Deliberation 2020-055 of May 14, 2020Commission Nationale de l'Informatique et des LibertésNature of the deliberation: AuthorizationLegal status: In force Date of publication on Légifrance: Saturday July 11, 2020Deliberation n° 2020-055 of May 14, 2020 authorizing the company IMPLICITY to put implements automated processing of personal data for the purpose of a study on the development and validation of algorithms for predicting heart decompensation attacks in patients with connected heart implants, entitled "HYDRO". (Corrigendum) (Request for authorization no. 920054) Deliberation no. 2020-055 of May 14, 2020 authorizing the company IMPLICITY to implement automated processing of personal data for the purpose of a study relating to the development and validation of algorithms for predicting heart decompensation attacks in patients with connected heart implants, entitled "HYDRO". (Corrigendum)(Request for authorization no. 920054)The National Commission for Computing and Liberties,Registration by the company IMPLICITY of a request for authorization concerning the automated processing of personal data for the purpose of a study relating to on the development and validation of algorithms for predicting cardiac decompensation attacks in patients with connected cardiac implants, entitled HYDRO; Having regard to Convention No. 108 of the Council of Europe for the protection of persons 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 circulation of this data, and repealing directive 95/46/EC; Having regard to law n° 78-17 of January 6, 1978 as amended relating to data processing, files and freedoms, in particular its articles 6 6, 72 and following; Having regard to law n° 2017-1836 of December 30, 2017 on the financing of social security, in particular its article 54; Having regard to law n° 2019-774 of July 24, 2019 relating to the organization and transformation of the health system; Considering decree n ° 2016-1871 of December 26, 2016 relating to the processing of personal data called National health data system Considering decree n ° 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; Having regard to the decree of March 22, 2017 relating to the security reference system applicable to the National Health Data System; Having regard to the decree of October 11, 2018 on the specifications for experiments relating to remote monitoring coverage implemented on the basis of Article 54 of Law No. 2017-1836 on the financing of social security for 2018; Having regard to the opinion of the Expert Committee for research, studies and assessments in the field of health of November 27, 2019; Having regard to deliberation n° 2020-044 of April 20, 2020 providing an opinion on a draft decree supplementing the decree of March 23, 2020 prescribing the measures for the organization and operation of the health system necessary to deal with the covid-19 epidemic in the context

of the state of health emergency (request for opinion no. 20006669); After hearing Mrs. Valérie PEUGEOT, Commissioner, in her report, and Mrs. Nacima BELKACEM , Government Commissioner, in his observations, Makes the following observations: The request for authorization submitted to the Commission requires access to data from SNIIRAM, PMSI and CépiDC, components of the National Health Data System (hereinafter SNDS), within the technical solution of the Health Data Hub (HDH) for the years 2010 to 2023. The processing project, which constitutes research that does not involve the human person, received a favorable opinion of the expert committee for research, studies and evaluations in the field of health on November 27, 2019. A letter extending the deadline was sent to the data controller on March 13, 2020. On the data controller: Created in 2016, the Implicity is a simplified joint-stock company specializing in e-health which has notably developed a remote monitoring platform for patients wearing connected medical devices, called Implicity. The Commission notes that the company Implicity is an industrialist in the health sector whose objective is the development and marketing of an algorithm for the diagnosis and prediction of heart decompensation attacks, considered to be a medical device of the software type. It thus observes that the provisions of the Public Health Code (hereinafter CSP) relating to access to SNDS data and in particular Articles L. 1461-1 and L. 1461-3 of the CSP apply in cash to the controller. The application file mentions that the Health Data Platform acts as a partner of Implicity insofar as it provides the technical infrastructure for hosting health data. The Commission infers from this that the Health Data Platform acts as a processor in the absence of joint responsibilities. The Commission recalls in this respect that the processing of data by subcontractors must be governed by a contract or a legal act in accordance with Article 28 of the GDPR. However, this analysis could be called into question when the decree is published. amending Decree No. 2016-1871 of December 26, 2016 relating to the processing of personal data called the National Health Data System. The Commission would like to point out that in such a case, the agreement concluded between Implicity and the Health Data Platform must be amended accordingly. It also recalls that such a modification will constitute a substantial modification requiring a modification of this authorization. On the legal basis of the processing and the exception allowing the processing of sensitive data The processing operations implemented by the company Implicity are part of the framework of its commercial activity. They are necessary for the purposes of the legitimate interests pursued by the data controller, taking into account the very indirectly identifying nature of the data and the guarantees, particularly in terms of the rights of individuals, provided for by the texts governing the provision of SNDS data. .This processing is, as such, lawful under Article 6-1-f) of the General Data Protection Regulation (hereinafter GDPR). In addition, the Commission considers that this processing,

necessary for scientific research purposes, fulfills the condition provided for in Article 9-2-j) of the GDPR allowing the processing of data concerning health. On the purpose and interest treatment public: The main objective of this study is to develop and validate an algorithm for diagnosing and predicting cardiac decompensation attacks. prevent hospitalization of heart failure patients with rhythmic prostheses, throughout the national territory and regardless of the brand of the implanted device. The objective is also to reduce the costs related to their medical care. This study is also part of technological development to respond to future telemedicine care in the world, as provided for in the specifications. charges relating to telemedicine experiments for the improvement of health pathways (ETAPES) provided for by the decree of October 11, 2018 on the specifications for experiments relating to care by remote monitoring implemented on the basis of the Article 54 of Law No. 2017-1836 on social security financing for 2018. The Commission considers that the purpose of the processing is determined, explicit and legitimate, in accordance with Article 5-1-b) of the GDPR. It also considers that this processing serves a purpose of public interest, in accordance with Article 66-I of the Data Protection Act. On the nature of the data processed: The categories of data whose processing is envisaged in this study are: Data from SNIIRAM, PMSI and CépiDC, components of the SNDS, for the years 2010 to 2023 concerning all people with heart failure and/or wearer of an implanted rhythmic heart prosthesis: identification data: month and year of birth, gender; health data: procedure and date of implantation, type of device implanted, drug treatments, medical stays, comorbidities , medical procedures performed, medical devices, list of examinations performed, comorbidities and deaths. Data from the IMPLICITY remote monitoring platform concerning people wearing a connected medical device over the last ten years and those of new patients: identification data month and year of birth, gender; health data: procedure and date of implantation, type of device implanted, clinical data, data from medical devices and determining the patient's state of health and data from algorithms or comparable sensors; data collected by the technical solution of the data controller as part of the DAI-PP study, carried out by the National Institute of Health and Medical Research (INSERM) and which has been the subject of a declaration of conformity with the reference methodology MR003 (n°2118761). 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. The Commission also notes that It is envisaged that data from the study will be made available to the Health Data Platform in a catalog of telecardiology data. In this respect, the Commission recalls that if these data are intended to integrate a permanent database, for the purpose of reuse for subsequent processing, the constitution of such a database falls under, except in the

case of collection of the express consent of the data subject, of the authorization scheme provided for by the general provisions of section 3 of chapter III of title 2 of the Data Protection Act applicable to the processing of personal data in the field of health. Any new study that would be implemented from these data will also have to be the subject of formalities with the Commission. On direct access to SNDS data by a health manufacturer: In order to be able to access SNDS data , the data controller is required, in accordance with the provisions of Article L.1461-3 of the Public Health Code: either to demonstrate that the methods of implementation of the processing make any use of the data impossible for one of the purposes mentioned in V of Article L. 1461-1; either to use a research laboratory or a design office, public or private, to carry out the processing. In this case, the data controller does not wish not resort to a research laboratory or a design office. It is therefore up to him to demonstrate that the methods of implementation of the processing make any use of the data for one of the prohibited purposes impossible, in particular for the promotion of certain health products to health professionals or health establishments. health. In this regard, the data controller presented a detailed argument including the implementation of a set of specific technical and organizational measures. Firstly, the Commission notes that the data controller undertakes that only the personnel specifically identified within the research and development team can be authorized to access the project space. A strict separation of roles between the research and development personnel and the personnel in charge of the commercial development of the company's products is in place. The Commission notes in this sense the active process of ISO 27001 certification and the performance of annual audits.Secondly, the Commission notes that the personnel concerned will be made aware of the risks and obligations incumbent on them when they are authorized by the data controller. to access the project space. These personnel must participate in awareness-raising actions led by the Health Data Platform, which will relate in particular to the prohibited purposes. Beforehand, each authorized user must formally and individually undertake not to use the data and results of the project for the realization of the prohibited purposes. The Commission also notes that the president of the company Implicity has undertaken to that neither he nor the hierarchical superiors of the authorized users encourage the latter to use the data of the HYDRO project for the realization of prohibited purposes. Similarly, the director of research, responsible for data export validations, has undertaken to ensure that the data and results of the HYDRO project will not be used for the realization of prohibited purposes. Thirdly, and above all , with regard to the risk of re-identification of establishments or healthcare professionals for the purpose of promoting health products, the Commission notes that the project data will not contain any code identifying the establishments or healthcare professionals or any indication geography concerning them. The

Committee also notes that the analysis of the risks of re-identification of establishments, healthcare professionals and patients which has been carried out has led to planning special efforts to blur as much as possible the characteristics of atypical cases of patients with rare particularities that can lead to re-identification.Concerning the risk of indirect re-identification after data export, the Commission recalls that only anonymous data can be exported outside an approved environment in accordance with the decree of March 22 2017 relating to the security reference system applicable to the National Health Data System. The Commission notes in this respect that dedicated procedures will be put in place by both the controller and the Platform. Thus, any export request will be subject to prior internal validation by a representative identified within the organization responsible for processing. A systematic and preliminary audit will also be carried out by the Platform on the basis of criteria tending to attest to the effective anonymity of the desired export. In this respect, it is provided that no export can relate to a number of persons concerned strictly less than ten. The Commission notes that the data controller undertakes to produce a list of authorized exports with the Health Data Platform. Any update to this list and any exception will be examined jointly by the parties. The Commission nevertheless points out that the criteria and procedures provided for need to be reviewed regularly in the light of developments in anonymization and re-identification techniques. With regard to of all these elements, the Commission considers that they seem likely to demonstrate that the methods of implementation of the processing make it impossible to use the data for one of the prohibited purposes mentioned in Article L. 1461- 1 of the CSP and in particular in this case for the purpose of promoting the products mentioned in II of Article L. 5311-1 towards health professionals and health establishments. On the retention period of the data: The data of the study will be made available on the project space of the Health Data Platform for a period of five years from the effective access to them and will be destroyed at the end of this period.C This duration does not exceed that necessary for the purposes for which the data is collected and processed, in accordance with the provisions of Article 5-1-e of the General Data Protection Regulations. On information and the rights of individuals: With regard to persons whose data comes exclusively from the SDNSWith regard to data coming exclusively from the SNDS, the persons concerned are informed of the possible reuse of their personal health data according to the procedures defined by article R.1461- 9 of the CSP.As regards the people who took part in the DAI-PP project The Committee notes that the patients in the DAI-PP study were individually informed in advance of the re-use of their data within the framework of the HYDRO project. Insofar as transfers outside the European Union are envisaged within the framework of the normal operation of the Platform, the Commission recalls that the information medium will have to be supplemented on this point in order to

comply with the provisions of the Article 14 of the GDPR. Concerning persons being monitored Individual information of the persons concerned will be provided as part of their remote monitoring. This information will be provided by the health professional in charge of their follow-up during a consultation. It will focus on the one hand on the collection of data in the context of remote monitoring and on the other hand on the reuse of this data for research purposes and more specifically in the context of the Hydro project, the design by the company Implicity of algorithms for calculating risks of cardiovascular events in patients with heart failure or arrhythmias. It is also specified that these data may be matched with SNDS data. This information note refers to a specific information system to which data subjects may refer prior to the implementation of each new data processing for research conducted by the data controller. This takes the form of the creation of a Research page on the data controller's website, one page of which is specifically dedicated to the HYDRO project. day-to-day operation of the Platform, the Commission recalls that the information medium must be supplemented on this point in order to comply with the provisions of Article 14 of the GDPR. Express consent relating to the reuse of data for research purposes and materialized by a specific checkbox is provided in order to ensure that the person concerned understands the possible reuse of his remote monitoring data for research purposes. This consent relates to reuse for research purposes generally and is not specific to the Hydro project. The person concerned can thus, as soon as the individual information is issued, refuse to allow their data to be used in the context of subsequent research without this having any consequences on their medical follow-up by telemonitoring. It is also reminded that it has a right of opposition to the use of its data for research purposes that can be exercised at any time for each of the projects that would be carried out and in particular the Hydro project. in the case of persons who are no longer being monitored in the context of remote monitoring Pursuant to Article 14-5-b of the GDPR, the obligation to provide individual information to the person concerned may be subject to exceptions in the event that the provision of such information proves impossible, would require disproportionate efforts or would seriously compromise the achievement of the objectives of the processing. In such cases, in accordance with the General Data Protection Regulation, the controller shall take 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 this case, the Commission notes that an exception will be made to the principle of individual information for persons who are no longer monitored in the context of remote monitoring and that appropriate measures will be implemented, in particular by the dissemination on the data controller's website of information relating to the research project including all the information provided for in Article 14 of the General Data Protection Regulation. The file mentions that the

exercise of the rights of access, rectification, limitation of processing, opposition and deletion may be exercised at any time by the persons concerned with the person in charge of t processing. The Commission notes that the rights of rectification, limitation of processing, opposition and erasure may be exercised on all project data until the date of destruction of the pseudonymisation secrets, scheduled for June 30 2021. In this respect, the file provides that in the event of the exercise of the right of opposition before this date, the data will be deleted from the project space and that no new data concerning the person will be included in the project database. .In addition, the file provides that from the date of destruction of the pseudonymisation secrets, the exercise of these rights can only be carried out directly for the data subsequently included in the project space. The persons participating in the research are informed of the procedures for exercising these rights before and after the destruction of the pseudonymisation secrets. The Commission recalls that in accordance with the principles of transparency and fairness of Article 5 of the GDPR and as specified in the guidelines on transparency adopted by the Article 29 Working Party on 29 November 2017, the data controller must inform data subjects of any specific restrictions applicable to these rights in order to ensure that their reasonable expectations have not been deceived . The Commission also recalls that if the persons concerned provide additional information allowing their re-identification, such an exercise must be made possible in accordance with Article 11 of the GDPR. The Commission considers that these methods of information and exercise of rights of people are satisfied with regard to the provisions of the GDPR and the Data Protection Act. On data security and risk assessmentIn the preamble, the Commission recalls that the processing of data from the SNDS and its components must be carried out in accordance with the provisions of Articles L. 1461-1 to L. 1461-7 of the Code of public health. In particular, the security measures must comply with the security baseline provided for by the decree of March 22, 2017. Pseudonyms will be calculated deterministically using hash functions and cryptographic secrets, for transmission by the data controller. to the CNAM for matching purposes and when health data is made available by the Platform. The Commission notes that no correspondence table will be stored and that only the cryptographic secrets will be kept by the data controller and by the Health Data Platform, on encrypted and physically protected media, access to which will require the intervention of two separate people, within each entity. On the matching: This study requires the matching of two types of data on the technical solution of the Platform: those coming from the remote monitoring platform of the data controller and those present in the SNDS for the people targeted by the study. Only implanted patient data will be matched. This matching will be done in a probabilistic way thanks to the data relating to the act of implantation of the device and the partial identification data of the

patient. Thus, the codes identifying establishments (FINESS, etc.) and health professionals (RPPS, ADELI, etc.) and geographical indications, initially present in the remote monitoring platform, will be transmitted to the CNAM for matching with the SNDS data. The Commission notes that these identifying data will be deleted by the CNAM before transmission to the Health Data Platform, and that the latter will check their deletion before the data set is made available in the HYDRO project space. data from the data controller to the Health Data Platform will be ad hoc (three times a year) and will be done on encrypted channels (virtual private network IPsec). The data itself will be encrypted with a temporary key and signed by the data controller, using secrets dedicated to this transmission, stored in a digital safe and renewed regularly or in case of doubt about their compromise. The CNAM will transmit the matched data to the Health Data Platform according to the same security measures, after having received the data to be matched via its SAFE platform. On the security measures of the HYDRO project area: The Commission notes that the security data from the HYDRO project space essentially depends on the technical solution of the Platform, which was the subject of a global analysis of the risks and impacts on privacy, followed by an approval on December 16, 2019 according to the SNDS security baseline, with a substantial action plan for implementing security measures. More specifically, an impact analysis relating to data protection was sent to the Commission concerning the Platform's technical solution version 1.0, which corresponds to a secure SNDS bubble and which will host the HYDRO project as such. Also, the data controller has carried out an impact analysis relating to the protection of specific data ue to the HYDRO project and integrating the elements provided by the Health Data Platform for its 1.0 platform, as well as an analysis of the risks of re-identification in connection with the prohibited purposes, both transmitted in support of the request for authorisation. The Commission notes that the data controller has provided elements demonstrating good maturity in terms of security management and that it has undertaken certification according to the international standard ISO/IEC 27001, which notably involves a formalization and regular monitoring of procedures related to the security of information systems. In this respect, the Commission notes that the distribution of roles and responsibilities between the data controller and the Health Data Platform, concerning user awareness of the project, the monitoring of traces, the management of alerts and incidents as well as the supervision of data transfers outside the European Union e, must be formalized by an agreement between the two parties. It acknowledges that the data controller will delegate to the Platform the analysis of traces of use of its project space and the transmission of a dashboard of performance indicators. security defined jointly, the regular monitoring of which will be integrated into the data controller's security management system. In addition, the Health Data Platform will report aggregate

security and privacy risk indicators for its underlying technology platform to the project space. The Commission also notes that the management of incidents and breaches will be formalized overall in the General Conditions of Use of the technical solution of the Health Data Platform. On these issues, the Commission recommends that the agreement specify the processes related to security indicators, incident management procedures and data breaches, as well as the methods of raising user awareness, distinguishing the particularities linked to the HYDRO project space and the technical solution of the underlying Platform. It recalls in particular that operational security indicators must be based on a objective and a precise method of calculation, a method and a frequency of collection, as well as rules of decision action to raise alerts. It also emphasizes that raising awareness among users of the HYDRO project space is the responsibility of both the data controller and the Health Data Platform, in a global manner (for example, through regular training) but also by targeted messages during specific operations (for example, a detailed alert in the user interface when exporting data that must be anonymous). In addition, user awareness should be fed by the monitoring of security indicators, in order to correct any behavioral drifts and take into account the appearance of new risks. Under these conditions, the Commission authorizes the company IMPLICITY to implement personal data processing for the purpose of a study on the development and validation of algorithms for predicting heart decompensation attacks in patients with connected heart implants, entitled HYDRO. President Marie-Laure DENIS