Deliberation 2018-295 of July 19, 2018 National Commission for Computing and Liberties Nature of the deliberation: Authorization Legal status: In force Date of publication on Légifrance: Tuesday October 23, 2018 Deliberation No. 2018-295 of July 19, 2018 authorizing the Center Hospitalier Universitaire de Nantes to implement automated processing of personal data for the purpose of a health data warehouse, called EHOP. (Request for authorization no. 2129203) The National Commission for Computing and Liberties, Seizure by the Center Hospitalier Universitaire de Nantes of a request for authorization concerning the automated processing of personal data for the purpose of storing health data; Having regard to Convention No. 108 of the Council of Europe for the protection of individuals with regard to automatic processing of personal data; 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, and repealing Directive 95/46/EC (general data protection regulation); Law No. 78-17 of January 6, 1978 as amended relating to data processing, files and freedoms, in particular Articles 8-II-8° and 54; Considering Decree No. 2005-1309 of October 20, 2005 as amended taken for the application of Law No. 7 8-17 of January 6, 1978 relating to data processing, files and freedoms; Considering the file and its supplements; On the proposal of Mrs Valérie PEUGEOT, commissioner, and after having heard the observations of Mrs Nacima BELKACEM, commissioner of the Government ,Formulates the following observations:Responsible for processingThe Center Hospitalier Universitaire de Nantes (hereinafter, the CHU of Nantes) On the legal basis and the purposeThe CHU of Nantes wishes to have, like other health establishments, a common information system, in the form of a health data warehouse, referred to as the EHOP warehouse. The legal basis for processing is the exercise of a public interest mission, within the meaning of Article 6-1 -e of the General Data Protection Regulation (hereinafter GDPR). The purpose of the processing envisaged is to constitute a warehouse of personal data including in particular health data. The latter aims to allow the subsequent performance, in the field of research, of the following activities: counting, feasibility of clinical trials; (activity requiring the full identity of patients because it aims to recontact them for a proposal to participate in a clinical trial); carrying out non-interventional/retrospective observational studies; epidemiology; population research; medico-economic studies; identification of clusters, cohorts; With regard to non-research purposes, the EHOP repository aims to enable the following activities: support for medical decision-making in the context of personalized medicine; control of vigilance and risks; optimization of the organization of care and strategic, medical and economic management; evaluation of activity, practices, studies in public health; for the Department of Medical Information: financial optimization of coding, evaluation, research;

technical validations. The Commission notes that specific governance is planned for the warehouse. Thus, each protocol will be reviewed by the data clinic evaluation committee, which will assess the scientific and ethical relevance of the projects. The Commission considers that the purpose of the processing is determined, explicit and legitimate, in accordance with the provisions of Article 5-1-b of the GDPR. It considers that it is necessary to apply the provisions of article 8-II 8° and 54 of the law of January 6, 1978 as amended, which make processing involving data relating to health and justified, as in this case, by the public interest. evaluation in the field of health and the processing of health data justified by the public interest are distinct processing operations which will have to be the subject of specific formalities under Chapter IX of the Data Protection Act. On the data processed The data in the warehouse relate to patients cared for by the Nantes University Hospital, including patients cared for before the constitution of the warehouse, as well as to healthcare professionals. Data relating to patients :Data relating to patients, taken from the local information systems medicalization program (PMSI), medical and nursing records and administrative records, are as follows:Identification data:maiden name;date of birth ;IPP number;telephone: it will be technically possible to deactivate the collection of this information. However, this is essential to recontact patients in the context of study screening, as well as to inform them and ask them not to object to the use of their data in a study; postal address and contact details of the study. ci (latitude and longitude) will be post-processed in the warehouse; this functionality is not currently activated in the application architecture planned at the Nantes University Hospital but will eventually allow screening to be carried out when a study includes a criterion for recruiting patients in a geographical area; e-mail address; date of death, civility; country and postal code of birth; health data from the computerized patient file and the treatment software; where applicable, genetic and genomic data from previous research unrelated to treatment. Patient files filed confidentially or hyper confidentiality, including in particular the files of people detained and cared for within the establishment, will not appear in the warehouse. Data relating to health professionals and users: Identification data in the warehouse: name, first name, e-mail address, telephone, affiliation (department, establishment), surname and first name of the referrer.Identification data of users of the en warehouse: surname, first name, e-mail address, login. The Commission considers that the data whose processing is envisaged are adequate, relevant and limited to what is necessary with regard to the purposes of the processing, in accordance with the provisions of Article 5-1 -c of the GDPR. On the recipients Members of the care team, as defined by the provisions of Article L. 1110-12 of the Public Health Code, will have access to all the data contained in the warehouse concerning the patients they take care of. The professionals who are members of the medical information department (DIM)

will have access to the data as part of their current missions. The data of the health professionals are intended for the administrators of the application, who are the users of the EHOP software. This data incorporates the identification data in the warehouse and the identification data of the users of the warehouse. Regarding subsequent research projects, the researchers and members of research teams (biostatisticians, monitoring CRAs, data managers, etc.) who do not belong to the care team will have access to indirectly identifying data from the warehouse, within the limits of strictly necessary and relevant data with regard to of their duties.Only authorized staff of the Nantes University Hospital, grouped in a dedicated cell, will be able to access the warehouse, within the limits of the exercise of the missions entrusted to them.The Commission notes that only coded or anonymized may be transferred outside the EU. The Commission considers that the categories of recipient do not call for observation. On information and the procedures for exercising rights With regard to patients: Persons admitted at the CHU de Nantes after this authorization will be informed of the processing of data concerning them carried out within the framework of the constitution of the warehouse, by means of an information note rem hand-delivered upon admission. People will also be informed by means of a welcome booklet during their hospitalization and by posting in the premises of the establishments. People admitted prior to this authorization will be informed of the constitution of the warehouse and the studies carried out using data from the warehouse through information campaigns (social networks, regional media, press release), public events within the Nantes University Hospital and displays within the establishment which will return on the Nantes University Hospital website. The data controller plans to publish information on its website to announce the constitution of the warehouse and specifying that any patient treated by the Nantes University Hospital, also including the previously treated patients, may oppose the use of their data in the warehouse, as well as for subsequent research purposes. The note will specify that patients have the option of objecting to the reuse of their data for research purposes. The existence and methods of exercising the rights of individuals will also be detailed. The Commission requests that the information media be supplemented in order to contain all of the information provided for in Articles 13 and 14 of the GDPR. The Commission also notes that patients are informed of the possibility of the use of personal data. for health research purposes. It recalls that this general information cannot replace the individual information provided for by the provisions of article 58 of the Data Protection Act and which must be carried out for each data processing carried out from the data of the warehouse, pursuant to the provisions of Chapter IX of the Data Protection Act. The rights of data subjects, the existence of which is recalled in the information documents, will be exercised with the director of the establishment or the hospital group, or by sending an email to

a specific address mentioned in the information documents. .Concerning the procedures for exercising the right of opposition, the Commission notes that the information medium mentions that individuals may oppose the use of data concerning them for research, whatever the reason for the opposition.Insofar as Article 57 of the Data Protection Act provides for the right to oppose the processing of personal data without reason, the Commission requests that the information note be clarified so as not to suggest that a reason for objecting to the use of the data in the context of research should be provided. With regard to health professionals: The information will be delivered to them in the application used to collect the data and by a visible mention in the user interface during each data export. General information as well as information in the Establishment Medical Commission (CME) will be produced and distributed to all professionals. Commission requests that the information media be supplemented in order to contain all the information provided for in Article 13 of the GDPR. Subject to the modification of the information documents, the Commission considers that these methods of information and exercise of rights are satisfactory. On security measuresFirstly, the Commission takes note of the performance by the Nantes University Hospital of an impact study on data protection which has made it possible to build and demonstrate the implementation of the principles of protection of life privacy in setting up the health data warehouse. As regards access to the health data warehouse, the Commission observes that this takes place in two stages. First, users must complete a request from an Internet-accessible portal, specifying the datasets they wish to access. The Commission notes that for this, each user has a personal space and that an authentication policy based on an individual identifier and a password has been put in place to access it. In this regard, it recalls that a satisfactory password policy must comply with its deliberation no. 2017-012 of January 19, 2017 adopting a recommendation relating to passwords. If validated by the warehouse administrators, users are authorized to consult the datasets. The Commission notes that the consultation and manipulation of data can only be carried out from the internal computer network of the Nantes University Hospital. Thus, in order to access the subsets of data requested, users of the warehouse must s 'authenticate using an individual smart card and a four-digit code. The Commission observes that authorization profiles therefore define the access, roles and information available to the various users of the warehouse. The creation of each subset of data is subject to a duration of use. Access permissions are therefore deleted for any user who is no longer authorized. A global review of authorizations is carried out on a regular basis in order to ensure that authorizations are properly erased. The Commission notes that only a small group of people are authorized to access the warehouse in its entirety in order to administer and manage user access requests. With regard to access to the warehouse for these personnel,

the Commission observes that in addition to authentication by individual smart card and four-digit code, an identifier/password pair is used. It recalls that the password policy must follow the recommendations cited above. The Commission notes that, depending on the requests that will be made to the various committees involved in the governance of the warehouse (strategic committee, operational committee, evaluation), the data may be aggregated to enable the production of statistics or be pseudonymised in order to provide users with only the data strictly necessary for research purposes. The Commission recalls that the use of pseudonymisation must ensure that the data handled can no longer be attributed to a specific person without resorting to additional information, this additional information having to be kept separately and subject to adequate technical and organizational measures. In particular, the Commission recalls the need to discard any identifying data such as first name, surname, maiden name, postal address, e-mail address, telephone number, date of birth/death, place of birth/death, NIR, number visit, technical identifier, etc. The Commission notes that the pseudonymisation will be carried out using secret key hashing algorithms. It recalls the need to use state-of-the-art algorithms and to implement key management procedures adapted, making it possible to guard against brute force attacks. The Committee observes that if necessary, it is technically possible to re-identify a patient, for example to come back to him and provided that this operation is authorized. It is also planned to use the pseudonymization of documents unstructured (such as medical reports for example). The Commission recalls that such an operation must be carried out with vigilance, in particular if it uses automated tools and therefore for which errors are likely to occur. The Commission notes that in the event of necessity, for example at for the purpose of collaboration with partners outside the Nantes University Hospital, the data may be anonymized in order to be communicated. The Commission recalls that it will be necessary to demonstrate the compliance of the solution and the anonymization techniques implemented with the three criteria defined by the opinion of the G29 n° 05/2014, and to send it to the Commission. Otherwise, if these three criteria cannot be met, a study of the risks of re-identification should be carried out. This study consists of demonstrating that the risks, linked to the publication of the dataset, have no impact on the privacy and freedoms of the persons concerned. The actions of users accessing the warehouse are subject to traceability measures. In particular, the connections to the warehouse are traced (identifiers, date and time) and the requests and operations carried out. The Commission recommends carrying out a control of the traces automatically, in order to detect abnormal behavior and to generate alerts if necessary. The Commission observes that the warehouse is accessible only on the internal network of the CHU of Nantes from a web browser. Access is secured using the HTTPS protocol. This uses encrypted communication

channels and ensures the authentication of the source and the recipient. Regarding the use of this protocol, the Commission recommends using the most up-to-date version of TLS possible. Measures are planned to ensure the compartmentalization of processing. The company network is subject to filtering measures aimed at restricting the transmission and reception of network flows to identified and authorized machines. Finally, an intrusion prevention system is in place and tests are carried out regularly. The Commission notes that software updates are installed on a regular basis. Specific measures are planned to guarantee the availability of data and services. An anti-malware policy is defined and anti-virus software is installed and regularly updated on all hardware involved in processing. Finally, a maintenance policy for IT environments is defined, ensuring that appropriate security measures data are implemented. The Commission notes that the Nantes University Hospital is an approved host of health data under the conditions of decree no. 2006-6 of 4 January 2006. A backup policy has been implemented. Backups are tested regularly to verify their integrity. The transfer of backups is secure. They are stored in a place that guarantees their security and availability. In addition, during disposal, the stored equipment is cleaned of any personal data. Used or broken down storage media are subject to a destruction or erasure procedure. Access to the premises housing the equipment taking part in the processing is restricted by means of locked doors controlled by a means of personal authentication. . Measures for detecting and protecting against the risk of fire, water damage and loss of power supply are proposed. Finally, a business continuity plan is planned, making it possible to resume activity by reducing the impact of a disaster as possible. The security measures described by the data controller comply with the security requirements provided for in Articles 5-1-f and 32 of the GDPR. The Commission recalls, however, that this obligation requires the updating of security measures with regard to the regular reassessment of the risks. On the other characteristics of the processing The Nantes University Hospital wishes to keep the data contained in the warehouse for the period provided for by the legal and regulatory provisions applicable in terms of retention 20-year-old medical records. Regarding research, access to data from the warehouse by applicants is limited to what is necessary for the study or analysis. The University Hospital of Nantes specified that the extractions carried out for research involving the human person would be destroyed after 15 years of archiving. The commission considers that these data retention periods do not exceed the period necessary for the purposes for which they are collected and processed, in accordance with the provisions of Article 5-1-e of the GDPR. Authorizes, in accordance with this deliberation, the Nantes University Hospital to implement the aforementioned processing. For the PresidentDeputy Vice-President Marie-France MAZARS