Deliberation 2019-057 of May 9, 2019 National Commission for Computing and Liberties Legal status: In force Date of publication on Légifrance: Saturday July 20, 2019 NOR: CNIL1920561X Deliberation No. 2019-057 of May 9, 2019 adopting a reference system relating processing of personal data implemented for the purposes of managing health vigilance

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 April 27, 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

Considering the law n° 78-17 of January 6, 1978 modified relating to data processing, files and freedoms, in particular its article 54-II;

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;

After having heard Mrs. Valérie PEUGEOT, commissioner, in her report and Mrs. Nacima BELKACEM, government commissioner, in her observations,

Adopts the reference system relating to the processing of personal data implemented for the purposes of managing health vigilance appended to this deliberation.

Decides that the reference system relating to the processing of personal data implemented for the purposes of managing health vigilance comes into force the day after its publication in the Official Journal of the French Republic.

Resolves that any modification made to the processing of personal data which would have been duly constituted prior to the date of entry into force of this reference system and which would be in compliance with it requires the data controllers concerned to make a declaration of compliance.Appendix

ANNEX

FRAMEWORK RELATING TO THE PROCESSING OF PERSONAL DATA IMPLEMENTED FOR HEALTH VIGILANCE MANAGEMENT PURPOSES

1. Who is this reference intended for?

This standard exclusively governs the processing of personal data:

- set up to manage health vigilance;

- and implemented by manufacturers, companies, operators, organizations responsible for marketing a drug, device or product and referred to below as data controllers.

By application of the provisions of 1° of article 65 of the amended law of 6 January 1978, the processing of personal data implemented by health professionals and health care systems or services (eg. : health establishments, nursing homes, health centers, health agencies, etc.) are not concerned by this standard.

2. Scope of the standard

This repository specifies the legal framework, resulting from the General Data Protection Regulation (GDPR) and national provisions, applicable to the processing of personal data constituted in the context of health vigilance. It covers the scope of the health vigilance mentioned in the decree of February 27, 2017 setting the list of categories of adverse health events for which the declaration or report can be made using the portal for reporting adverse health events.

Data controllers who send the CNIL a declaration of compliance, for the processing of personal data meeting the requirements set by this standard, via the declaration of compliance form to be completed on the CNIL website, are authorized to implement them.

Any processing of personal data that exceeds the scope or requirements defined by these standards must, however, be the subject of a request for specific authorization in accordance with the provisions of article 66-III of the law of January 6 1978 modified.

Data controllers must implement all appropriate measures (technical and organizational) to guarantee the protection of the personal data processed, both from the design of the processing and by default. They must also demonstrate this compliance throughout the life of the treatments. The processing implemented within the framework of the reference system must also be recorded in the register of processing activities provided for in Article 30 of the GDPR (see the model registers on the cnil.fr website).

The principles set out by the CNIL, in this reference system, constitute an aid to carrying out the data protection impact analysis that the data controllers concerned must carry out. Data controllers will thus be able to define the measures allowing them to ensure the proportionality and necessity of their processing (points 3 to 7 of the reference system), to guarantee the rights of individuals (points 8 and 9 of the reference system) and control of their risks (points 10 to 12 of the guidelines).

3. Objective(s) pursued by the processing (PURPOSES)

Processing implemented for the purpose of managing health vigilance is intended to enable the prevention, monitoring, evaluation and management of adverse health events implemented by the data controller.

The processing aims to allow:

- the collection, recording, analysis, monitoring, documentation, transmission and storage of data relating to all adverse health events;

- the management of contacts, by the data controller, with the person who notified him of the adverse health event (member of an approved association, health professional, member of a health authority, patient, etc.) or the professional who may be questioned to obtain, in compliance with medical secrecy, details of the adverse health event reported (professional following the person who suffered the adverse health event, etc.).

The information collected for these purposes cannot be reused to pursue a purpose other than that provided for in this reference system.

4. Legal basis(s) of processing

In the context of health vigilance falling within the scope of this standard, compliance with the legal obligations imposed on the controller by the health vigilance systems provided for in particular by the Public Health Code is retained as the legal basis for the processing of personal data. trained staff.

The collection of health data in the context of health vigilance is necessary for reasons of public interest; its main objective is to ensure compliance with high standards of quality and safety of health care and medicines, devices or products in accordance with the provisions of Article 9 of the GDPR and Article 66 of the Law of January 6, 1978 amended.

5. Personal data concerned

Only data relevant to the purpose of the processing, namely the management of health vigilance, can be collected and processed. As such, the data controller may collect and process, depending on the objective pursued by the processing and the situations:

a) The data relating to the exposed person strictly necessary for the assessment of the adverse health event:

- data making it possible to indirectly identify the person exposed to the adverse health event (identifying information such as age, year or date of birth, sex, weight, height) or identification number of the person (alphanumeric code, alphabetical

identification code as provided for by the existing forms) making it possible to guarantee respect for his private life, excluding the registration number in the national identification directory of natural persons and the national health identifier;

- data relating to the identification of the product concerned by the report of the adverse health event: type of medicine, device or product used, serial number, etc. ;

- health data, in particular: treatments administered, results of examinations, nature of the undesirable effect(s), personal or family history, associated illnesses or events, risk factors, information relating to the method of prescription and use of medicines and to the therapeutic conduct of the prescriber or health professionals involved in the management of the disease or adverse health event.

In addition to these data, the data controller may also collect and process other data provided that they are strictly necessary for the assessment of the adverse health event (professional life, consumption of tobacco, alcohol, drugs, habits life and behavior). Data relating to ethnic origin may be collected by the controller when a document presenting the characteristics of the medicinal product, device or product validated by a competent authority (e.g.: summary of product characteristics for medicinal products, summary of the characteristics of the medical device, etc.) states, based on scientific work, the fact that the ethnic origin of the person may have an impact on its effectiveness or safety.

b) The contact details of the person who notified the adverse health event or of any health professional likely to provide further details (surname, first name, postal, electronic, telephone contact details, if necessary specialty of the health professional ).

Depending on the situation, the person who made the notification may be: the member of a health authority, a health professional, the person exposed to the adverse health event or his entourage, the holder(s) of the parental authority, beneficiary in the event of death, an approved patient association, etc. The notification of the adverse health event, which would be carried out directly by the exposed person, has the effect of lifting the secrecy of his identity, and must be limited to what the data controller needs to know in order to meet his obligations in in terms of health vigilance and for a period strictly limited to what is necessary to meet the said obligations.

6. Data recipients

Only authorized employees of the data controller should be able, under the latter's responsibility, to access the personal data processed, within the limits of their respective powers and as far as they are concerned, in particular:

- the vigilance manager, as well as his collaborators and agents involved in the health vigilance management process;

- the staff of the audit department, on a timely and motivated basis, to verify compliance with regulatory requirements;

- authorized personnel in charge of complaints management, depending on the files they have to deal with.

The following may also be recipients of the data necessary for the exercise of their missions, exclusively within the framework of their vigilance activity:

- subcontractors working on behalf of and under the responsibility of the organization, within the limits of their functions and under the conditions defined by the subcontracting contract. In the event of recourse to a subcontractor, the contract which binds the data controller to the subcontractor must mention the obligations incumbent on him in terms of data protection (article 28 of the GDPR). The subcontractor's guide published by the CNIL specifies its obligations and the clauses to be included in the contracts;

- the other companies of the group to which the organization belongs which participate in the exploitation or marketing of the medicinal product, device or product in question;

- third parties whose medicine, device or product could be implicated, with the exception of data directly identifying the person exposed to the adverse health event who notified the event;

- the healthcare professionals involved in monitoring the patient and the healthcare professionals or other professionals who can provide additional information;

- the notified bodies in charge of evaluating a medicinal product, device or product, with the exception of data directly identifying the person exposed to the adverse health event who would have notified the event;

- national public bodies (e.g.: regional health agencies, health agencies, etc.) or foreign ones in charge of vigilance within the framework of the exercise of their missions as defined by the texts, the health authorities or agencies foreign national authorities and international health authorities or agencies (eg European Medicines Agency), with the exception of data directly identifying the person exposed to the adverse effect who reported the event.

7. Storage periods

The data collected and processed to manage health vigilance cannot be kept indefinitely. A precise retention period must be set beforehand depending on the purpose of the processing.

With regard to the purposes of the processing, the data is kept in an active database for the duration of current use of the data. They are then kept in intermediate archiving for the legal or regulatory period applicable to each health vigilance. In the

absence of a legal or regulatory duration, the data cannot be kept beyond a period of seventy years from the date of withdrawal from the market of the drug, device or product.

At the end of these periods, the data is deleted or archived in an anonymized form.

The retention and archiving of data must be carried out under security conditions in accordance with the provisions of Article 32 of the GDPR.

8. Information of persons

Processing of personal data must be implemented in complete transparency vis-à-vis the persons concerned (persons exposed to the adverse health event, person who notified the adverse health event and health professional who followed the person concerned by the event). The data controller takes the appropriate measures to provide the data subject with concise, transparent, understandable and easily accessible information, in clear and simple terms.

From the collection stage, the persons concerned by the processing must be individually informed of the methods of processing their data under the conditions provided for by Articles 13, where applicable, 14 of the GDPR, 69 and 70 of the Data Protection Act. .

In the event of notification of the adverse health event by the person who is exposed to it, specific information must be provided to him beforehand, in order to inform him that the secrecy of his identity will not be preserved.

The information support is free (oral or written).

If the data subject so requests, he or she may obtain the provision of written information support.

In the event of notification of the adverse health event by a person other than the person exposed to it, the information is produced by the notifier on the basis of the written information provided by the data controller to the notifier.

The data controller must at all times justify that the information of the persons concerned has been delivered, it being up to the data controller to obtain proof of this delivery from the notifier.

Data subjects must also be informed of how to exercise their rights.

9. Rights of persons

The persons concerned by the processing (persons exposed to the adverse health event, person having notified the adverse health event and health professional having followed the person concerned by the event) have the following rights, which they exercise under the conditions provided by the GDPR:

- permission to access ;

- right of rectification;

- right to limit processing (for example, when the person disputes the accuracy of their data, they can ask the data controller to temporarily freeze their data while they carry out the necessary checks).

Insofar as the processing is based on compliance with a legal obligation, the persons concerned by the collection of the data have neither the right of opposition, nor the right to erasure of the data, nor the right to portability. Datas. The persons concerned are informed in advance.

10. Security

In general, the data controller must take all necessary precautions with regard to the risks presented by its processing to preserve the security of personal data and, in particular at the time of their collection, during their transmission and their storage, prevent that they are deformed, damaged or that unauthorized third parties have access to them.

In particular, in the specific context of this standard, either the data controller adopts the following measures, or he justifies their equivalence or the fact of not needing or being able to use them:

Categories

Measures

Train users

Inform and raise awareness of the people handling the data

Write an IT charter and give it binding force

Authenticate users

Define a unique identifier (login) for each user

Use a strong authentication method, based on a verified directory

Adopt a user password policy in accordance with the recommendations of the CNIL

Force user to change password after reset

Limit the number of attempts to access an account

Manage authorizations

Define authorization profiles

Remove obsolete access permissions

Carry out an annual review of authorizations

Trace access and manage incidents

Provide a logging system

Inform users of the implementation of the logging system

Protect logging equipment and logged information

Provide procedures for personal data breach notifications

Securing workstations

Provide an automatic session locking procedure

Use regularly updated anti-virus software

Install a software firewall

Obtain the user's agreement before any remote intervention on his workstation

Securing Mobile Computing

Provide encryption means for mobile equipment

Make regular data backups or synchronizations

Require a secret to unlock smartphones

Protect the internal computer network

Limit network flows to what is strictly necessary

Securing the remote access of mobile computing devices by VPN

Implement WPA2 or WPA2-PSK protocol for Wi-Fi networks

Securing servers

Limit access to administration tools and interfaces to authorized persons only

Install critical updates without delay

Ensure data availability

Securing websites

Use the TLS protocol and verify its implementation

Check that no password or identifier passes in the URLs

Check that user input matches what is expected

Put a consent banner for tracers (cookies) not necessary for the service

Back up and plan for business continuity

Make frequent backups of data, whether in paper or electronic form.

Store backup media in a safe place

Provide security means for the transport of backups

Plan and regularly test business continuity

Archive securely

Implement specific access procedures for archived data

Securely destroy obsolete archives

Supervise the maintenance and destruction of data

Record maintenance interventions in a logbook

Supervise by a person in charge of the organization the interventions by third parties

Erase data from any hardware before disposal

Manage subcontracting

Include a specific clause in subcontractor contracts

Provide the conditions for restoring and destroying data

Ensure the effectiveness of the guarantees provided (security audits, visits, etc.)

Secure exchanges with other organizations

Send data encrypted (either by directly encrypting the data or using an encrypted tunnel)

Make sure it's the right recipient

Transmit the secret in a separate send and through a different channel

Protect the premises

Restrict access to the premises by means of locked doors, whether to paper files or computer equipment, in particular servers.

Install intruder alarms and check them periodically

Supervise IT developments

Offer privacy-friendly settings to end users

Avoid comment boxes or strictly frame them

Test on fictitious or anonymized data

Use cryptographic functions

Use recognized algorithms, software and libraries

Store secrets and cryptographic keys securely

To do this, the data controller may usefully refer to the Personal Data Security Guide published by the CNIL.

Any data breach must be notified to the CNIL under the conditions provided for in Article 33 of the GDPR.

It is requested that, in the event of recourse to an external service provider for the storage and retention of personal health data by the data controller, this service provider must be an approved or certified health data host. By way of exception, when the data controller is not established in France, the data controller must demonstrate that the service provider he uses offers equivalent security guarantees.

The use of the services of a subcontractor must be made under the conditions provided for in Article 28 of the GDPR.

11. Transfer of data outside the European Union

Indirectly identifying data of persons exposed to an adverse health event and directly identifying data of persons who notified the adverse health event may be transferred outside the European Union if the following conditions are met:

- the provisions of article 6 relating to the recipients of the data are respected;

- the transfer of data is strictly necessary for the implementation of the vigilance system.

The transfer can be carried out within the framework of the declaration of conformity with this standard when one of the following conditions is met:

- the transfer is made to a country or an international organization recognized by the European Commission as providing an adequate level of protection, in accordance with Article 45 of the GDPR (adequacy decision);

- the transfer takes place subject to appropriate safeguards, listed in Article 46(2) of the GDPR (in particular: standard contractual clauses approved by the European Commission, binding corporate rules, code of conduct, certification mechanism);

- in the absence of an adequacy decision or appropriate safeguards, the transfer may be based on one of the exceptions provided for in Article 49 of the GDPR when such a transfer is not repetitive, massive or structured .

The data controller must have previously informed the persons concerned of the transfer of their personal data to countries outside the European Union, of the existence or absence of an adequacy decision or appropriate guarantee and ways to obtain a copy in accordance with Article 13(1)(f) GDPR.

12. Data Protection Impact Assessment (DPIA)

In accordance with Article 35 of the GDPR, the controller must carry out a data protection impact analysis.

To carry out its impact analysis, the data controller may refer to:

- the principles contained in this reference system;

- the methodological tools offered by the CNIL on its website.

Where appropriate, the Data Protection Officer (DPO) should be consulted.

In accordance with Article 36 of the GDPR, the data controller must consult the CNIL prior to the implementation of the processing if, following the impact analysis, he is unable to identify sufficient measures to reduce risks to an acceptable level (residual risk remaining too high).

The president,

M. L. Denis