PATIENT PRIVACY POLICY

Article 1 Purpose

UZ Brussel [Brussels University Hospital] attaches great importance to protecting the privacy of its patients. UZ Brussel therefore wants to inform its patients as fully as possible through this Privacy Policy about the way in which the care facility handles the personal data that it collects and processes about them. This Privacy Policy clarifies in particular the way in which the personal data of patients are processed in UZ Brussel and how the patient can exercise control over this processing of his or her personal data.

This policy was drawn up in implementation of:

- the restated Hospitals and Other Care Institutions Act of 10 July 2008 (hereinafter referred to as the "Hospital Act") and Annex A. III. Article 9quater of the Royal Decree of 23 October 1964 defining the standards to be observed by hospitals and their services;
- Regulation EU No. 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (hereinafter referred to as the "GDPR"), and its implementing laws and decrees;
- The Protection of Natural Persons with regard to the Processing of Personal Data Act of 30 July 2018.

Article 2 Definitions

The definitions marked with an asterisk (*) are identical to those contained in the GDPR (Article 4). We hereby reproduce these definitions for the sake of transparency. In the event of a discrepancy between the definitions of this Privacy Policy and the definitions of the GDPR, the definitions of the GDPR shall take precedence.

For the purposes of this policy, the following definitions shall apply:

- **Personal data** (*) means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an on-line identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- **Data concerning health**: data concerning health means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;
- **Anonymous data**: all data that cannot (or can no longer) be linked to an identified or identifiable person and which therefore do not (or no longer) constitute personal data;
- **Pseudonymisation**: means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;
- **Pseudonymised personal data**: personal data that have undergone the process of pseudonymisation;
• **Filing system**: means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

• **Processing**: means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated 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, restriction, erasure or destruction;

• **Controller**: means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

• **Editor**: the person who is authorised to process the data under the authority of the controller;

• **Processor**: means a natural person or legal entity, public authority, agency or other body which processes personal data on behalf of the controller;

• **Recipient**: means a natural person or legal entity, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

• **Patient**: the natural person admitted to or treated in hospital;

• **Consent of the data subject (in this case, the patient)**: a freely given, specific, informed and unambiguous indication of the data subject's agreement, by declaration or unambiguous active action, to the processing of personal data relating to him or her.

### Article 3 Scope

This policy shall apply to the processing of personal data of patients in UZ Brussel, as described in Articles 4, 5 and 6 hereof, compiled or performed by its employees and/or independent professionals.

### Article 4 Categories of persons whose data are processed

Pursuant to Articles 20 and 25 of the Hospital Act, the collection and processing of personal data shall apply to all patients of UZ Brussel.

Health-related data are collected - by the independent professionals and/or employees of the hospital - from the patient himself, from referring healthcare providers and from secure government platforms, unless another collection method is required in function of the purposes of the processing or unless the patient himself is unable to provide the data.

### Article 5 Nature of the processed data and the way they are obtained

The following personal data of patients are processed in UZ Brussel:

- identification data, including the national register number
- financial and administrative data with regard to admission and invoicing, including the membership of the health insurance fund
Article 6 Processing purposes and legal framework

§1. The processing of patient personal data is possible on the basis of Articles 6 and 9 of the GDPR, inter alia, under:

- the provision of healthcare services as referred to in the Patient Rights Act of 22 August 2002;
- the provisions of the Hospital Act (in particular Articles 20 and 25);
- the Compulsory Insurance for Medical Care Act, restated on 14 July 1994;
- legal actions; or
- an explicit and informed consent of the patient, insofar as consent to the processing of patient data is required in accordance with Articles 6 and 9 of the GDPR.

Within the limits of this legal framework, the processing of personal data of patients at UZ Brussel has one or more of the following purposes in particular:

- patient care: carrying out 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: the follow-up of the stay and treatment of patients with a view to invoicing;
- patient registration: the registration of medical data and residence data of patients for internal purposes imposed by the government, as well as for research and policy purposes;
- drug administration: processing operations related to the prescription and dispensing of medicines;
- complaint management: the registration of personal data of patients and/or their confidants for the purpose of mediating complaints. Registering complaints;
- quality of care: the collection and processing of all data relating to medical and paramedical diagnostic and therapeutic practices administered to patients with the aim of improving the quality of care;
- scientific registration: the registration of (medical) personal data of an epidemiological, scientific and/or managerial nature for the purpose of research, educational or objectives required by the federal or regional authorities;
- organ donation: the processing of personal data in the context of the Royal Decree of 10 November 2012 on local donor coordination;

§2. Under no circumstances shall personal data be included in such processing operations other than those that are necessary for the purposes specified in §1 and these personal data shall not be processed any further in a way that is incompatible with said purposes.

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

UZ Brussel, 101 Laarbeeklaan, 1090 Jette, Brussels Register of Legal Entities no. 0449.012.406 is the data controller of the personal data of patients.

The persons acting on behalf of the controller are the chairperson of the UZ Brussel Executive Council, the managing director, the general manager, the nursing director, the medical director and the head doctor.
Article 8 Supervision of the processing of personal data

§1. In accordance with Article 9 (3) 3 GDPR, health data shall only be processed under the supervision and responsibility of a healthcare professional.

Central responsibility for and supervision of patient files containing personal data concerning health rests with the chief medical officer (Dr Jan Schots) assisted by the general manager for the non-medical and non-nursing personal data from the patient files and by the nursing director for nursing and paramedical data.

§2. A Data Protection Officer (hereinafter referred to as the "DPO") has been appointed in UZ Brussel who also serves as information security consultant. The tasks of DPO and information security consultant are performed by Mr Luc Maes.

This person is responsible for the supervision of all aspects relating to the processing of personal data, including the security of personal data and the exercise of patients’ rights with regard to their personal data. He assists the hospital with advice on all these aspects. He may also be contacted by any patient regarding any matter concerning the processing of personal data at UZ Brussel by email gegevensbescherming@uzbrussel.be or telephone: 92 477 69 20

Article 9 The editors of patient files and their authority

§1. The internal consultation and processing of the personal data of the patients are carried out by the persons and within the limits as described in this paragraph.

1. The personal data concerning health are collected and processed under the direction of the head doctor, as stated in article 8, §1 of this Privacy Policy;
2. The (independent) doctors affiliated with the hospital are given delegated responsibility for the collection and processing of the personal data of the patients in the medical services or departments in which they work;
3. The employees and staff members connected with the various nursing and paramedical services of the hospital draw up the respective processing modules of the patient files for which they are responsible;
4. The employees and staff members of the kitchen (including the diet kitchen) are responsible for processing the personal data in the patient files with a view to personalised meal distribution;
5. The employees and staff members of the various medical secretariats are responsible for processing the personal data in the patient files for medical administration purposes;
6. The employees and staff members of the admission, administration and invoicing services are responsible for the execution, storage, search and technical processing of personal data of patients with a view to invoicing;
7. The employees and staff members of support services, such as the IT department, are responsible for the technical processing of the personal data into anonymous data, for the purposes imposed by the government and for internal research and policy purposes, or for processing the personal data to provide administrative support for such purposes;
8. The employees and staff members of patient support services are responsible for processing the personal data in the patient files for follow-up purposes in the social, psychological, palliative or pastoral care service;
9. The employees and staff members of the ombudsman are responsible for the processing of personal data in the patient files in the context of the ombudsman function;
10. The employees and staff members of the pharmacy are responsible for processing the personal data in the patient files for the distribution of medicines;
11. The information security consultant and the DPO process personal data in the patient files to the extent necessary for the performance of their respective tasks;
The various editors have access only to the personal data that they absolutely need to carry out their tasks on behalf of the controller. In case of an electronic file, a list may be drawn up of who has gained access to the programme and the information contained in it.

§ 2. All employees and staff members of the hospital who need access to personal data of patients in order to perform their tasks have committed themselves to respect the provisions of these Privacy Regulations and the GDPR, as well as all other principles of privacy protection, when processing and consulting the patient files. They also adhere to their professional secrecy or to an equivalent statutory or contractual confidentiality obligation.

Article 10 Transfer of patient data

§1. Within the limits of Articles 6 and 9 of the GDPR and insofar as necessary for the purposes mentioned in Article 6 of this Privacy Policy, the following categories of recipients are authorised to obtain patient personal data from UZ Brussel:

- insurance institutions to the extent required by or pursuant to law or with the consent of the patient;
- the National Institute for Health and Disability Insurance to the extent required by or pursuant to law or with the consent of the patient;
- the provision of healthcare services as referred to in the Patient Rights Act of 22 August 2002; the patients concerned or their representatives within the limits of what is provided for in the Patients’ Rights Act of 22 August 2002;
- public bodies authorised to do so by a governmental decree;
- external healthcare providers of the patient within the framework of the patient care referred to in Article 6 of this Privacy Policy;
- other agencies, to the extent required by or pursuant to law or with the consent of the patient;
- the professional liability insurer of the hospital or of the professional appointed by the hospital, without the patient's consent, insofar as such communication is necessary for the defence of a right in legal proceedings or for the establishment, exercise or substantiation of a legal claim;
- external processors which UZ Brussel calls on for the processing of personal data

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

Article 11 Organisation of the circuit of personal data concerning health to be processed

The circuit of personal data concerning health to be processed is organised as follows:

- data are entered as processed in the manner and by the persons described in Article 7 of this Privacy Policy;
- documents and invoices are transferred to insurance companies, patients and external pricing services;
- medical data are transferred to external health care providers for patient care as referred to in Article 6 of this Privacy Policy;
- anonymised data are transferred to the Federal Public Service Health or to the Flemish Community as per Article 92 of the Hospital Act.
Article 12 Data anonymisation procedure

The employees of the IT department are responsible for the technical processing of the personal data into anonymised data. This anonymisation means that the personal data can no longer reasonably be traced back to an individual patient.

Personal data may/can be anonymised only if it has been established that it is no longer necessary to retain said personal data for the intended processing. This is the case particularly with the following processing operations:

- the transfer of medical data in accordance with Article 92 of the Hospital Act to the Federal Public Service Health or to the Flemish Community;

Article 13 Security procedures

All the necessary measures shall be taken to make sure that the recorded data are accurate and complete. The necessary technical and organisational measures shall also be taken to protect the patient files against data loss or damage and against unauthorised access, modification or withdrawal, including pseudonymisation and procedures for testing, assessing and evaluating the effectiveness of the security measures. Computerised programmes shall have access control (a priori) and may also maintain a list of access logs (a posteriori).

Article 14 Retention periods

§1. In compliance with any legal regulations a retention period shall apply to personal data that permit identification, starting from the last discharge or treatment of the patient.

This period will be at least:

- 7 years for billing data from patient files that serve as accounting records;
- 7 years for duplicates of the certificates for provided assistance, of the individual invoice and of the collective invoice;
- 30 years for medical data;
- 30 years for nursing data;
- 1 year for the files that are handled by the ombudsman service.

§2. If the retention period has expired, the personal data concerned shall be inactivated from the files within a period of one year. For patient data, this can be done only with the prior consent of the head doctor.

§3. Inactivation may, however, be omitted if:

- retention is required on the grounds of a legal regulation
- or retention is considered reasonably important from a medical point of view, the patient's life expectancy or in order to defend his or her legitimate interests or those of his or her legal successors;
- or retention is agreed upon by the patient and the attending hospital doctor or, in his or her absence, the head doctor.
§4. If the data in question have been processed in such a way that it is reasonably impossible to trace them back to individual persons, they may be kept in anonymous form.

Article 15 Interrelationships, connections and consultations

The following parts of the patient files are mainly electronic, and to a lesser extent manual/written:

a. Administrative data
   - Patient identification data: name, sex, date of birth, unique patient number, national register number, address data, family data, contact addresses;
   - data of mutual insurance and other insurance organisations
   - administrative admission and hospitalisation data: admission and discharge dates, treating physicians, clinic locations (service-room-bed)
   - social file
   - meal distribution
   - various signed justification documents (admission statement, room selection form, general terms and conditions, etc.)

b. Medical and nursing data
   - critical data (blood group, allergies)
   - physical parameters (weight, height, ...)
   - reason for admission, diagnoses
   - operations and deliveries
   - nursing attention points and observations
   - requests and results (lab, RX, EKG, ...)
   - medical reports
   - medication
   - nursing care including the care plan
   - minimum nursing, clinical, and psychiatric data as required by the government
   - Medical images for the above purposes
   - progress notes from various care providers

c. Invoicing and financial data
   - services and products provided
   - stay data, nursing days, lump sums,
   - payment status of the patient and insurance organisation
   - payment status of the patient and insurance organisation

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

Article 16 Deletion of data

The data from the patient files are deleted:
   - upon expiry of the retention period, as defined in Article 14 of this Privacy Policy;
   - in the cases determined by or pursuant to the law;
   - at the justified request of any interested party; or
   - as a result of a court decision.
Article 17 Rights and possibilities of defence of the patient in the context of protection of privacy

§1. At the latest at the time that personal data pertaining to the patient are collected, the patient shall, pursuant to the provisions of the GDPR, be informed about the processing of thereof and the legal basis for said data processing via the admission form, the reception brochure or the UZ Brussel website. Furthermore, a copy of this Privacy Policy is available for perusal at the reception desk. A copy may also be obtained if required.

§3. The patient who requests such a copy is entitled to be informed by the controller and to receive a copy once free of charge of:

- any processing of personal data concerning him or her;
- the data that are being processed and any available information on the origin thereof, unless such right is excluded by law;
- the purposes of such processing;
- the categories of data concerned by such processing and the time limits for the retention thereof;
- the categories of recipients to whom the data are disclosed;
- the rights of the patient with regard to the personal data processed;
- the source of these personal data, if not collected from the patient him- or herself;
- the existence of automated decision-making on the basis of these personal data, as well as the underlying rationale and the consequences of such decision-making.

§4. The patient who so requests is also entitled to have all incorrect or incomplete personal data corrected or supplemented free of charge by the controller. In addition, the patient may request that his or her personal data be temporarily suspended from further processing (except in a number of legally defined cases) until the accuracy thereof has been checked. The personal data must be corrected or supplemented only if the controller establishes that they are indeed incorrect or incomplete.

§5. The patient also has the right to request that the controller provide a copy of his or her personal data to that patient and/or directly to another institution or person of the patient's choice in a format that allows for easy transfer of such personal data. This right shall, however, apply only to personal data provided by the patient that are processed by automated means solely on the basis of an explicit authorisation by the patient and in so far as the transfer does not adversely affect the privacy of others.

§6. If the patient is of opinion that his personal data may no longer be processed (e.g. because they are no longer required for the processing purpose or because they are processed unlawfully), he or she may request that his or her personal data be permanently erased. Alternatively, instead of erasure, the patient may request that his or her personal data be retained, but not processed further (except in certain cases defined by law).

The controller is not, however, required to erase the personal data if it they may or must still be processed lawfully in accordance with the GDPR.

§7. Unless the processing is necessary for compelling legitimate reasons, the patient may object to the processing of his or her personal data which is based solely on the legitimate interests of the controller or on the performance of a task carried out in the public interest or under public authority.

§8. In addition to the cases referred to in paragraphs 4, 6 and 7 of this article, the patient may also request that his or her personal data be retained, but not processed further (except in a number of statutorily defined cases) if the controller no longer needs them, but the patient still needs them in the context of a legal action.

The legally defined cases in which processing may still take place, despite the patient's request that his personal data not be processed any further for the time being, as referred to in paragraphs 4, 6, 7 and 8 of this article, are the following:
- if the patient gives his or her specific consent;
- if the controller needs the personal data in the context of a legal claim;
- to protect the rights of another natural person or legal entity; or
- for important reasons of general interest.

§9. In addition, the patient who so requests shall always have the possibility to object to automated processing of his or her personal data for the purpose of individual decision-making which produces legal effects or consequences that have a similar impact on the patient.

The controller shall not be required to accede to this request if it can rely on a legal provision or the explicit consent of the patient.

§10. To exercise his or her rights referred to in paragraphs 2 to 9 of this Article, the patient can submit a request to UZ Brussel by email to gegevensbescherming@uzbrussel.be.

Once said request has been submitted, 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 of what action will be taken in response thereto. In the event of complex or frequent requests, this period may be extended to three months following the submission of the request. In such a case, the controller will inform the patient whether the patient's request is unclear, or if there are doubts about the identity of the requesting party, the controller may request such additional information as necessary. If the requesting party refuses to provide the necessary information, the controller may refuse the request.

The request procedure is free of charge for the patient. If, however, the patient's request is manifestly unfounded or if the patient makes excessive use of his or her rights, in particular if the same request is made repeatedly, the controller may either refuse the request or charge a reasonable fee in accordance with the administrative costs associated with such requests.

§11. If the patient is of opinion that the provisions of this Privacy Policy or the GDPR are not being complied with or has any other complaints regarding the protection of privacy, he or she can directly turn to:
- the persons mentioned in Article 8, §2 and 3 of the Privacy Policy;
- The Data Protection Authority; and/or
- the competent court.

**Articles 18 Entry into force and amendments**

This Privacy Policy shall enter into force on 25 May 2018. UZ Brussel reserves the right to amend its Privacy Policy at any time. Amendments will be made by the Executive Council of UZ Brussel.