Process No. 8436/2018

/

Authorization No. 7267/2018

I - Order

The Instituto Português de Oncologia do Porto Francisco Gentil, E.P.E., NIPC 506362299, notified the CNPD of a processing of personal data for “other purposes”, explaining that “The Hospital Benchmark project consists of a Business Intelligence platform with indicators oriented to the hospital reality, specific to the control of the use of medicines. On this platform, the hospital will be able to carry out analyzes of consumption standardized by hospital production and specialty, allowing its performance to be compared with the national reality and with reference groups. Based on this decision-making support system, the hospital will be able to easily identify areas with potential for improvement in the use of medicines, and from there, define strategies to reduce costs or improve the safety and quality of care provided.”.

With the request, descriptive elements of the process and an impact assessment on privacy regarding the treatment to be developed were delivered.

From the authorization request it is verified that:

a) The personal data to be processed are: Medication (Drug Code, Description, CHNM Code, Medication Dose, Unit of measurement, Route of Administration, Form of Presentation, Pharmaceutical Form, Pharmacotherapeutic Group, ATC Code, Unit Price, Family, Family Description, Whether it is categorized as Medical Device, Whether it is categorized as Clinical Consumables); Characterization of movements (Type of movement - whether it is a consumption, return, purchase or return to the supplier; Description of the type of movement, Type of movement - detail, Movement Value, Movement Date, Movement Quantity, Movement Unit, Batch , Validity Term, Brand, State, Unit Price, Value); Suppliers (Supplier Code, Supplier Name, Taxpayer Number); Visit data (Service Code, Service Description, Valencia Code, Valencia Description, Cost Center Code, Cost Center Description); Patient ID and Episode - Consumption and Prescription (Patient Type,

1 v.

Patient Internal Number - Data coded at source, Type of episode, Episode Number - Data coded at source); Specific prescription information (Dosage, Date, Duration, Frequency); Information regarding diagnoses/GDHs (Year of birth of the patient (Year range), Main (1) and secondary (2 to 20) Diagnoses (icd9), Surgical procedures performed (icd9), Birth weight (Kg) (if applicable), Type of admission, GDH classification according to the All Patients classification version 21, GCD classification according to the All Patients classification version 21 (GCD are the groupings of GDH s), Episode Number (Data source coded), Discharge service, Date High);

b) Data collection is done directly, by an extracting agent according to the submitted privacy impact assessment;

a) The right of access is exercised in person and in writing to Rua Dr. António Bernardino de Almeida, 4200-072 Porto, the applicant being declared that "The exercise of the right of opposition must be made in writing to the person responsible for Access to Information of the IPO. After validation of the request, the IPO will add the user in question to a list of users in opt-out (Black List), existing at the agent responsible for the aggregation and encoding of the data. After this operation, the agent will suspend future processing or sending to hmR of data generated by the activity of the user in question.";

b) Data communications to third parties are declared: to hmR- Health Market Research, Lda.;

c) There are no interconnections of treatments;

d) There are no international data flows to third countries;

e) Regarding the retention period of the personal data collected, the applicant states that: "The vast majority of the data collected will be retained in the local IPO database for a maximum period of 2 months, with the exception of a specific set of data relating to information on diagnoses and procedures that come from the coding system in GDH, which will need

a longer retention period (up to 6 months). Since the coding process is based on the premise of the multiple cardinality of data that can be considered conspicuous (visible), certain elements need to be retained until, faced with an increasingly complete data set, the system can say that there is already enough cardinality (sufficient set of data) to allow sending to hmR, or, until,

given an already complete data set, the system determines the need to encode data that do not reach the required cardinality.

Now, considering this set of rules, for a set of data with a slow temporal evolution such as the coding data, which result from a process with few automatisms, with delays of up to 4 months to complete the coding of one month, it is understood -if necessary to retain the data for a maximum period of 6 months. For all other data that are recorded daily, the data retention will be a maximum of two months".

Physical and logical security measures are indicated.

II - Appreciation

A- Resolution No. 589/2018, of May 22

This treatment has already been analyzed in determination no. For the rest, refer to the documentation contained in this process for the configuration of the treatment.

Remember that the intention is to use a set of information, duly anonymized, for statistical treatment. Thus, because this is an imperfection in the formulation of the request, and in order to supply an erroneous indication of the purpose of the treatment, under paragraph 2 of article 108 of the Code of Administrative Procedure (CPA), we have redefined the purpose to "Statistical treatment of drug consumption data within the scope of hospital activity". This should make it possible to guide hospital management more efficiently, without jeopardizing the protection of patients.

personal data of the data subjects whose information will be used. In this way, hospitals undertake to implement a set of technical measures that guarantee the pseudonymization of the personal data processed, sending to hmR expunged identification data and which, for the latter, constitute anonymized information, since it will not directly, indirect or inferred to re-identify the information.

B- Order

1. As described in the aforementioned CNPD Determination, within the scope of the aforementioned process, hmR (Health Market Research) intends to implement a "Hospital Intelligence" project, which includes the "Hospital Benchmark", "Hospital Watch" and "Hospital Watch" solutions. DiagWatch Hospital". The first "compares data from each hospital with dynamic

reference groups" and the last two are electronic platforms for statistical information on the consumption of medicines in hospitals at a national level.

Upon submission of the form, several documents were delivered with additional information to the form:

1. Presentation of the Hospital Benchmark project;

2. hmR Hospital Benchmark - Privacy Policy;

3. Privacy Impact Assessment - Health Market Research;

4. Risk Analysis - Anonymization Protocol;

5. Privacy Impact Assessment - Draft participating hospitals;

6. Online Services Terms, version 8/1/2016 - Microsoft;

7. Data Supply Agreement.

2. Examining the request, it is noted that several data will be processed: Drug (Drug Code, Description, CHNM Code, Drug Dose, Unit of measurement, Route of Administration, Form of Presentation, Pharmaceutical Form, Pharmacotherapeutic Group, ATC Code , Unit Price, Family Code, Family Description, Whether it is categorized as Medical Device, Whether it is categorized as Clinical Consumables); Characterization of movements (Type of movement - whether it is consumption, return, purchase or return to the supplier; Description of the type of

movement, Type of movement - detail, Transaction Value, Transaction Date, Transaction Quantity, Movement Unit, Lot, Validity Term, Brand, State, Unit Price, Value); Suppliers (Supplier Code, Supplier Name, Taxpayer Number); Visit data (Service Code, Service Description, Valencia Code, Valencia Description, Cost Center Code, Cost Center Description); Patient ID and Episode - Consumption and Prescription (Patient Type, Internal Patient Number - Source-coded data, Episode Type, Episode Number - Source-coded data); Specific prescription information (Dosage, Date, Duration, Frequency); Information regarding diagnoses/GDHs (Year of birth of the patient (Year range), Main (1) and secondary (2 to 20) Diagnoses (icd9),

Surgical procedures performed (icd9), Birth weight (Kg) (if applicable), Type of admission, GDFI classification according to the All Patients classification version 21, GCD classification according to the All Patients classification version 21 (GCD are the groupings of GDH s), Episode Number (Data source coded), Discharge service, Date High). This is, moreover, explained by the applicant herself in the supporting documents attached to the file.

From all the elements brought to the process, it was clear that it is intended to process the data described above for the purpose of aiding hospital management, supporting health units with this information.

In order to carry out this processing of information, avoiding risks to the personal data and privacy of its holders, a process of pseudonymization (based on coding) of information is proposed, whereby the identity or identification of any natural person is unattainable to the hmR company. It should be noted that this will process the encoded data and, from this treatment, will result in the information to be made available to hospitals and other interested parties in the health sector (public or private).

To this end, two additional servers will be installed in the hospital, with the function of (in one of them) collecting the necessary information and (in the rest) coding it so that it can later be sent to hmR. The latter will only be responsible for processing the information sent to it by the second server.

3. It is also clear from the information sent along with the file that personal data will never reach HMR, that is, under the terms of article 3, al. a), of Law No. 67/98, of 26 October, amended by Law No. 103/2015 of 24 August (Data Protection Law, hereinafter LPDP): «any information of any nature and regardless of of the respective support, including sound and image, relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'.

In addition to the fact that only the hospital has access to information containing personal data, the indicated anonymization algorithms (reviewed in accordance with the CNPD indications), and which are applied to the set of elements transmitted to hmR for statistical treatment, present a technical robustness1 solid enough to depart that same information from the aforementioned concept of personal data. This, of course, only in relation to this company, keeping that data the qualification

of article 3, al. a), of the LPDP, regarding the hospital that collects and maintains the personal data of its users and professionals.

This CNPD assessment is supported by Guideline No. 4/2007, on the concept of personal data, of the Article 29.02 Group. It states that “If, taking into account “all the means that potentially and reasonably will be used by the person responsible or any other person”, that possibility [of identifying the data subject] is non-existent or negligible, the person should not be considered “ identifiable", and the information should not be considered "personal data". The criterion "set of means likely to be reasonably used either by the person in charge or by any other person" must take into account in particular all the factors involved. The cost of the process identification is one of the factors, but not the only one. The intended purpose, the way in which the treatment is structured, the

1 Pay attention to version 3.2 of the document where the anonymization algorithm is described, more specifically in point 2.

2 Advisory group, provided for in article 29 of Directive 95/46/EC, of 24 October, where all the supervisory authorities of the European Union have a seat.

advantage expected by the controller, the interests of the data subjects involved, as well as the risk of dysfunctional organizations (eg breaches of confidentiality obligations) and technical failures must all be taken into account.3».

Indeed, through the measures applied to mitigate the risk of identification or re-identification (de-identification of information prior to its transmission to the hmR, solid anonymization algorithms, erasure of information on patients whose pathologies, due to their atypical nature, could be, although subject to the foreseen anonymization, facilitating the re-identification of data subjects), the probability or even the technical possibility of arriving at the identity of the data subjects is practically nil.

Therefore, we will have to consider that hmR does not process personal data.

C- Legality

Article 7(4) of Law No. 67/98, of 26 October, amended by Law No. 103/2015, of 24 August - Personal Data Protection Law (LPDP), admits the processing of health data when necessary for the purposes of preventive medicine, medical diagnosis, provision of medical care or treatment or for the management of health services, provided that the processing of such data is

carried out by a health professional subject to medical confidentiality or by another person bound by professional health secrecy and provided that information security measures are guaranteed.

When data are processed for the purposes of preventive medicine, medical diagnosis, provision of health care or medical treatments or management of health services, there is legitimacy to carry out automated processing when this is done by persons bound by professional secrecy. To that extent, the collection of information must be combined with the principle of confidentiality, thus respecting the respective professional secrecy or secrecy under the terms of the statutes to which such professionals are legally and statutorily bound, as a way of

3 Free translation of an excerpt from page 15 of said guideline.

guarantee the implementation of adequate measures to preserve information security.

The information processed is collected lawfully (Article 5(1)(a) of the LPDP) for specific, explicit and legitimate purposes (cf.(b) of the same article) and the information collected is not excessive. . The CNPD considers that, in this case, there is legitimacy for the processing, pursuant to Article 7(4) of the LPDP.

As for the right of access (Article 11 of the LPDP), it is important to clarify that it should not be confused with the right of opposition (Article 12 of the LPDP), even if the data subject can exercise any of them.

Regarding the right of access, it must respect the provisions of article 3, no. 34, of Law no. 12/2005, of 26 January (Personal Genetic Information and Health Information Law), in the wording 26/2016, of 22 August, and which now only requires the intermediation of a doctor in accessing the data subject's health when the latter requests it. This undoubtedly revokes paragraph 5 of article 11 of the LPDP, which made “access to information on health data, including genetic data” depend on the intermediation of a doctor.

The precision introduced by the new version of the Law on Personal Genetic Information and Health Information does not, however, detract from the most elementary rules for the protection of personal data, namely with regard to the right of access. Thus, article 3, no. 3, of Law no. 12/2005, of 26 January, should be read in conjunction with the provisions of article 11, no. 1, of the LPDP , maintaining the right, on the part of the holder, to access their personal data and “...to obtain from the person

responsible for the treatment, freely and without restrictions, with reasonable frequency and without delays or excessive costs of all that is provided for in paragraphs of the aforementioned precept of the LPDP.

This novelty is also without prejudice to cases in which the will of the data subject cannot be ascertained, where the obligation of medical intermediation in accessing the

4 Which states: “Access to health information by its holder, or by third parties with their consent or under the terms of the law, is exercised through a doctor, with their own qualification, if the holder of the information so requests. ”.

health information, as prescribed in paragraph 4 of article 3 of the Law on Personal Genetic Information and Health Information.

Regarding the conservation of health data, we understand that the proposed deadlines are justified and proportionate to the purpose described, and most of the information must be deleted after 2 months, with the exception of data relating to information on diagnoses and procedures that come from the coding system in GDH, which is admitted to be eliminated only after 6 months.

As for the anonymized information held by hmR, the LPDP does not apply, so no deadline is set for its conservation.

The applicant declares that data is communicated to hmR. However, and because only data previously subject to pseudonymization processes are transmitted, and it is certain that hmR cannot reverse this process and identify the data subjects, the LPDP does not apply, as there is, for the purposes of the law, any communication.

Particular attention should be paid to the need to ensure:

a) The right of information to data subjects, under the terms of articles 10 of the LPDP;

b) The logical separation between administrative data and health data (cf. Article 15(3) of the LPDP);

c) Security measures must be adopted to prevent access to information by unauthorized persons. The health information that identifies the data subjects must be of restricted access to doctors or, under their direction and control, to other health professionals bound by professional secrecy (cf. Article 7.4 of the LPDP).

III - Decision

In these terms and under the provisions of paragraph 4 of article 7, article 28 and article 30 of the LPDP, the CNPD authorizes the notified treatment, stating the following:

Responsible: Portuguese Institute of Oncology of Porto Francisco Gentil, E.P.E.; Purpose: statistical treatment of drug consumption data within the scope of hospital activity;

Categories of personal data processed: Medication (Drug Code, Description, CHNM Code, Medication Dose, Measuring Unit, Route of Administration, Presentation Form, Pharmaceutical Form, Pharmacotherapeutic Group, ATC Code, Unit Price, Family Code, Description of the Family, If it is categorized as Medical Device, If it is categorized as Clinical Consumption Material); Characterization of movements (Type of movement - whether it is consumption, return, purchase or return to the supplier; Description of the type of movement, Type of movement - detail, Movement Value, Movement Date, Movement Quantity, Movement Unit, Batch , Validity Term, Brand, State, Unit Price, Value); Suppliers (Supplier Code, Supplier Name, Taxpayer Number); Visit data (Service Code, Service Description, Valencia Code, Valencia Description, Cost Center Code, Cost Center Description); Patient ID and Episode - Consumption and Prescription (Patient Type, Internal Patient Number - Source-coded data, Episode Type, Episode Number - Source-coded data); Specific prescription information (Dosage, Date, Duration, Frequency); Information regarding diagnoses/GDHs (Year of birth of the patient (Year range), Main (1) and secondary (2 to 20) Diagnoses (icd9), Surgical procedures performed (icd9), Birth weight (Kg) (if applicable), Type of admission, GDH classification according to the All Patients classification version 21, GCD classification according to the All Patients classification version 21 (GCD are the groupings of GDH s), Episode Number (Data source coded), Discharge service, Date High). Data are subject to a pseudonymization process prior to statistical treatment;

Data communication: None;

Form of exercising the right of access and rectification: in person and in writing to the address of the person in charge;

Data interconnection: None;

Data transfer to third countries: None;

Data retention: most information must be deleted after 2 months, with the exception of data relating to information on

diagnoses and procedures that come from the coding system in GDH, which is allowed to be deleted only after 6 months.

Process No. 8436/2018

NATIONAL COMMISSION

DATA PROTECTION

Lisbon, May 22, 2018

Filipa Calvão (President)

Rua de São Bento, 148-3° | 1200-821 LISBON | http://www.cnpd.pt | Tel: 213 928 400 | Fax: 213 976 832