the event that the breach is likely to create a high risk for the rights and freedoms of a natural person, the controller is required to communicate the data breach to the persons concerned as soon as possible, in accordance with the article 34 of the GDPR.

10.3. These measures are not exhaustive and must be supplemented by any provisions deemed necessary when carrying out the data protection impact analysis carried out as detailed in section 13 of these guidelines.

10.4. Articles 5.1.f and 32 of the GDPR require the updating of security measures with regard to the regular reassessment of the risks so that they comply with the state of the art.11. Subcontractors

11.1. In the event of recourse to a service provider, the service must be carried out under the conditions provided for in Article 28 of the GDPR. A subcontracting contract must be concluded between the service provider and the data controller. This contract must in particular specify the distribution of responsibilities relating to security measures and the management of data breaches between the various actors.

11.2. The service provider must, in its capacity as processor, keep a register of processing activities under the conditions of

article 30.2 of the GDPR.

11.3. Only warehouses using a subcontractor coming exclusively under the jurisdictions of the European Union or of a country considered adequate within the meaning of Article 45 of the GDPR comply with this standard.

11.4. In the event that the data controller uses the services of a subcontractor for the hosting, storage or retention of health data, this subcontractor must be an approved or certified health data host according to the provisions of CSP.12. Transfer of data outside the European Union

12.1. Any remote access to data from outside Europe is considered a transfer.

12.2. The establishment and operation of a warehouse cannot result in the transfer of personal data, directly or indirectly identifying, outside the European Union or to a country that does not have an adequate level of protection. 13. Data Protection Impact Analysis

13.1. The data controller must carry out and document a data protection impact analysis.

13.2. To this end, the data controller may refer to:- the principles contained in this reference system;

- the methodological tools offered by the Commission on its website.13.3. If necessary, the data controller may draw up a procedure relating to the DPIA allowing the involvement of the relevant actors and persons for its implementation, in particular the data protection officer (DPD/DPO) who must be consulted.

13.4. The DPIA will have to be reviewed and updated regularly, in particular if significant changes are planned in the processing or if the risks for the data subjects have evolved (such as the pursuit of an additional purpose, the use of a new processor , new data collected, data leak allowing re-identification, etc.).

(1) The local PMSI corresponds to the PMSI of the establishment, except in the case of a GHT in which the lead establishment could have the PMSI of the GHT.

(2) In accordance with the G29 criteria or any future advice from the EDPS.

(3) G29, Guidelines on transparency within the meaning of Regulation (EU) 2016/679, adopted on April 11, 2018.

(4) A password alone is not considered an authentication device equivalent to a certificate.

(5) Including by mobilizing salts, hash keys or correspondence tablesThe President,

M. L. Denis