AZ JAN PORTAELS
Algemeen Ziekenhuis Vilvoorde

PATIENT PRIVACY REGULATIONS

AZ JAN PORTAELS

Publication date

10/10/2022

Version 1.0

Article 1. Objective

The non-profit making organisation Algemeen Ziekenhuis Jan Portaels, with its registered office at 1800 Vilvoorde, Gendarmeriestraat 65 and with company number 0267.386.438 (hereafter "the Jan Portaels General Hospital") attaches great importance to protecting the privacy of its patients. With these privacy regulations, the Jan Portaels General Hospital wishes to inform its patients as fully as possible about how the hospital handles the personal data it collects and processes about them. Among other things, these privacy regulations clarify the way in which patients' personal data are processed at the hospital and how patients can exercise control over this processing of their personal data.

These regulations were made in implementation of applicable regulations, including:

- the Coordinated Act of 10 July 2008 on Hospitals and Other Care Facilities (hereinafter the "Hospital Act") and Annex A. III. Article 9quater of the Royal Decree of 23 October 1964 determining the standards to be observed by hospitals and their services; and
- the Regulation EU No 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data ('GDPR'), and its implementing laws and acts.

Article 2. Definitions

For the purposes of these regulations, the following definitions shall apply:

- **Personal data**: any form of information relating to an identified or identifiable natural person, such as a patient. An identifiable natural person is considered to be one who can be identified, directly or indirectly, in particular by means of an identification number (e.g. the National Register number), location data, an online identifier (e.g. an IP address) or one or more elements characterising his or her physical, physiological, psychological, economic, cultural or social identity;
- **Personal data on health**: personal data relating to the physical or mental health of a natural person, including data on health services provided that provide information on their health status;
- **Anonymous data**: any data that cannot (no longer) be associated with an identified or identifiable person and is therefore not (no longer) personal data;
- **Pseudonymised personal data**: personal data processed in such a way that they can no longer be linked to a specific natural person without the use of additional data, provided that such additional data are kept separately and technical and organisational measures are taken to ensure that the personal data are not linked to an identified or identifiable natural person. It is therefore not anonymous data, as the natural person is still identifiable after pseudonymisation;
- **File**: any structured set of personal data, compiled and held in a logically structured manner that allows systematic consultation, whether centralised, decentralised or dispersed in a functional or geographical manner;
- **Processing**: any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, as well as blocking, erasure or destruction of personal data;
- **Controller**: the natural person, legal entity, public authority, agency or other body which alone or jointly with others determines the purposes and means of processing personal data;

- **Processor**: the person authorised under the authority of the controller to process the data;
- **Processor**: the natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller, without being under the direct authority of the controller;
- **Recipient**: the natural or legal person, public authority, agency or other body to whom/to which personal data are disclosed;
- **Patient**: the natural person, admitted or treated at the hospital;
- **Patient consent**: any freely given, specific, informed and unambiguous expression of will by which the patient or his legal representative accepts, by means of a statement or unambiguous active act, that personal data concerning that patient are processed.

Article 3. Scope of application

These regulations apply to the processing of personal data of patients at Jan Portaels General Hospital as defined in Articles 4, 5 and 6 of these regulations, compiled or performed by its employees and/or independent professionals.

Article 4. Categories of persons whose data are processed

The collection and processing of personal data applies, in accordance with Articles 20 and 25 of the Hospital Act, to all patients of Jan Portaels General Hospital.

Personal data relating to health is collected - by independent professionals and/or hospital employees - from the patient themselves, or is obtained through referring healthcare providers and secure government platforms. A different collection method may impose itself when the patient himself is unable to provide the data or when the purpose of the processing requires it.

Article 5. The nature of the data processed and the manner in which they are obtained

The personal data of patients processed within Jan Portaels General Hospital are as follows:

- **identification data**, including the national register number;
- **financial and administrative data** relating to admission and billing, including health insurance fund membership;
- **medical, paramedical and nursing data**; **social data**;
- **other data** necessary for carrying out the purposes determined or imposed by law (judicial data).

Article 6. Processing purposes and legal framework

§1. Under Articles 6 and 9 of the GDPR, the processing of patients' personal data is possible in the context of, inter alia:

- the provision of healthcare services as referred to in the Law of 22 August 2002 on Patients' Rights;
- the provisions of the Hospital Act (in particular Articles 20 and 25);
- Law on compulsory insurance for medical care, coordinated on 14 July 1994; □ legal claims; or
- an explicit and informed consent of the patient, insofar as the consent to process patient data is required in accordance with Articles 6 and 9 of the GDPR.

Within the limits of this legal framework, the processing of patients' personal data within Jan Portaels General Hospital has one or more of the following purposes in particular in mind:

- **patient care**: performing preventive medicine or making a medical diagnosis, providing (medical, paramedical, nursing and social) care or treatment to the person concerned or a relative or managing health services, in the interest of the person concerned;
- **patient administration**: following up on patients' stay and treatment for billing purposes;
- **patient registration**: the recording of medical and stay data of patients for internal government-mandated purposes, as well as for research and policy purposes;
- **medicines management**: processes related to prescribing and dispensing of medicines;
- **complaint handling**: registering personal data of patients and/or their confidants in order to mediate complaints made. Registering complaints;
- **quality of care**: collection and processing of all data relating to medical and paramedical diagnostic and therapeutic practices administered to patients with the aim of improving quality of care;
- **scientific registration**: the registration of (medical) personal data of an epidemiological, scientific and/or management nature with a view to objectives on research, education or objectives imposed by the federal or regional authorities;
- **organ donation**: the processing of personal data under the Royal Decree of 10 November 2012 on local donor coordination.

§In no event shall personal data other than those necessary for the purposes set out in §1 be included in such processing, nor shall such personal data be further processed in a manner incompatible with those purposes.

Article 7. The controller and persons who may act on behalf of the controller

§General Hospital Jan Portaels is the controller of patients' personal data.

The persons acting on behalf of the controller are the chairman board of directors, general manager and the chief physician of Jan Portaels General Hospital.

In some cases, another person will be jointly responsible with Jan Portaels General Hospital for processing patient data. Where appropriate, patients will be further informed about this.

Article 8. Supervision of the processing of personal data

§1. Personal data on health will be processed in accordance with Article 9(3) GDPR only under the supervision and responsibility of a healthcare professional.

Responsibility for and supervision of the patient files containing health-related personal data rests with the chief physician herein assisted by the nursing director for nursing and paramedical data, and by the finance director for non-medical and non-nursing personal data from the patient files. The final responsibility for complying with the legal obligations in the hospital regarding data protection as a data controller rests with AZJP, represented by the Board of Directors.

§2. A data protection officer (DPO) was appointed within Jan Portaels General Hospital,
data protection officer).

This person is in charge of monitoring all aspects related to the processing of personal data, including the security of personal data and the exercise of patients' rights regarding their personal data. He assists the hospital with advice on all these aspects. He can also be contacted by any patient in connection with all matters relating to the processing of personal data at the Jan Portaels General Hospital via email (ombudsdienst@azjanportaels.be) or by telephone on 02/257.56.54.

Article 9. Patient file processors and their competence

§ Internal consultation and processing of patients' personal data shall be carried out by the persons and within the limits defined in this paragraph.

1. Personal data relating to health will be collected and processed under the direction of the **chief medical officer**.
2. The (independent) **doctors** attached to the hospital are given delegated responsibility for the collection and processing of patients' personal data in the medical services or departments in which they work.
3. The **staff members and independent professionals associated with the** hospital's **various nursing and paramedical services** prepare the processing modules of the patient files for which they respectively have responsibility.
4. The **staff members associated with the kitchen (incl. diet kitchen)** are responsible for processing personal data in the patient files, with a view to individualised meal distribution.

5. The **staff members of the various medical secretariats** are responsible for processing personal data in the patient files, for the purpose of handling medical records.
6. The **staff members of admission planning, administration and billing** are responsible for the execution, storage, retrieval and technical processing of patients' personal data for billing purposes.
7. The **staff members of support services such as the computer and medical records department** are responsible for the technical processing of personal data into anonymised data, both for government-mandated purposes and for internal research and policy purposes, or for the processing of personal data for administrative support for these purposes.
8. **Medical records staff** are responsible for processing personal data in patient files, with a view to digitising paper patient records.
9. **Staff members associated with patient support services** are responsible for processing personal data in patient files for the purpose of follow-up within the social, psychological, palliative or pastoral services, respectively.
10. **Ombuds staff members** are responsible for processing personal data in patient files, as part of the ombuds function.
11. **Staff members associated with the pharmacy** are responsible for processing personal data in patient files, for the purpose of drug distribution.
12. The **information security consultant** and the **data protection officer** process personal data in patient files to the extent that this would be necessary for the performance of their respective assignments.
13. **Students and trainees in the above-mentioned professional groups**, connected to an educational institution, are given limited internal access to (parts of) patient files as described above by professional group as part of their training.

The various processors only have access to those personal data that they absolutely need to perform their tasks on behalf of the controller. In the case of an electronic file, a list can be drawn of who accessed the programme and the information contained in it.

§ 2. All employees and staff of the hospital who need access to patients' personal data for the performance of their duties shall undertake to respect the provisions of these privacy regulations and the GDPR, as well as all other privacy protection principles, when processing and consulting patient files. They also abide by their professional secrecy or equivalent statutory or contractual confidentiality obligation.

Article 10. Transfer of patient data

§1. Within the limits of Articles 6 and 9 GDPR and to the extent necessary for the purposes specified in Article 6 of these privacy regulations, the following categories of recipients are entitled to obtain personal data of patients on behalf of Jan Portaels General Hospital:

- **external treating healthcare providers** of the patient in the context of patient care referred to in Article 6 of these privacy regulations;

- **external suppliers** who perform certain processing for Jan Portaels General Hospital so that Jan Portaels General Hospital can function properly (including IT services, financial, accounting and similar other services, for printing and sending invoices). As these third parties have access to personal data in the context of the services requested by Jan Portaels General Hospital, the necessary technical, organisational and contractual measures have been taken to ensure that personal data are processed and used only for the purposes stated in this statement.
- the **patient's health insurance fund** and the **National Institute for Sickness and Disability Insurance** (Riziv) to the extent imposed by or under the law or with the patient's consent;
- **public authorities** authorised to do so by a government decision;
- **insurance institutions** insofar as imposed by or pursuant to law or with the patient's consent, as well as the hospital's **professional liability insurer** or the professional appointed by the hospital, without the patient's consent, insofar as such communication is necessary for the defence of a right in court or for the institution, exercise or substantiation of a legal claim;
- **concerned patients themselves or their representatives** within the limits of what is stipulated within the Law of 22 August 2002 on Patients' Rights;
- **other bodies**, to the extent imposed by or under the law or with the patient's consent;

§2. If a transfer referred to in §1 of this article means that the patient's personal data is transferred to a country outside the European Union or to an international organisation, the patient will receive additional information on the consequences of this transfer for the security of his personal data.

§3. Outside the cases set out in §1 of this article, only anonymous data may be exchanged with other persons and bodies.

Article 11. The organisation of the circuit of personal data on health to be processed

The organisation of the health personal data circuit to be processed is as follows:

- entering and processing data in the manner and by the persons, as defined in Article 7 of these privacy regulations;
- Transferring records and invoices to insurance institutions, patients and external pricing services;
- transfer of medical data to external treating healthcare providers as part of patient care as referred to in Article 6 of these privacy regulations;
- transmitting the data referred to in Article 92 Hospital Act to the Federal Public Service of Public Health or to the Flemish Community in an anonymised way.

Article 12. Procedure according to which data will be anonymised

Information technology staff are responsible for the technical processing of personal data into anonymised data. This anonymisation means that the personal data are no longer reasonably traceable to an individual patient.

Personal data may/may only be anonymised to the extent that it is established that retaining such personal data is no longer necessary for the intended processing. This includes the following processing operations:

- the transfer of medical data pursuant to Article 92 Hospital Act to the Federal Public Service of Public Health or to the Flemish Community;
- scientific and clinical studies (these studies require ethics committee approval);
- Ombuds service registrations (annual report);
- the reports in the hospital's incident reporting system.

Article 13. Security procedures

All necessary arrangements shall be made to promote the accuracy and completeness of the data recorded. Necessary technical and organisational measures shall also be taken to secure patient records against loss or corruption of the data and against unauthorised access, modification or departure, including pseudonymisation and procedures for testing, assessing and evaluating the effectiveness of security measures. Computerised programmes have access control (a priori) and may also maintain a list of access logging (a posteriori).

Article 14. Retention periods

§1. Subject to any legal requirements, a retention period of at least one year, counting from the patient's last discharge or treatment, applies to personal data that allow identification:

- 30 years for medical records;
- 20 years for nursing data;
- 7 years for billing data from patient files that serve as accounting justification and for duplicate certificates for assistance provided, individual invoice and collective invoice;
- 1 year for settled files of the ombuds service.

§2. If the retention period has expired, the personal data concerned shall be deleted from the files, whether or not by anonymisation, within a period of one year.

§3. However, erasure, whether by anonymisation or otherwise, may be omitted where:

- or the retention is required by a statutory provision;
- whether the preservation is considered reasonably important from a medical point of view or from the point of view of the patient's life expectancy, or from the point of view of defending his legitimate interests or those of his assignees;
- either the custody is agreed between the patient and the attending hospital doctor or, in his absence, the chief physician.

§4. If the data in question have been processed in such a way that tracing back to individual persons is reasonably impossible, they may be kept in anonymised form.

Article 15. Interconnections, links and consultations

The following parts of the patient files are partly electronic, partly manual:

1. Administrative data

- Patient identification details: name, gender, date of birth, unique patient number, national register number, address details, family details, contact addresses;
- Health fund data and other insurance organisations
- Administrative admission and stay data: admission and discharge dates, treating physicians, clinic locations (service-room-bed)
- Social dossier
- Meal distribution
- Various signed accountability documents (e.g. admission statement, room selection form, general conditions)

2. Medical and nursing data

- Critical data (blood group, allergies)
- Physical parameters (weight, height ...)
- Reason for admission, diagnoses
- Interventions and deliveries
- Nursing concerns and observations
- Requests and results (lab, RX, EKG ...)
- Medical reports
- Medication
- Nursing care including the care plan
- Minimum nursing, clinical, psychiatric data (MVG, MKG, MPG)
- Imaging
- Progress notes from various healthcare providers

3. Invoicing and financial data

- Delivered services and products
- Stay data, nursing days, flat rates,
- Patient payment status and insurance organisation
- Debtor data

The interconnections, connections and consultations of these automated components are recorded at the patient level by means of a unique patient number and contact number.

Article 16. Deletion of data

Data from patient files will be deleted:

- upon expiry of the retention period, as stipulated in Article 15 of these privacy regulations;
- in cases determined by or under the law;
- upon the justified request of any interested party; or in accordance with a court decision.

Article 17. Patient's rights and possibilities of defence in the context of privacy protection

§1. Information: At the latest at the time of the collection of personal data relating to the patient, the patient is informed, in accordance with the provisions of the GDPR, about the processing of this data and the legal basis for this data processing via the **admission form**, the **reception brochure** or the Jan Portaels General Hospital **website**. A copy can be obtained via the reception if required.

§2. Copy: Patients who so request shall have the right to inspect and obtain a copy of their patient file and the personal data processed about them by the Jan Portaels General Hospital free of charge from the controller.

§3. Correct & complete: Patients who so request are entitled to have all incorrect or incomplete personal data processed corrected or completed by the controller free of charge. In doing so, the patient may also request that their personal data temporarily not be further processed (except in certain legally defined cases) until the accuracy of their personal data has been verified. Only if the controller establishes that the personal data are indeed incorrect or incomplete should they be corrected or completed.

§4. Transfer: The patient has the right to ask the controller to transfer a copy of his personal data to that patient and/or directly to another institution or person of the patient's choice, and this in a format that allows the personal data to be transferred easily. However, this right only applies to personal data provided by the patient and processed by automated processes solely on the basis of the patient's explicit consent and provided that the transfer does not adversely affect the privacy of others.

§5. Erasure: If the patient believes that his personal data should no longer be processed (e.g. because they are no longer necessary for the purpose of processing or are processed unlawfully), he may request that his personal data be permanently erased. Instead of erasure, the patient may alternatively request that his personal data remain stored, but not further processed (except in certain legally defined cases).

However, the controller is not obliged to delete the personal data if it may or should still be lawfully processed in accordance with the GDPR.

§6. Cessation: unless the processing is necessary for compelling legitimate reasons, the patient may have the processing of his personal data based solely on the legitimate interests of the controller or on the performance of a task carried out in the public interest or in the exercise of public authority, cease by lodging an objection. Pending the response of the controller, the patient may request that such personal data be temporarily not further processed in the meantime (except in a number of legally defined cases).

In any case, any processing for direct marketing purposes can be stopped by the patient by filing an objection.

§7. Restricted processing: Apart from the cases referred to in paragraphs 3, 5 and 6 of this article, patients may also request that their personal data be kept but not further processed (except in a number of legally defined cases) if the controller no longer needs them, but the patient still needs them in the context of legal proceedings.

The legally defined cases where processing may still take place despite the patient's request not to further process their personal data for the time being, as referred to in paragraphs 3, 5, 6 and 9 of this article, are as follows:

- if the patient gives his specific consent;
- if the controller needs the personal data in the context of legal proceedings;
- to protect the rights of another natural or legal person; or
- for important reasons of public interest.

§9. Moreover, the patient who requests it always has the possibility to oppose automated processing of his personal data for the purpose of individual decision-making that produces legal effects or consequences with similar impact for the patient.

The controller is not obliged to comply with this request if it can rely on a legal provision or an explicit consent of the patient.

§10. For the exercise of his rights referred to in paragraphs 2 to 9 of this article, the patient may submit a request to the **ombudsman service** of the General Hospital Jan Portaels, Gendarmeriestraat 65, 1800 Vilvoorde, via mail (ombudsdienst@azjanportaels.be) or by telephone at 02/257.56.54.

Following the submission of the patient's request, the patient will receive an acknowledgement of receipt and the controller will inform the patient as soon as possible and at the latest within one month what action will be taken on the request. In the case of complex or frequent requests, this period may be extended to three months from the submission of the request. In this case, the controller will inform the patient.

If the patient's request is unclear or if there is doubt about the identity of the requester, the controller may request the necessary additional information. If the requester refuses to provide the necessary information, the controller may refuse the request.

The request procedure is free of charge for the patient. However, if the patient's request is manifestly unfounded or if the patient makes excessive use of his rights, in particular if the same request is made excessively repetitively, the controller may refuse the request or charge a reasonable fee according to the administrative costs associated with these requests.

§11. If the patient considers that the provisions of these privacy regulations or of the GDPR are not complied with or has other grounds for complaint regarding the protection of privacy, the patient may also apply directly to:

- The Data Protection Authority. More information at www.gegevensbeschermingsautoriteit.be; and/or the competent court.

Article 18. Entry into force and amendments

Jan Portaels General Hospital reserves the right to amend its privacy regulations at any time.

If significant changes are made to this statement, Jan Portaels General Hospital will also notify patients.