Deliberation 2018-257 of June 7, 2018 National Commission for Computing and Liberties Legal status: In force Date of publication on Légifrance: Tuesday July 17, 2018 data processing requiring access on behalf of persons producing or marketing products mentioned in II of Article L. 5311-1 of the Public Health Code to centralized PMSI data made available by ATIH by via a secure solution (MR 006) The National Commission for Computing and Liberties,

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;

Having regard to the public health code;

Considering the law n° 78-17 of January 6, 1978 modified relating to data processing, files and freedoms;

Having regard to law n° 2016-41 of January 26, 2016 on the modernization of our health system;

Considering the decree n° 2005-1309 of October 20, 2005 modified taken for the application of the law n° 78-17 of January 6, 1978 relating to data processing, files and freedoms;

Having regard to Decree No. 2016-1871 of December 26, 2016 relating to the processing of personal data called the national health data system;

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 July 17, 2017 relating to the reference system determining the criteria of confidentiality, expertise and independence for research laboratories and design offices;

After having heard Mrs. Marie-France MAZARS, commissioner, in her report, and Mrs. Nacima BELKACEM, government commissioner, in her observations,

Makes the following observations:

Regulation (EU) No 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 (hereinafter the GDPR), and in particular its article 5, point 2, provides that the data controller must be able to demonstrate that the principles of the regulation

are respected.

Article 9(4) of the GDPR clarifies that Member States may maintain or introduce additional conditions, including limitations, with regard to the processing of genetic data or data relating to health.

Thus, pursuant to the amended law of 6 January 1978 (hereinafter the Data Protection Act), the processing of personal data for the purposes of research, study or evaluation in the field of health is authorized by the National Commission data processing and freedoms (hereinafter the Commission).

The Commission can approve and publish reference methodologies, under the reference systems mentioned in II of Article 54 of the Data Protection Act, established in consultation with the National Institute for Health Data (hereinafter the INDS). , as well as with public and private bodies representing the players concerned.

Among the most common treatments are the treatments carried out by persons producing or marketing the products mentioned in II of Article L. 5311-1 (hereinafter health products) of the Public Health Code (hereinafter CSP) from data centralized by the Technical Agency for Hospitalization Information (hereinafter ATIH), i.e. data from the program for the medicalization of information systems (hereinafter PMSI).

The PMSI consists of a synthetic and standardized collection of administrative and medical information within health establishments, public or private, for-profit or non-profit, whose main objectives are to organize hospital care on French territory. (planning) and to finance establishments according to their activity (activity-based pricing).

Governed by articles L. 6113-7 and L. 6113-8 of the CSP, the PMSI was generalized in the 1990s and is now applied regardless of the hospital sector but with different collection methods depending on the categories of supported. It includes data on the following activities:

- medicine, surgery, obstetrics and odontology (MCO);
- follow-up and rehabilitation care (SSR);
- collection of medical information in psychiatry (RIM-P);
- hospitalization at home (HAD).

A specific file is used to link all the PMSI data concerning the same patient (ANO file).

These treatments make it possible in particular to prepare the files for discussions with the competent authorities and committees, mainly in the field of medicinal products and medical devices (marketing, price discussions, CE marking, etc.) and

the carrying out of studies under actual use.

In view of these needs, the Commission considered that the framework of a reference methodology was appropriate to facilitate and supervise the numerous data processing operations carried out by persons producing or marketing the products mentioned in II of Article L. 5311- 1 of the CSP from PMSI data.

Data controllers who send a commitment to comply with this reference methodology are authorized to implement processing as long as it meets the conditions provided for by these provisions.

Decides: Title I: DEFINITIONS, DATA CONTROLLERS CONCERNED, SCOPE AND PUBLIC INTEREST

1.1. Definitions

For the purposes of this methodology, the following terms are thus defined:

- personal data: any information relating to an identified or identifiable natural person (hereinafter referred to as the data subject); an identifiable natural person is deemed to be a natural person who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier, or to one or more specific elements specific to his physical, physiological, genetic, psychological, economic, cultural or social identity;

- processing: any operation or set of operations carried out or not using automated processes and applied to data or sets of personal data, such as the collection, recording, organization, structuring , storage, adaptation or modification, extraction, consultation, use, communication by transmission, dissemination or any other form of making available, reconciliation or interconnection, limitation, erasure or destruction;

- data controller: the natural or legal person who, alone or jointly with others, is responsible for research, study or evaluation not involving the human person, manages it, checks that its financing is planned and which determines the purposes and means of the processing necessary for it. These are persons producing or marketing the products mentioned in II of article L. 5311-1 of the CSP;

- processor: the natural or legal person, public authority, service or other body which processes personal data on behalf of the controller;

- research laboratory/design office: responsible for the implementation of data processing and responsible for their analysis, having made a commitment to comply with the Commission with the decree of July 17, 2017 relating to the reference framework determining the criteria confidentiality, expertise and independence for research laboratories and design offices. It

is a subcontractor within the meaning of the GDPR who, in the context of this reference methodology, is the only one who can access PMSI data;

- persons in charge of carrying out the study: the natural person or persons who work on the individual data of the PMSI;

- study: research not involving the human person, study or evaluation in the field of health; a study may require the performance of several queries in the database made available by ATIH via a secure solution;

- protocol: document indicating in particular the methodology of the study, the purpose of the processing of personal data, the categories of persons concerned by the processing, the origin, the nature and the list of the personal data used and the list of justifications for the use of these, the duration and organizational methods of the study, the method of data analysis, as well as, when the characteristics of the study so require, the justification for the number of people and the method of observation chosen.

1.2. Data controllers concerned

Only persons producing or marketing the products mentioned in II of article L. 5311-1 of the CSP can make a commitment to comply with this reference methodology.

1.3. Processing of personal data included in the scope of this methodology

Only the processing of personal data for the purpose of carrying out studies of a public interest nature and respecting the security, organizational and transparency:

- data processing can only be carried out through a research laboratory or a design office, public or private, having made a commitment to comply with the Commission with the decree of July 17 2017 relating to the reference system determining the criteria of confidentiality, expertise and independence for research laboratories and design offices; the data controller signs a data access agreement with ATIH and sends it the updatable list of research laboratories or design offices it uses; the data is made available to the research laboratory or the design office by ATIH via a secure solution; no export of personal data is possible outside of the secure solution used. Only anonymous results can be exported;

- the controller appoints a data protection officer and keeps a record of processing activities. A protocol must be validated by the data controller before the start of the implementation of data processing;

- the data controller undertakes not to pursue one of the prohibited purposes, in particular the promotion of the products mentioned in II of article L. 5311-1 of the CSP towards health professionals or health establishments ; the data controller

carries out an independent external audit on compliance with the purposes within three years of the commitment to comply with this reference methodology and then every three years after the first audit carried out;

- the data controller registers all the processing carried out within the framework of the reference methodology in a public directory kept by the INDS; the method and the results obtained are published by the INDS at the end of the processing, according to the procedures provided for in paragraph 6.2 Principle of transparency .

This reference methodology is not applicable to processing:

- requiring an export of personal data outside the secure solution used;

- requiring matching with personal data other than those made available by ATIH.

1.4. Public interest and prohibited purposes

Access to personal data from the national health data system (hereinafter SNDS) and its components, including data from the information systems mentioned in Article L. 6113-7 of the CSP, may be authorized to allow processing for study purposes in the public interest.

The processing carried out within the framework of this reference methodology must respond to a reason of public interest, justified by the data controller to the INDS.

Beyond the ban on re-identification of patients, two prohibited purposes are recalled:

1° The promotion of the products mentioned in II of Article L. 5311-1 towards healthcare professionals or healthcare establishments;

2° The exclusion of guarantees from insurance contracts and the modification of contributions or insurance premiums for an individual or a group of individuals presenting the same risk. Title II: PROCESSING RELATING TO THE DATA OF PERSONS CONCERNED BY STUDIES

2.1. Purpose of processing

The processing of personal data of the persons concerned must not have as its main or secondary objective, or the effect of enabling the achievement of one or more prohibited purposes, described in Article L. 1461-1 V of the CSP.

The public interest reason is justified by the data controller in the protocol and with the INDS in accordance with paragraph 6.2 Principle of transparency of this reference methodology.

In any event, the processing of study data for the following purposes may be carried out within the framework of the reference

methodology:

- preparation of records for discussions and meetings with the competent authorities and committees (example: annual meetings of the prospective committee for medicinal innovations (CPIM), economic committee for health products (CEPS), etc.);

- carrying out studies in real conditions of use for or at the request of the authorities;

- targeting centers and/or carrying out feasibility studies within the framework of research involving or not involving the human person;

- carrying out studies in the context of vigilance and post-market surveillance.

2.2. Origin and nature of the data

2.2.1. Origin of personal data

The data must come exclusively from the databases compiled by ATIH under the PMSI.

2.2.2. Nature of personal data

Pursuant to Article 5(1)(c) of the GDPR, the data processed must be relevant, adequate and limited to what is necessary in relation to the purposes for which they are processed (principle of data minimization). In this respect, the data controller undertakes to process only the data that is strictly necessary and relevant to the objectives of the study. Therefore, each of the categories of data can only be processed if their processing is justified in the protocol.

The categories of personal data that may be processed are centralized data made available by the Technical Agency for Information on Hospitalization (ATIH), on all files in the fields:

- medicine, surgery, obstetrics and odontology (MCO);

- follow-up and rehabilitation care (SSR);

- collection of medical information in psychiatry (RIM-P);

- hospitalization at home (HAD);

- with the possibility of linking all the PMSI data concerning the same patient by means of the ANO file.

The processing operations included in this reference methodology relate to national PMSI data, the maximum historical depth of which is nine years plus the current year.

The geographical area concerned as well as the historical depth of the data consulted are justified in the protocol.

2.3. Recipients of the personal data processed

ATIH data is made available to the research laboratory or design office through a secure solution. No export of personal data can be carried out outside the secure solution used within the framework of this reference methodology.

Only the staff of the research laboratory and the design office can access the data, in compliance with the provisions provided for in article 3 of the reference system determining the criteria of confidentiality, expertise and independence for research laboratories and design offices.

These categories of persons are subject to professional secrecy under the conditions defined by Articles 226-13 and 226-14 of the Criminal Code.

The qualification of authorized persons and their access rights must be regularly reassessed by the research laboratory or design office in accordance with the procedures described in the authorization procedure that it has established.

2.4. Publication of results

In accordance with the provisions of the Data Protection Act, the presentation of the results of the data processing cannot under any circumstances allow the direct or indirect identification of the persons concerned.

2.5. Information and rights of the persons concerned by the study

The information of the persons concerned, as to the possible reuse of their data and the procedures for exercising their rights, is ensured by a notice appearing on the website of the data controllers, research laboratories and design offices, health establishments, health insurance organizations and on media enabling it to be brought to the attention of individuals, in particular posters in premises open to the public or documents given to them.

The rights of access, rectification and opposition are exercised with the director of the body managing the compulsory health insurance scheme to which the person is attached, in accordance with the provisions of article R. 1461-9 of the CSP .

2.6. The duration of the conversation

The PMSI's personal data cannot be stored outside the secure solution used by the research laboratory or the design office. Only anonymous results can be exported.

The duration of access to the data in the secure solution must be limited to that necessary for the implementation of the processing. When the data controller justifies it, access to the data may be maintained at the end of the study, within the limit of two years from the last publication relating to the results.

When the secure solution is held by the research laboratory or the design office, the duration of access to the data and the retention period in the secure solution must be limited to the duration necessary for the implementation of the processing.

When the data controller justifies it, access to the data and their storage may be maintained at the end of the study, within the limit of two years from the last publication relating to the results.Title III: PROCESSING RELATING TO DATA OF PERSONS RESPONSIBLE FOR CARRYING OUT THE STUDY

The data processing of the persons responsible for carrying out the study must have the sole purpose of implementing the study and complying with the legal obligations of the data controller or the design office/research laboratory.

In particular, the data processed are intended for the management of declarations of interest, their transmission to the INDS if necessary and the management of the internal authorization procedures of the design office or research laboratory.

The only categories of personal data relating to data subjects that may be processed are the following:

- surname, first name(s), function, access profiles;
- if relevant: professional telephone, postal and/or electronic contact details, employing body;
- training / qualifications ;
- elements necessary for the evaluation of knowledge in order to carry out the study.

The information of the persons concerned as well as the procedures for exercising their rights comply with the principle of transparency provided for in Chapter III of the General Data Protection Regulation.

The personal data of the persons concerned in charge of carrying out the study cannot be kept beyond a period of five years after the end of the study or for a period in accordance with the regulations in force.Title IV : IMPLEMENTATION AND SAFETY

The implementation of personal data processing occurring within the framework of the study is carried out under the responsibility of the data controller, and of the research laboratory or design office acting on its behalf, in compliance with the provisions articles 24, 25, 28, 32 to 35 of the GDPR, as well as the decree of March 22, 2017 relating to the security reference system applicable to the SNDS and the decree of July 17, 2017 relating to the reference document determining the confidentiality criteria, expertise and independence for research laboratories and design offices.

The systems making the PMSI data available must therefore comply with the security reference system applicable to the aforementioned SNDS; two methods of provision are included in the framework of this reference methodology:

- the data is made available to the research laboratory or design office via the secure access service provider designated by ATIH;

- the data is exported to a research laboratory or a design office having a secure solution and having concluded an agreement with ATIH.

The Commission recalls that it is up to the data controller, in accordance with the reference framework set by the aforementioned decree of July 17, 2017, to ensure that the contract concluded with the research laboratory or design office specifies the measures and conditions certificate attesting to compliance with the decree of March 22, 2017 mentioned above.

Title V: SUBCONTRACTORS

As part of this reference methodology, the data controller never accesses PMSI data and must use, for all processing, a research laboratory or an independent design office, subcontractor, having declared compliant with the Commission with the reference system determining the criteria of confidentiality, expertise and independence for research laboratories and design offices, set by decree of July 17, 2017. In accordance with this decree and article 28 of the GDPR, the respective commitments of the controller and the research laboratory or design office are formalized in a contract whose content is defined by these texts.

In particular, the contract must provide that this subcontractor:

- only processes data on documented instructions from the data controller and takes all required security measures;

- does not subcontract without the written authorization of the data controller;

- helps the data controller to guarantee compliance with his various obligations (rights of individuals, security of processing, notification of breach, impact analyses, etc.);

- provides the data controller with all the information necessary to demonstrate compliance with its obligations and to enable audits to be carried out;

- immediately informs the data controller in the event of an instruction which, in his opinion, constitutes a violation of the GDPR or the Data Protection Act.

In addition, this subcontractor:

- appoints, where applicable, a data protection officer in accordance with Article 37 of the GDPR;

- keep a register of the categories of processing carried out on behalf of the controller, in accordance with Article 30 of the

GDPR.

The controller undertakes to:

- not have any links of interest with the research laboratory or the design office and the purpose of the processing likely to constitute a conflict of interest;

- not seek to access the personal data made available to the research laboratory or the design office;

- not to use the results provided for one of the prohibited purposes. Title VI: IMPLEMENTATION OF THE PRINCIPLE OF RESPONSIBILITY

6.1. Formalities

Each controller appoints a data protection officer, pursuant to Article 37 of the GDPR. This data protection officer will in particular be responsible for monitoring compliance with the processing implemented according to this methodology.

Data controllers send the Commission a single commitment to comply with this methodology for all the processing operations they implement provided they are carried out in compliance with all the provisions of the methodology. A request for an opinion from the expert committee for studies in the field of health (CEREES) is not required.

In accordance with Article 30 of the GDPR, the data controller keeps up to date, within the register of processing activities, the list of processing operations implemented within the framework of this methodology.

6.2. Principle of transparency

The provision of data from the SNDS and its components is designed to account for their use to civil society. To this end, article L. 1461-3 of the CSP makes access to data from the SNDS and its components subject to the communication to the INDS of several elements by the data controller, before and after the study.

Thus, the data controller undertakes to register with the public directory kept by the INDS each study carried out within the framework of this reference methodology. This registration, to be carried out by the data controller or the person acting on his behalf, before the start of each study, is accompanied by the transmission to the INDS of a file comprising:

- the protocol, including the justification of the public interest, as well as a summary, according to the model made available by the INDS;

- in relation to the subject of the study, the declaration of interests of the data controller and that of the research laboratory or the design office, as provided for in article 5 of the decree of July 17, 2017 aforementioned.

At the end of the study, the method and the results obtained must be communicated to the INDS with a view to their publication in compliance with business secrecy and intellectual property.

The recording of the processing and the transmission of the results are carried out in accordance with the methods defined by the INDS.

6.3. External audits

The data controller undertakes to have an independent external audit carried out within it every three years from the commitment to comply with this reference methodology and then every three years after the first audit carried out, with a view to ensure compliance with the principles laid down by law, in particular compliance with prohibited purposes. The audit covers the purposes pursued and the use by the data controller of the results of the studies carried out.

The audit report is sent to the chairman of the SNDS audit committee provided for by the Data Protection Act. Title VII: ENTRY INTO FORCE

This reference methodology comes into force as of its publication in the Official Journal.

This deliberation will be published in the Official Journal of the French Republic.

The president,

I. Falque-Pierrotin