Deliberation 2020-081 of June 18, 2020Commission Nationale de l'Informatique et des LibertésLegal status: In force Date of publication on Légifrance: Wednesday July 29, 2020NOR: CNIL2019851XDeliberation no. personal data intended for the management of medical and paramedical practicesThe 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;

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

Having regard to the public health code;

Having regard to decree n° 2019-536 of May 29, 2019 as amended, taken for the application of 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 intended for the management of medical and paramedical practices, which will be published in the Official Journal of the French Republic.

RELATING TO THE PROCESSING OF PERSONAL DATA INTENDED FOR THE MANAGEMENT OF MEDICAL AND PARAMEDICAL PRACTICESTable of contents1. Who is this reference for?

11. Additional measures: Impact analysis and Data Protection Officer1. Who is this reference for?

This reference system, taken pursuant to the provisions of article 8-I-2-b of the law of January 6, 1978 as amended, governs the implementation of the processing of personal data by the medical and paramedical professions within the framework of the medical and administrative management of their patients.

It is aimed at health professionals practicing in a liberal capacity.

It does not apply to treatments implemented by healthcare services (health establishments, health centres, territorial professional health communities, etc.), nor to those implemented by the medical services of public entities. or private (occupational medicine, school medicine, PMI, etc.), by pharmacists, by medical biology analysis laboratories or by opticians.2. Scope of the repository

Processing aimed at enabling medical and administrative management within medical and paramedical practices, whether implemented using internal tools or outsourced to a service provider, leads to the collection of data relating to persons identified or identifiable individuals (patients, healthcare professionals, etc.). As such, they are subject to the provisions of the general data protection regulations (RGPD), the law of 6 January 1978 as amended (LIL) as well as the provisions of the public health code.

The healthcare professionals concerned, as data controllers, must implement all appropriate technical and organizational measures to guarantee a high level of protection of personal data from the design of the processing operations and throughout the life of the processing operations. this. They must also be able to demonstrate this compliance at any time.

The processing carried out by healthcare professionals must be entered in the register provided for in Article 30 of the GDPR (see register model in the practical guide for doctors).

This reference has no binding value. In principle, it makes it possible to ensure the compliance of the data processing carried out by healthcare professionals practicing in a liberal capacity with the principles relating to data protection and medical secrecy, in a context of changing practices in the era digital.

Healthcare professionals who deviate from the standard with regard to the particular conditions relating to their situation must be able to justify the existence of such a need, then take all appropriate measures to guarantee the compliance of the treatments with the personal data protection regulations

The repository is not intended to interpret the rules of law other than those relating to the protection of personal data. It is up to

the players concerned to ensure that they comply with the other regulations which may also apply.

This reference also constitutes an aid to the realization of an impact analysis relating to data protection (DPIA) in the event that this is necessary.

The CNIL regularly publishes practical guides to support professionals in the implementation of the obligations provided for by the new regulations on the protection of personal data, which they are invited to consult in addition to this reference document

(1).3. Objective(s) pursued by the processing (purposes)

The processing implemented must meet a specific objective and be justified with regard to the missions and activities of the healthcare professional.

It is implemented in order to allow the exercise of prevention, diagnosis and care activities as well as administrative management.

It allows in particular, for the needs of patient care:

- the management of appointments;
- management of medical records;
- the management and keeping of the files necessary for the follow-up of the patient;
- the use of remote care practices requiring information and communication technologies, such as telemedicine and telecare;
- communications between identified professionals and care structures involved in the care of the person concerned and in the coordination of the latter;
- the establishment and electronic transmission of documents intended for the payment of health costs by the health insurance (treatment sheets, work stoppage, electronic treatment protocol, etc.);
- bookkeeping.

Personal health data may only be used in the direct interest of the patient or the management of the medical practice, under the conditions determined by law, for the needs of public health and the obligations of health professionals.

They can be reused for studies when they are carried out by the personnel monitoring the patient and intended for their exclusive use. Failing this, they must be the subject of formalities in application of articles 72 and following of the Data Protection Act relating to processing for the purposes of research, study or evaluation in the field of health.4. Legal basis(s) of processing

Each purpose of the processing must be based on one of the legal bases set by the regulations (see The lawfulness of the processing: the essentials on the legal bases provided for by the GDPR).

It is up to the data controller to determine these legal bases before any processing operation, after having carried out a reflection, which he can document, with regard to his specific situation and the context. Having an impact on the exercise of certain rights, these legal bases are part of the information that must be brought to the attention of the persons concerned.

In order to help healthcare professionals in this analysis, this standard offers, for information purposes, a choice of legal basis for each purpose in the table below (2).

Purposes

Possible legal bases (3)

Maintaining medical records

Legal obligation

Establishment and electronic transmission of documents for health insurance

Legal obligation

Keeping the health care file (such as the nursing care file)

Legal obligation

Appointment booking

Legitimate interest

Bookkeeping

Legitimate interest

Telemedicine (art. L. 6316-1 of the CSP), telecare (art. L. 6316-2 of the CSP)

Legitimate interest5. Personal data concerned

Principle of relevance, fairness and minimization of data

In order to minimize the personal data processed, the healthcare professional must take care to collect and use only the relevant and necessary data with regard to his own treatment needs for the medical and administrative management of his patient population. The following data are in principle considered relevant, for the purposes mentioned above:

a) The identity and contact details of the patient (such as surname, first name, date of birth, postal address, e-mail address

and telephone number);

b) The national health identifier (INS) for the health or medico-social care of a patient;

c) The social security number for billing purposes and financial coverage of health expenses;

d) Family status (such as marital status, number of children);

e) Professional status (such as occupation, working conditions);

f) Health (such as weight, height, medical history, medical diagnoses, therapy followed, treatments prescribed, nature of procedures performed, test results, biological, physiological and condition likely to influence the patient's reaction to his medical care and any element likely to characterize the patient's health and considered relevant by the healthcare professional);

g) Information relating to lifestyle habits depending on the context, when collected with the consent of the patient and necessary for the diagnosis and care of the patient (such as relating to dependence [alone, in an institution, independent, bedridden], assistance [domestic, family help], physical exercise [intensity, frequency, duration], diet and eating habits, leisure);

h) Functional traces (those which report on the business actions of users or machines within the information system) and technical traces (those which report on the activity of the software and hardware components used by the information system to ensure the functionality requested by a user or a machine).

After ensuring the necessity and relevance of the personal data they use, the healthcare professional must also check, throughout the lifetime of the processing, the quality of the data they process. This means in practice that according to the regulations, the data must be updated.6. Recipients and access to information

The following persons may be required to access patient data for the performance of their duties and under legislative provisions:

- health professionals and professionals contributing to prevention and care, in order to ensure continuity of care in compliance with the provisions of Articles L. 1110-4 and L. 1110-12 of the Public Health Code, including including via access to the shared medical file and to the digital health space;

- the persons in charge of the secretariat, who must only have access, in compliance with the provisions on professional secrecy, to the information necessary for the performance of their duties, i.e. to information relating to the management of the

office and in particular the management of appointments as well as certain information of a medical nature under conditions strictly limited to what is necessary for the exercise of their missions and under the control of the health professional;

- in order to allow the reimbursement of acts, services and their control, the staff of the health insurance organizations, who are aware, within the framework of their functions and for the duration necessary for the accomplishment of these, of the the identity of the insured, his social security number and the code number of the acts and services performed and the pathologies diagnosed under the conditions defined in article L. 161-29 of the social security code;

- the staff of complementary health insurance organizations, authorized by their function to process health data, in particular the identity of their insured persons, their social security number and in the form of grouped codes, categories of acts and services performed;

- research organizations in the field of health and organizations specializing in the evaluation of care practices, which may be recipients of personal health data under the conditions defined by the GDPR and the law of January 6, 1978 as amended (in particular respecting the principle of data minimization).

In the event of recourse to a service provider to ensure the maintenance of the software and the workstations managing the patient files, the latter accesses the personal data in compliance with medical secrecy. The data must be protected by physical and logical means, such as encryption, in order to allow the technician to carry out his missions without being able to read this data.

When the patient file management software is accessible remotely and is hosted by a service provider (generally the software publisher, an online appointment booking platform or a telemedicine platform) or if the storage of patient data patient's health is entrusted to a service provider responsible for ensuring its storage in remote servers (for example, a backup or hotline service provider), this service provider must be an approved or certified host for hosting, storage, the retention of health data in accordance with the provisions of Article L. 1111-8 of the Public Health Code.

If an online appointment booking platform is used, a clear distribution of responsibilities should be made according to the services offered.

In any case, as soon as a service provider is requested to process personal data on behalf of the healthcare professional (maintenance company, online platform, approved or certified healthcare data host), this service must be carried out under the conditions provided for in Article 28 of the GDPR. A subcontracting contract must be concluded between the service provider

and the data controller. It must mention that the service provider, as a subcontractor:

- only processes personal data on instructions from the data controller;

- ensures that staff sign confidentiality agreements;

- takes all required security measures;

- does not recruit a subcontractor without the prior written authorization of the controller;

- cooperates with the data controller for the respect of his obligations, in particular when patients have requests concerning their data;

- deletes or sends back to the data controller all the personal data at the end of the services;

- makes available to the data controller all the information necessary to demonstrate compliance with the obligations to enable audits to be carried out.

The service provider must, in its capacity as processor, keep a register of processing activities under the conditions of article 30.2 of the GDPR.

The service provider must, in the event of an incident related to the data that it manages on behalf of the data controller (security breach, hacking, loss, etc.) inform it as soon as possible, so that the latter can respect its own incident management and notification obligations (4).7. Storage periods

A precise retention period for the data must be set according to each purpose: this data cannot be kept for an indefinite period.

With regard to the management purposes of the medical or paramedical practice, the data recorded in the application may be kept for a period of twenty years from the date of the last treatment of the patient: on an active basis, for a period of five years from the last intervention on the patient's file, then, at the end of this period, in archived form on a separate medium for fifteen years, under security conditions equivalent to those of the other data recorded in the 'application.

The duplicates of the electronic care sheets must be kept for three months in accordance with article R. 161-47 of the social security code.

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

It is up to service providers providing software solutions to integrate automatic archiving functionalities on a due date.

Otherwise, the healthcare professional will do it manually.

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

32 of the GDPR.

To find out more, you can refer to the CNIL guides:

- Security: Archive securely;

- Limit the retention of data.

Data used for statistical purposes are no longer qualified as personal data once they have been duly anonymised (see EDPS guidelines on anonymisation); pseudonymization is not anonymization: erasing the surnames and first names of the persons concerned is not enough to anonymize the data.8. Information of people

Processing of personal data must be implemented in complete transparency vis-à-vis the persons concerned.

Thus, from the stage of collecting personal data, individuals must be informed of the procedures for processing their data under the conditions provided for in Articles 12, 13 and 14 of the GDPR (see practical guide for doctors).

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

The persons whose data are recorded and stored in the processing of personal data by the health professional are informed by posting on the premises of the medical or paramedical practice or by the delivery of a specific document, in particular in the context of home visits (such as a pamphlet given to the patient or made available in the waiting room or an email confirming an appointment).9. Rights of persons

Data subjects have the following rights, which they exercise under the conditions provided for by the GDPR (see the section dedicated to rights):

- right to object to the processing of their data, subject to the conditions for exercising this right pursuant to the provisions of Article 21 of the GDPR: thus, for example, the right of opposition will not apply in the medical file;

- right of access to their patient file, and to all data concerning them in general;

- right of rectification of the data concerning them, if they are inaccurate;

- right to erase data concerning them subject to the conditions for exercising this right pursuant to the provisions of Article 17 of the GDPR;

- right to restriction of processing. For example, when the person disputes the accuracy of their data, they can ask the healthcare professional to temporarily freeze the processing of their data, while the latter carries out the necessary checks on their request.

It should be noted that the choice of a legal basis for processing conditions the existence of certain rights (https://www.cnil.fr/fr/la-liceite-du-traitement-lessentiel-sur-les-bases- legal-provided-for-by-the-gdpr). Thus, keeping a medical file meets a legal obligation. The patient cannot therefore object in principle to the processing of his personal data, in accordance with the provisions of Article 21 of the GDPR.10. Security

The healthcare professional must take all necessary precautions with regard to the risks presented by his processing to preserve the security of personal data and, in particular at the time of their collection, during their transmission and their storage, to prevent them from being distorted, damaged or that unauthorized third parties have access to it. To do this, the data controller may usefully refer to the Personal Data Security Guide.

In accordance with Article L. 1110-4-1 of the Public Health Code, the healthcare professional must ensure that the information systems, services or digital tools that he uses comply with the security standards (5) and interoperability (6) approved by order of the Minister for Health. He must also respect the safety instructions concerning him provided by the latter.

In particular, in the specific context of this standard, the organization is invited to adopt the following measures, to justify their equivalence or the fact that their implementation is not necessary:

Categories

Measures

Educate users

Inform and raise awareness among firm staff accessing the data

For a firm pooling IT resources, draft an IT charter and give it binding force

Authenticate users

Define an identifier (login) specific to each user

Adopt a user password policy that complies with the

CNIL recommendations (7)

For users accessing health data, use strong authentication via their healthcare professional card (CPS) or any alternative two-factor means

Maintain the CPS at a strictly personal level, without communicating the secret code to the practice staff (e.g.: medical secretary) (8)

Manage authorizations

Assign an authorization profile adapted to each user (distinguishing in particular between administrative data and medical data)

Remove obsolete access permissions

Inform users of the implementation of the logging system

Provide procedures for personal data breach notifications

Securing workstations

Provide an automatic computer session locking procedure

Allow regular antivirus updates

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

Limit the storage of medical information on a tablet or smartphone (because of the consequences for patients in the event of theft or loss of the equipment). If this equipment is used, their level of data security must be equivalent to that of other equipment (encryption, access codes, etc.)

Require a secret to unlock smartphones or tablets

Protect screens from prying eyes (orientation, optical filter)

Limit the use of removable storage media (USB keys, external hard drives) and systematically encrypt sensitive data stored there

Do not lend a smartphone or tablet for professional use

Protect the internal computer network

Limit connections from non-work devices on the network

Securing servers

Limit access to administration tools and interfaces to authorized persons only

Allow installation of critical updates without delay

Back up and plan for business continuity

Perform or allow regular backups to be performed

Store backup media in a safe place

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 firm manager interventions by third parties

Erase data from any hardware before disposal

Manage subcontracting

Include specific clauses in subcontractor contracts

Provide conditions for the return and destruction of data

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

Secure exchanges with other health professionals and with patients

Make sure it is the right recipient

Use secure electronic health messaging for exchanges between health professionals

For discussions with other professionals involved in the care of the patient or with the patients themselves:

- encrypt the data before sending it to standard electronic messaging (9) and transmit the secret by a separate transmission and via a different channel;

- use a transfer protocol guaranteeing the confidentiality of messages and the authentication of the messaging server;

- choose a messaging system hosting the data in a country or with a service provider guaranteeing data protection in accordance with European rules.

Protect the premises

Restrict access to premises with locked doors

Install intruder alarms and check them periodically

Secure the storage of files in paper format (secure premises, lockable cabinet)

Retrieve printed documents containing data immediately after they are printed or, when possible, perform secure printing

Destroy paper documents containing data that are no longer useful using an appropriate shredder (certified at least class 3 of

the DIN 32757105 standard) In the event of outsourcing of data hosting, IT service providers must be approved or certified for the hosting, storage and retention of health data in accordance with the provisions of Article L. 1111-8 of the Public Health Code.

Service providers responsible for developing and maintaining the software and workstations managing patient files or offering an appointment platform are invited to adopt the following measures, under the control of the data controller:

Categories

Measures

Educate users

Inform and raise awareness among firm staff accessing the data

For a firm pooling IT resources, contribute to the drafting of an IT charter

Authenticate users

Define an identifier (login) specific to each user

Integrate a user password policy in accordance with the recommendations of the CNIL (10)

Force user to change password after reset

Limit the number of attempts to access an account

For users accessing health data, require a

strong authentication via their healthcare professional card (CPS) or any alternative two-factor means

Manage authorizations

Integrate authorization profiles distinguishing in particular between administrative data and medical data

Remove obsolete access permissions

Carry out an annual review of authorizations

Limit the distribution of paper documents containing health data to people who need to have them as part of their activity

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 computer session locking procedure

Implement regularly updated anti-virus software

Install a software firewall

Encrypt stored data

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

Securing Mobile Computing

For remote access to patient files, respect the interoperability and security standards provided for in Article L. 1110-4-1 of the Public Health Code

Protect screens from prying eyes

Limit the use of removable storage media (USB keys, external hard drives) and systematically encrypt sensitive data stored on them

Provide backup measures and regular synchronization of data

Protect the internal computer network

Limit network flows to what is strictly necessary (block protocols and ports that are not used)

Limit connections from non-work devices on the network

Securing the remote access of mobile computing devices with a VPN

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

Securing servers

Limit access to administration tools and interfaces to authorized persons only

Encrypt stored data

Install critical updates without delay

Ensure data availability

Securing websites

Use the TLS protocol and verify its implementation

Check that no password or username is embedded in URLs

Back up and plan for business continuity

Schedule regular backups

Plan to store backup media in a safe place

Provide security means for the transport of backups if necessary

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

Physically erase data from any hardware before disposal

Manage subcontracting

Include specific clauses in the contract with the data controller

Provide conditions for the return and destruction of data

Allow the data controller to ensure the effectiveness of the guarantees provided (security audits, visits, etc.)

Secure exchanges with other organizations

Provide secure electronic health messaging for exchanges between health professionals

For discussions with other professionals involved in the care of the patient or with the patients themselves:

- provide for the encryption of the data before they are sent to standard electronic messaging (11) and the transmission of the secret code by a separate sending and via a different channel;

- use a transfer protocol guaranteeing the confidentiality of messages and the authentication of the messaging server;

- choose a messaging system hosting the data in a country or with a service provider guaranteeing data protection in accordance with European rules

Supervise IT developments

Offer default privacy-friendly settings to end users

Avoid free comment areas or strictly frame them

Test on fictitious or anonymized data (and not just pseudonymized)

Use cryptographic functions

Use recognized algorithms, software and libraries

Store secrets and cryptographic keys securely11. Complementary measures: Impact analysis and Data Protection Officer

The CNIL considers that the completion of a DPIA and the appointment of a data protection officer (DPO) should be necessary for health professionals who, practicing in a grouped practice, share a common information system, from an annual threshold of 10,000 patients.

To carry out an impact study, the data controller may refer to:

to the principles contained in this reference document,

the methodological tools offered by the CNIL on its website.

In accordance with Article 28 of the GDPR, the processor must provide the data controller with any information necessary to carry out this analysis.

(1) For example, the guide written jointly by the CNOM and the CNIL for doctors.

(2) Other legal bases, such as contract or public interest, could also apply.

(3) Subject to different choices justified by a specific context.

(4) https://www.cnil.fr/fr/notifications-dincidents-de-securite-aux-autorites-de-regulation-comment-sorganiser-et-qui-sadresse.

(5) https://esante.gouv.fr/securite.

(6) https://esante.gouv.fr/interoperabilite.

(7) https://www.cnil.fr/fr/authentication-par-mot-de-passe-les-mesures-de-securite-elementaires.

(8) It is possible to set up strong authentication for firm personnel, for example by means of a single-use password (username, password and sending of a code at each connection) or means of an establishment staff card (CPE, to be requested from the Digital Health Agency).

(9) Instant messaging (chat) must be used with the utmost care and in a secure manner.

(10) https://www.cnil.fr/fr/authentification-par-mot-de-passe-les-mesures-de-securite-elementaires.

(11) Instant messaging or chat should be used with the utmost care and in a secure manner.

The president,

M. L. Denis