Deliberation 2021-118 of October 7, 2021Commission Nationale de l'Informatique et des LibertésLegal status: In force Date of publication on Légifrance: Tuesday October 26, 2021NOR: CNIL2131763XDeliberation no. of personal data implemented for the purpose of creating data warehouses in the field of healthThe National Commission for Data Processing and Liberties,Having regard to Regulation (EU) 2016/679 of the European Parliament and April 27, 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (general data protection regulation), in particular its article 58; 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; After having heard the report of Mrs Valérie PEUGEOT, Commissioner, and the observations of Mr Benjamin TOUZANNE, Government Commissioner, Adopts a reference system relating to the processing of personal data implemented for the purpose of creating data warehouses in the field of health.The PresidentMarie-Laure DENISREFERENTIAL RELATING TO THE PROCESSING OF PERSONAL DATA IMPLEMENTED FOR THE PURPOSES OF CREATING DATA WAREHOUSES IN THE FIELD OF HEALTH[You can consult the full text with its images from the extract from the authenticated electronic Official Journal.] 1. Who is this reference intended for? This repository 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 Such processing is hereinafter referred to as data storage. health data .1.2 The repository 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 repository: 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 diagnosis, the administration of care or treatment, or the management of healthcare and implemented by healthcare professionals and healthcare systems or services (e.g. electronic medical records); data processing s of a personal nature 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 Health Code public.2. Scope of the framework2.1 This framework 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 to the Commission compliance with this standard 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 compliance 2.3 Any processing of personal data aimed to implement a health data warehouse that does not comply with all the

requirements defined by this standard must be the subject of a specific authorization request, in accordance with the provisions of article 66 III of the law computing and Freedom . To request authorization: Declare a file - health authorization request section - 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 repository also constitute an aid to carrying out the analysis impact on data protection (AIPD) that the processing managers concerned must carry out (see point 13 of this reference document). consent in accordance with Article 7 of the GDPR on the basis of Article 9.2.a of the GDPR of each of the persons concerned are not subject to prior authorization by the Commission or to a declaration of compliance with this standard. The Commission recalls, however, that the principles and measures set out in these guidelines can apply 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, constitute separate processing operations which must be subject to the necessary formalities under Articles 66 and 72 and following of the Data Protection Act .3. Objective(s) pursued by the processing (Purposes) and governance 3.1 The purposes covered by the repository 3.1.1 The warehouses governed by this repository 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 compliance with 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 care pathway, assessment of the quality and relevance of care); improving the quality of medical information or optimizing coding as part of the medicalization of information systems (PMSI); the operation of tools to assist in medical diagnosis or care; the performance of feasibility studies (pre-screening). 3.1.3 The data can also be reused for the purposes of research, study or evaluation in the field of health. This processing 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 must request a research authorization on the basis of Article 66. III of the Data Protection Act. to promote the products mentioned in II of Article L. 5311-1 of the Public Health Code towards healthcare professionals or healthcare establishments, nor for the purpose of excluding guarantees from insurance contracts, or modification of contributions or insurance premiums for an individual or a group of individuals presenting the same risk.3.2 Governance of the warehouse3.2.1 In order to verify compliance with the purposes pursued, the implements governance for each warehouse it constitutes. 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 warehouse.3.2.2.1 It is its responsibility to keep an exhaustive list of the data of the warehouse and to justify their need, within the limit of the data listed in 5.2 of this reference system.3.2.2.2 Within the framework of a structure equipped with a DIM, this governance must involve the latter, as well as a representative of the conference or of the establishment's medical committee. project proposals requiring the reuse of data from the warehouse. 3.2.3.1 Only projects that have been examined by this body can use the warehouse. The opinion must be communicated without delay to the project leader wishing to reuse the data from the warehouse. 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 may also choose not to systematically decide on 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 ethics in health; a person independent of the data controller (for example: non-salaried); health and medico-social professionals; researchers; a representative of users or of a patient association4. Legal basis(s) of the processing 4.1 The standard only applies to health data warehouses whose constitution is based on the exercise of a mission of public interest, within the meaning of Article 6 -1-e 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 the law n°78-17 of January 6, 1978 modified.5. Personal data that may be included in the warehouse5.1 Only personal data that is adequate, relevant and limited to what is necessary in relation to the purposes of the processing may be collected and processed. As such, the data controller can only collect and process: data which appears 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 Data that can be processed includes:5.2.1 Data relating to patients :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, title; 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 residential address; permanent patient identification number (IPP); care episode identification number (IEP); identification number at 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.), result s examinations, 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, illnesses or associated events; medico-administrative data from the local PMSI; genetic data strictly necessary to meet the objectives or purposes of the warehouse and having been interpreted prior to their deposit in 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; sexual life; data revealing ethnic origin; photograph 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 provisions on the right to image and right to voice; data relating to professional life (profession, employment history, unemployment, professional journeys and travel, occupational exposure, category socio-professional INSEE, etc.); level of training (p. ex. primary, secondary, higher); social security affiliation scheme, supplementary insurance (mutual insurance, private insurance); travel (e.g.: to the place of care or research: mode, duration, distances or trips );consumption of tobacco, alcohol, drugs;life habits and behaviors, for example: addiction (alone, in an institution, autonomous, bedridden), assistance (housekeeper, family), physical exercise (intensity, frequency, duration), diet and dietary behaviour, leisure; way of life (e.g.: urban, semi-urban, nomadic, sedentary), habitat (private house, building, floor, elevator, etc.); vital status and cause of death; scale quality of life 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: name , first name, title; function, department and former unit ercice; professional contact details (professional e-mail address and telephone number); ADELI number or RPP number (excluding the registration number). 5.3 No data may be collected solely for the purpose of supplying 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 a 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 cannot be combined in the warehouse only 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; to contact patients again following discoveries of genetic characteristics that may be responsible for a condition justifying preventive or care measures for their benefit or for the benefit of their f amille, with the exception of cases in which the patient has objected, in accordance with Article L. 1130-5 of the Public Health Code; recontacting patients following additional discoveries related to the identification of syndromic risk and/or identification factors capable of modifying their management (therapeutic or follow-up); warning a person of a health risk to which they are exposed. 5.6 The directly identifying data mentioned in point 5.2.1.1 do not 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 for the realization of a research involving people aged less than two years.5.7 The relevance of the data included in the warehouse must be reviewed. -regularly evaluated by the governance of the warehouse, in particular with regard to the use made of it for the various projects carried out. Data no longer appearing to be necessary should be deleted. pseudonymised data, using the methods described in security requirements SEC-LOG-4 through SEC-LOG-6.6. Access to information6.1 The 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 and use of directly identifying data must be restricted to the purposes listed in point 5.5 and only to persons responsible for carrying out the operations necessary to achieve these purposes. research, study or evaluation validated by the governance of the warehouse, the internal research teams (e.g.: made up of employees of the data controller) or external (e.g.: made up of partners from the controller) to the controller, authorized for this purpose. 6.4 The internal staff of the controller authorized for this purpose may be recipients of e pseudonymized 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

within a project space of the warehouse, the anonymous data resulting may be published or transmitted to any recipient.7. Retention periods7.1 The retention period for data in 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 at from their collection in the context of care 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 periods, all data must be anonymized or destroyed.8. Information of persons8.1 Information of patients:People must be informed by the data controller(s) that the data collected during their treatment are placed in the warehouse.8.2 Information relating to the constitution of the warehouse for data from medical records8.2.1 When setting up a warehouse, initial information relating to the constitution of a warehouse must be transmitted to the persons concerned.8.2.2 Collection of information from patients admitted or readmitted after the constitution of the warehouse8.2.2.1 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 includes 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 constitution of the warehouse and no longer being monitored8.2.3.1 Patients who are no longer being monitored are informed individually of the constitution of the warehouse (eg by post). The information medium(s) used includes all the elements provided for in Article 14 of the GDPR.8.2.3.2 These information notices must include the personal data protection policy of the data controller and be presented in a dedicated section.8.2.2.3.The reuse of data as well as the procedures for exercising the rights of access and opposition must be specifically highlighted 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 Article 14.5.b of the GDPR.8.2.3.5 In this respect, the following may be invoked, in view of his situation: the number of persons concerned; the age of the data; the cost and time of issuing the information. the most Apart from the cases, the exception to the obligation to inform will only be justified for a 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 to provide individual information, the data controller makes the information publicly available, in particular by: distributing the information note relating to the creation of the warehouse on its website, in a dedicated section accessible from the home page, supplemented by detailed information on each processing operation implementation based on data from the warehouse; communicating about the warehouse on social networks, in regional media, with ass 8.3.1 If the warehouse integrates data from research research, data subjects must be informed individually of the reuse of data resulting from research 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 for which the 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 controller are unable to provide the information or that it would require disproportionate effort. the warehouse: Professionals whose data is placed in the warehouse must be informed individually and in writing of the information provided for in Article 13 of the GDPR. If the responsible able of treatment is the employer of the professionals, the information sheet may take the form of a letter or an 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 using posters in the staff rest areas.8.5.2 Concerning the information of professionals n not or no longer practicing 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 is collected in the warehouse, he must provide individual information in writing to each of them, including the information provided for in Article 14 of the GDPR.9. Rights of individuals9.1 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 through the publication 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 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: right of access; right of rectification; right to erasure; right to limitation of processing; right of opposition. 9.3 The

right of opposition of health professionals is exercised subject to the conditions of exercise of this right in application ion of the provisions of article 21 of the GDPR.9.4 The right of opposition of patients must be able to be exercised by any means. In the context of this Referential, 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 applicable, this may be the data protection officer of the controller. 9.6 The 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 must put in place 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 transmitted to him for the exercise of the rights. their right to object and may constitute a means of re-identifying the data of persons exercising their other rights.10. Security10.1 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. 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 subject to partitioning measures separating network flows specific to the warehouse from the rest information system flows.SEC-RES-2Filtering measures must also restrict the issuance and r receipt of these network flows to machines specifically identified and authorized for the operation of the warehouse.SEC-RES-3All data transmissions from or to the warehouse, as well as all data flows internal to the warehouse, must the subject of encryption measures in accordance with appendix B1 of the general security reference system (RGS) in order to guarantee its confidentiality.Logical and cryptographic partitioningSEC-LOG-1The data controller must collect and store personal data 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 in accordance with Annex B1 of

the RGS. An operational key management procedure must be formalized.SEC-LOG-3Backups of this data must also be encrypted in accordance with appendix B1 of the RGS.SEC-LOG-4In the event that data directly identifiers 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 separate data categories defined in The SEC-LOG-4 requirement must be carried out via different user accounts, or via a single user account that must choose, when connecting, one of the different authorization profiles assigned to it.SEC-LOG-6In the event that genetic data or location tracking is collected, these 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 populating the warehouse and exporting data to a workspace. warehouseSEC-ALI-1The 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-2In the event that the warehouse is fed manually via data entry software which 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 dataSEC-PSE-1No 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. Data must be pseudonymized 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 the SEC-PSE- 1 must be generated when feeding the warehouse.SEC-PSE-3In the event that data relating to healthcare professionals is collected, the data controller must pseudonymize this data.SEC-PSE-4Unstructured documents added to the warehouse must be deleted or masked before being integrated 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 the headers of the letters and the title blocks of the images), to the metadata contained in these files (such as the name of the imaging operator) and file attributes (such as their name). Physical access to dataSEC-PHY-1Physical access to servers and premises hosting 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 dataSEC-HAB-1Different authorization profiles must be planned in order to manage access to data as needed and in a exclusive.SEC-HAB-2A 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-3Persons 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; or by their line manager in the case of system and network engineers and administrators.SEC-HAB-4Privileged 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-5A 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-6Access permissions must be withdrawn as soon as the authorizations are withdrawn, for example after the departure of an employee or a modification of their missions.Authentication for the consultation and administration of the warehouseSEC-AUT-1Access to personal data must be subject to a 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-2This strong authentication must be implemented for both internal and external access to the warehouse.SEC-AUT-3All data transmissions from or to the warehouse, as well as all internal flows to the warehouse. warehouse, performed automatically without action from a user, must be performed by servers mutually authenticated by certificate or equivalent authentication device. 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 must be minimized and limited to only the data necessary for the project. A unique pseudonymous number specific to each workspace must be generated under the same conditions as in requirement SEC-PSE-1. SEC-ESP-3In 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 workspacesSEC-EXP-1Except data relating to re-identification procedures SEC-REI-1 to SEC-REI-3, only anonymous data sets can be exported out of the warehouse or a workspace. The anonymisation process must produce a dataset that complies with the three criteria defined by the G29 Opinion No 05/2014 or any subsequent EDPS Opinion on anonymisation. This compliance must be documented and demonstrable. Failing this, if these three criteria cannot be met, a study of the risks of re-identification must be carried out and documented.SEC-EXP-2Data exports must be subject to prior validation by a manager in order to endorse principle, particularly with regard to requirement SEC-EXP-1. SEC-EXP-3Exports 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 authorized.SEC-EXP-4The systems put in place 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 functionalities for filtering and selecting these restitutions. This restitution process must comply with the three criteria defined by the G29 opinion n° 05/2014 or any subsequent opinion of the EDPS 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-5The returns mentioned in requirement SEC-EXP-4 must be exported in accordance with the requirements SEC- EXP-2 and SEC-EXP-3. Awareness of users and security of workstationsSEC-SEN-1Each person authorized to access the warehouse must be trained in respect of medical secrecy and regularly made aware of the risks and obligations inherent in the processing of health data.SEC-SEN-2Each person authorized to access the warehouse must sign a confidentiality charter specifying in particular his 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 penalties relating to the non-compliance with these obligations.SEC-SEN-3The 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 locking of

sessions, 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.JournalisationSEC-JOU- 1User actions of warehouse workspaces 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-JOU-2Access by engineers and system and network administrators must be carried out through a specific system ensuring authentication as well as the detailed traceability of the accesses and actions carried out. For example, an administration bastion can be used to control access and record sessions. a research project. This control must be carried out by: a solution carrying out automatic monitoring with a feedback of alerts processed manually by an authorized operator; or by a semi-automatic control via execution of programs allowing a selection of abnormal traces, followed by manual re-reading by an authorized operator.SEC-JOU-4The 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 proceduresSEC-REI- 1The 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 correct 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, 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 its rights (deletion of data or extraction for transmission). SEC-REI-2 Where appropriate, and in the event of duly justified and documented necessity, 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-3Where applicable, 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-4Authorizations and access relating to the re-identification procedures defined in requirements SEC-EXC-1 to SEC-EXC-3 must be reserved for a small team and be limited to what is strictly necessary. The members of this restricted team must be trained specifically in this

procedure.SEC-REI-5The data controller implements the appropriate measures to manage the risks inherent in these re-identification procedures and in particular to guarantee that they cannot be used only in the case of a request actually coming from a data subject or a duly authorized healthcare professional.Management of security incidents and personal data breachesSEC-INC-1The data controller provides a and processing of 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-2Any security incident, whether malicious in origin or not and occurring intentionally or unintentionally, having the consequence, even temporarily, of compromising the integrity, confidentiality or availability of donation personal data, must be documented internally in a breach register.SEC-INC-3 When such an incident is likely to create a risk for the rights and freedoms of the persons concerned, the breach resulting data must be notified to the Commission under the conditions provided for in Article 33 of the GDPR.SEC-INC-4In the event that the violation is likely to create a high risk for the rights and freedoms of a person physical, the data controller is required to communicate the data breach to the persons concerned as soon as possible, in accordance with Article 34 of the GDPR.10.3 These measures are not exhaustive and must be supplemented by any provisions that have been deemed necessary when performing the data protection impact assessment conducted as detailed in section 13 of this framework.10.4 Articles 5.1.f and 32 of the GDPR require updating our security measures with regard to the regular reassessment of the risks so that they comply with the state of the art.11. Subcontractors11.1 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 subcontractor, keep a register of processing activities under 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 Union12.1 Any remote access to data from outside European territory is considered to be 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 destined for a country that does not have an

adequate level of protection. an impact analysis on data protection.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 Where applicable, the data controller may draw up a procedure relating to the DPIA allowing the involvement of the actors and persons relevant to its implementation, in particular the data protection officer. eds (DPD/DPO) who should be consulted. an additional purpose, the use of a new subcontractor, new data collected, a data leak allowing re-identification, etc.).