DELIBERATION n°2019-103 of SEPTEMBER 5, 2019National Commission for Computing and LibertiesNature of the deliberation: AuthorizationLegal status: In force Date of publication on Légifrance: Tuesday, November 05, 2019Deliberation n° 2019-103 of September 5, 2019 authorizing the hospital center University of Lille to implement automated processing of personal data for the purpose of a health data warehouse, entitled "INCLUDE" (Authorization request no. 2202081)The National Commission for Computing and Freedoms, Entry by the Lille University Hospital Center of a request for authorization concerning the automated processing of personal data for the purpose of setting up a health data warehouse; Having regard to Convention No. 108 of the Council of Europe for the protection of individuals with regard to the 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 ); Having regard to the public health code; Having regard to law n° 78-17 of January 6, 1978 as amended relating to data processing, files and freedoms, in particular its articles 44-3° and 66-III and following; Decree No. 2019-536 of May 29, 2019 taken for the application of Law No. 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 Ms Valérie PEUGEOT, commissioner, and after having heard the observations of Ms Nacima BELKACEM, government commissioner, Makes the following observations: On the controller The university hospital center of Lille (the University Hospital of Lille). On the purpose and legal basis of the processingThe purpose of the Lille University Hospital health data warehouse is to enable research, studies and evaluations in the field of health to be carried out by the professionals of the University Hospital and its partners outside (health establishments, research institutes, universities, drug and medical device manufacturers). More specifically, it is intended to facilitate the performance of internal and multicentre studies involving or not involving the human person, medico-economic analyzes for decision-making and strategic purposes or hospital epidemiology, research aimed at producing models predictive in terms of health vigilance, quality and safety of care, pre-screening of patients for the purpose of clinical trials, design of medical decision support tools operating from an artificial intelligence device. The Commission notes that specific governance is planned by the CHU for the data warehouse via the creation of a scientific and ethical committee competent to determine the use that will be made of the data from the warehouse, in particular within the framework of multicenter research projects, as well as a strategic and operational committee. The legal basis for processing is the exercise of a mission in the public interest, within the meaning of Article 6-1-e

of the European Regulation data (hereinafter GDPR). The Commission considers that the purposes pursued are determined, explicit and legitimate, in accordance with the provisions of Article 5-1-b GDPR. The Commission considers that the provisions of Articles 44-3° and 66 should be applied. -III et seq. of the amended law of 6 January 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 personal data health of a personal nature which will be implemented subsequently for the purposes of research, study and evaluation in the field of health, based on data extracted from the health data warehouse of the Lille University Hospital, are processing of data distinct from the warehouse which must be the subject of specific formalities in accordance with the provisions of articles 72 and following of the “data-processing law and freedoms”. On the data processed The data in the warehouse relate to patients cared for by the CHU, including patients cared for before the constitution of the warehouse, as well as to healthcare professionals. With regard to data relating to patients, coming from the hospital information system and collected in the context of care (computerized patient file, specialized medical files, - emergency, imaging, resuscitation, medical biology, anesthesia, operating room monitoring -, software used for the information systems medicalization program and for monitoring health vigilance): identification data: address, date and place of birth, identification number; data related to personal life: family situation and lifestyle; data related to professional life: professional situation, schooling, training, occupational exposure; economic and financial data: social coverage and assessment of people's social difficulties; sensitive data: health data (pathologies, conditions, medical history, data relating to care, imaging data, biology data, risk situations and behaviours, genetic data, etc.), data relating to presupposed racial or ethnic origin. With regard to data relating to healthcare professionals: identification data: title, surname and first name; data related to professional life: employee number, job title, division, department, functional unit in which the professional is affiliated, address professional electronics. The Commission considers that the data whose processing is envisaged are adequate, relevant and linked. 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 RGPD. On the recipients Subject to compliance with the specific provisions of the law "IT and freedoms" applicable to the realization of research, studies and evaluations in the field of health, the health professionals of the Lille University Hospital and the professional members of the medical information department will have access, for the performance of their missions, to all the data contained in the warehouse and for the purpose of carrying out the research, studies and evaluations referred to in this authorisation, Subject to this same reservation, the external partners of the Lille University Hospital (health establishments, research institutes,

universities, drug and medical device manufacturers ) will also have access to health data from the warehouse that will be strictly necessary and relevant to the objectives of the research, studies and evaluation. readings that they carry out from said data. The Commission points out, on the one hand, that industrialists' access will be limited to anonymised data within the meaning of G29 opinion no. 05/2014 of 10 April 2014 relating to anonymisation techniques and that, on the other On the other hand, the CHU excludes access to the warehouse to professionals from the banking and insurance sector. The Commission considers that the categories of recipients do not call for any particular observation. On information and the rights of individuals 69 of the law "Informatique et Libertés", the persons from whom the personal data are collected or about whom such data are transmitted must be recipients of individual information, including the elements provided for in article 13 or 14 of the GDPR. With regard to patients whose data was collected prior to this authorisation: The Commission notes that the Lille University Hospital wishes to supply the health data warehouse with patient data v been at the University Hospital since 2008. She observes that, given the number of patients concerned (more than 1 million), the uncertainty concerning their vital status, the age of some of the data, the economic cost generated by the individual information, the CHU as data controller considers that informing patients individually would constitute a disproportionate effort. Pursuant to article 14-5-b of the GDPR and article 69 of the law amended, the obligation to provide individual information to the data subject may be subject to exceptions in the event that the provision of such information proves impossible, requires disproportionate effort or seriously compromises the achievement of the objectives of the treatment. In such cases, in accordance with the GDPR, the controller takes appropriate measures to protect the rights and freedoms, as well as the legitimate interests of the data subject, including by making the information publicly available. In the present case, the Commission notes that an exception will be made to the principle of individual information for persons with regard to patients whose data has been collected prior to this authorization and that appropriate measures will be implemented, in particular means of collective information on the constitution of the warehouse by posting in the premises of the CHU, a mention on its website and the welcome booklet given to patients, the use of social networks and a publicity information in the local newspaper. The Commission notes that the collective information media given to it in support of its request do not explicitly mention the constitution of the warehouse, its purpose and the rights of the persons concerned. . It requests that these information media be supplemented on these points to comply with the requirements of Articles 13 and 14 of the GDPR. With regard to patients whose data will be collected after this authorization (new patients or patients undergoing ): The Commission notes that the personnel of the Lille University Hospital (doctors,

nurses, medical secretaries, agents from the admissions office) will proceed, from the delivery of a written document, to inform the patient as well as to collect his consent. This will be carried out, initially, by manual entry in the hospital information system and that the CHU plans to eventually set up an interoperable system for collecting patient consent allowing the latter to express their consent before, during and after coming to the hospital and to reconsider it. The Committee indicates that the interoperable consent collection system envisaged in the long term should not replace the current manual entry system, in order to facilitate the expression of consent by all patients. In addition, the CHU will also provide collective information (provision of a written document in the consultation waiting rooms, specific mention in the welcome book and on the CHU website). The Commission recalls that the individual information provided must strictly comply with the requirements of Articles 13 and 14 of the GDPR and must relate specifically to the warehouse, its purposes and the rights of the persons concerned. With regard to healthcare professionals:The individual information of these professionals is provided via information accompanying the payslip and the internal magazine of the Lille University Hospital.The rights of the persons concerned (patients and healthcare professionals) are exercised with the data protection officer of the Lille University Hospital by sending an electronic message or by post. Subject to the modification of the collective information media made available to patients, the Commission considers that the methods of information retained and exercise of rights are satisfactory. On security measures The Commission takes note of the implementation by the CHU de Lille of a data protection impact analysis that made it possible to build and demonstrate the implementation of privacy protection principles in the constitution of the health data warehouse. Provided that the corrective measures proposed in the part dedicated to areas for improvement of the impact analysis produced are actually implemented, it makes the following observations. With regard to access to the data warehouse of health: The Commission observes that these are issued by a scientific and ethical committee participating in the governance of the warehouse. Following the filing of a request and its validation, the administrators of the warehouse prepare the data which will be made available to the applicants. The Commission notes that it should be ensured that each data set created has a limited and previously defined period of use. Different authorization profiles are provided in order to manage access to the data as needed. Access permissions are removed for any user who is no longer authorized. The Commission recalls that an overall review must be carried out on a regular basis in order to ensure that authorizations are properly erased. Each user has a unique, individual and nominative user account. An authentication policy based on an individual identifier and a password is in place to allow user access to datasets in the warehouse. This authentication policy complies with Commission deliberations

n° 2017-012 of January 19, 2017 and n° 2017-190 of June 22, 2017 concerning recommendations relating to passwords. It is reinforced in the case of administrators with access to health data by increasing the minimum size of passwords to 14 characters associated with a mechanism for locking access to the account in the event of multiple entry of incorrect passwords. Commission notes that depending on the requests that will be made, the data may be subject to different types of pre-processing. They may thus be aggregated, pseudonymized or anonymized. The Commission notes that the processes for anonymizing and pseudonymizing data have not yet been defined. It is therefore not in a position to comment on their validity. The Commission recalls that: in the case of anonymisation: it will be necessary to demonstrate the compliance of the solution and the anonymisation techniques implemented with the three criteria defined by the opinion of the G29 n°05/2014 of 10 April 2014 cited above, and forward it to the Commission. This opinion holds that data processing is a priori anonymous when it is not possible to individualize, correlate or interfere with the data. 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 data set, have no impact on the privacy and freedoms of the persons concerned. in the case of pseudonymization: the data handled must no longer be attributed to a specific person without having recourse 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, visit number, technical identifier, etc. In the event that it is envisaged to resort to the pseudonymisation of unstructured documents (such as medical reports for example), the Commission points out that such an operation must be carried out with vigilance, in particular if it implements automated tools for which errors are likely to occur. 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 an automatic trace control, in order to detect abnormal behavior and to generate alerts if necessary. The Commission observes that the warehouse is only accessible on the internal network of the Lille University Hospital from an interface provided for this purpose. 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. With regard to access to pseudonymised data accessible via the CHU intranet, the Commission recommends the implementation of a strong

authentication policy. It also recalls that access to health data by health professionals must be in accordance with the interoperability and security standards pursuant to Article L. 1110-4 of the Public Health Code. The Commission notes however, it is envisaged in the long term to open up the possibility of remote access. It recalls in this regard that it will be necessary to specify the terms of delivery and the security means implemented, in order to ensure the effectiveness of the measures with regard to the risks that such access could pose to the processing. Regarding data security: 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 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, an IT environment maintenance policy is defined, ensuring that appropriate data security measures are implemented. Interventions are thus subject to traceability. A backup policy is 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 to detect and protect against the risk of fire, water damage and loss of electrical power are proposed. Finally, a business continuity plan is planned, making it possible to resume activity by reducing the impact of a disaster as much as possible. The security measures described by the data controller comply with the security requirement 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 retention period of the data The data will be kept in accordance the storage periods provided for by the provisions of Article R. 1112-7 of the Public Health Code for the storage of patients' medical records. The Commission considers that the storage periods provided for do not exceed the period necessary for the purposes for which the data is collected and processed, in accordance with the provisions of Article 5-1-e) of the GDPR. Authorizes, in accordance with this deliberation, the Lille University Hospital to implement implements automated processing of personal data for the purpose of setting up a health data warehouse aimed at carrying out research, studies and assessments in the field of health. For the President The Deputy Vice-President Sophie LAMBREMON