Deliberation 2020-028 of February 27, 2020 National Commission for Computing and Liberties Nature of the deliberation: Authorization Legal status: In force Date of publication on Légifrance: Saturday July 11, 2020 Deliberation No. 2020-028 of February 27, 2020 authorizing the University Hospital Center of Rennes to implement personal data processing for the purpose of a health data warehouse called "eHop Rennes" (Authorization request no. 2212496) The National Commission for Computing and Liberties, Seized by the Center university hospital of Rennes of a request for authorization concerning a warehouse of health data called eHop Rennes; Having regard to convention n ° 108 of the Council of Europe for the protection of individuals with regard to the automatic processing of personal data personnel; 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 the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation); Having regard to Law No. 78-17 of 6 January 1978 as amended relating to data processing, files and freedoms, in particular its articles 44-3° and 66-III; Having regard to decree n° 2019-536 of May 29, 2019 taken for the application of law n° 78-17 of January 6, 1978 relating to data processing, files and freedoms; Considering the file and its supplements, and in particular the impact analysis relating to data protection; On the proposal of Mrs. Valérie Peugeot, commissioner, and after having heard the observations by Mrs. Nacima BELKACEM, Government Commissioner, Makes the following observations: On the data controller The Rennes University Hospital Center (CHU) On the legal basis and purpose The CHU wishes to set up a health data warehouse called eHop Rennes . This warehouse will bring together the data produced during the care of patients by the CHU for the purposes of health research, improvement of patient care in the establishment, management of the establishment and teaching. .The file specifies that the processing carried out will not be carried out for commercial purposes. The Commission specifies that, like the national health data system (SNDS), data from the CHU must not be used for the purpose of promoting health products for health professionals or health establishments. or for the purpose of excluding guarantees from insurance contracts and modifying insurance contributions or premiums for an individual or a group of individuals presenting the same risk. The Commission notes that specific governance is implementation for the warehouse. It is entrusted to the clinical data center (CDC) and organized around a steering committee, in charge of validating the strategic and scientific orientations and a scientific and ethics committee in charge of examining the research projects carried out since the warehouse data. The legal basis for the processing is the exercise of a task in the public interest, within the meaning of Article 6-1-e of the European Data Protection Regulation (hereinafter the GDPR) . 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 the provisions of Articles 44 3° and 66 should be applied. III of the amended law of January 6, 1978, which requires authorization for processing involving data relating to health and justified, as in this case, by the public interest. The Commission recalls that the processing of health data of a personnel which will be implemented, for research purposes in the field of health, from the data contained in the warehouse are separate processing operations which must be the subject of specific formalities under Articles 66 and 72 et seq. of the Data Protection Act. On the data processed The warehouse will group the data produced in the context of the care of patients from the hospital information system of the CHU. More specifically, with regard to patients, the following data is collected: identification data and contact details: patient identification number in the establishment, surname, first names, date of birth (transformed into month and year of birth), sex, telephone and electronic contact details, geographic coordinates (generation of latitude and longitude from the postal address of patients), country and postal code of birth; data relating to the professional situation (socio-professional category); health data and genetic analysis data; medico-administrative data from the local PMSI. CHU staff, identification and contact data are collected: title, surname, first name, function, department and practice unit, email address and phone number. o professional telephone numbers. The Commission considers that the data whose processing is envisaged is 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. the recipientsThe recipients of the data in the warehouse are healthcare professionals from the CHU, members of research teams internal or external to the establishment in the case of multicentre healthcare research projects. The Commission recalls that the recipients not belonging not to the care team are only authorized to access the data in the warehouse within the limits of the data strictly necessary and relevant with regard to the objectives of the research project, their functions and the mandate given by the person responsible for the processing implemented within the framework of the project.The Commission also recalls that this access must be carried out in strict compliance with the confidentiality of the data.Back sier indicates that the transmission of personal data to a team outside the CHU can only be done within the framework of data processing authorized by the CNIL. The Committee takes note of this.With these reservations, the Committee considers that the categories of recipients do not call for comment.On information and the rights of individualsAs regards the information of individualsAs regards patients admitted prior to the constitution of the warehouse: The Commission notes that, given the number of people concerned (approximately 1 million patients), the low number of usable email addresses available to the CHU (the file indicates

that the emails of 47,000 patients have been collected for the purposes of a satisfaction survey, but without being able to assess the relevance of these addresses), the CHU considers that individually informing all the persons concerned would require a disproportionate effort. In accordance with Article 14-5-b of the GDPR, the data controller undertakes to take the following measures to protect the rights and freedoms as well as the legitimate interests of the persons concerned: n collective information about the warehouse on its website; relay this collective information via social networks, regional media and press releases; ask patient associations to relay this information. or readmitted) after the establishment of the warehouse: The Committee notes that they will be informed individually as follows, depending on the patient's management method: by the delivery of an information note to patients when their admission or their registration in consultation by the agents of the admissions office or the medical secretariats; by the delivery of an information note to the patients during their pre-admission by the medical secretariats or the programming nurses. Rennes also provides for collective information via dissemination on its website and the use of information campaigns (on social networks, regional media, associations patient reports and press release). With regard to CHU staff: The staff will be informed individually by means of a letter from the CHU attached to the payslip. The information will also be distributed to the Establishment Medical Commission and on the establishment's intranet site. rights of data subjects are exercised, for patients with the data protection officer, for CHU staff with the clinical data center. Articles 13 and 14 of the GDPR. Subject to taking these observations into account, the Commission considers that these procedures for information and the exercise of rights are satisfactory with regard to the provisions of the GDPR and the Data Protection Act. On the security measuresFirstly, the Commission notes that the data controller has carried out an impact analysis relating to data protection in order to demonstrate the compliance of the health data warehouse; it takes note of the accompanying action plan. The data is stored on a secure CHU server, for which an HDS certification process is in progress. The Commission notes that measures are planned to ensure the partitioning of processing. The network is subject to filtering measures aimed at restricting the transmission and reception of network flows to identified and authorized machines. The warehouse is only accessible on the internal network of the Rennes University Hospital from an interface provided for this purpose. Access is secured using the HTTPS protocol, which guarantees the confidentiality of the data exchanged as well as 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. Finally, the Commission takes note of the data controller's commitment to set up an administration stronghold. The Commission also notes that directly identifying data is logically separated from pseudonymized

data and that the action plan provides , a physical separation of these data. The Commission notes that the used names are replaced by a unique pseudonymous number resulting from the application of a hash function to the IPP number and that the date of birth is replaced by the age. It 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 appropriate technical and organizational measures. Furthermore, the Commission points out that the documents added to the warehouse are subject to a specific process of deiden tification as soon as they are integrated into the database: directly identifying information such as surname, first name, postal code, city and telephone number are then replaced by a generic term (BIRTH NAME, FIRST NAME, CP, CITY, TEL). The Commission notes that different authorization profiles are provided in order to manage access to data as needed (users, experts, and administrators). The Commission recommends that the data controller put in place technical and organizational measures to ensure that these rights and profiles are exclusive:* For users and experts who access the datamart part (set of data associated with a study ) of the warehouse, three independent rights are defined:- access to aggregated data;- access to de-identified individual data;- direct access to nominative individual data. * For experts, specific rights are defined to allow them to create datasets or extract study files from the pseudonymised part of the warehouse. The data will then be made available to the research teams through the warehouse interfaces. In this respect, the Commission notes that exports are restricted to a controlled workspace and that specific traceability measures are implemented: atypical exports are subject to automated alert reporting and are subject to validation of a manager. In addition, the transmission of personal data to a team outside the Rennes University Hospital can only be done within the framework of data processing authorized by the CNIL. * Finally, the administration responsibilities are separated into different roles: study administrator, data administrator, log administrator and database administrators. For each subsequent study, there will be specific access to the data. Access authorizations concerning a study will be granted for a limited duration and scope corresponding to the needs of the study. Access permissions will be removed for any user who is no longer authorized. A global review will be carried out annually. Each user will have a unique, individual and nominative user account. In addition, the Commission notes that a data analysis module will allow the production of aggregated statistics on the pseudonymised data of the warehouse, which will then be accessible to all users. The Commission recalls that such a tool must only allow perfectly anonymous restitutions. Failing this, additional measures must be implemented in order to limit the risks of re-identifying individuals, in particular by limiting the targeted queries and the level of detail of the data provided. As

regards the authentication mechanisms for healthcare professionals, the Commission notes that the data controller recommends the use of the CPX card for access to the warehouse, without making it compulsory. The Commission recalls in this respect that access to health data by health professionals must be 'carry out in accordance with the interoperability and security standards, pursuant to article L. 1110-4-1 of the CSP. With regard to access to data by administrators, researchers and members of research teams, the Commission notes that the data controller has undertaken to set up a strong authentication mechanism. strong state-of-the-art authentication for all access to pseudonymised data from a health data warehouse. The Commission notes that the actions of users accessing the warehouse are subject to logging measures. In particular, connections to the warehouse (identifiers, date and time), requests and operations carried out are traced, and certain sensitive actions are subject to enhanced traceability (in particular the assignment of rights to a user, a access to personal data, lifting of a patient's opposition, deletion of a batch of data, import of a pairing file). Trace control will be carried out at the end of each authorization period linked to a research project. The Commission also recommends setting up automatic trace control, in order to detect abnormal behavior and raise alerts. where applicable. Subject to the previous observations, 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 and the impact analysis relating to data protection with regard to the regular reassessment of the risks. On the duration of data retention Data is kept in the warehouse for 20 years from of the patient's last stay and will be deleted by means of a request scheduled annually. The Commission considers that this data retention period does not exceed the period necessary ssary for the purposes for which they are collected and processed, in accordance with the provisions of Article 5-1-e of the GDPR. Authorizes the Rennes University Hospital Center, in accordance with this deliberation, to implement the processing mentioned. The PresidentMarie-Laure DENIS