Private Life Policy for the attention of patients of the H.U.B and its partner institutions

Mise à jour : le «25/02/2024»

Contents

1. RECITAL

The hospital structures of the Brussels University Hospital (hereinafter the H.U.B or the Institution), namely:

- The Brussels University Clinics – Erasmus Hospital, including:
  - The Trauma and Rehabilitation Centre (CTR);
  - The Geriatric Rehabilitation Centre (CRG);
  - The Lothier Polyclinic;
- The Brussels Hospital Association – Jules Bordet University Hospital;
- And the Brussels Hospital Association – Queen Fabiola University Children's Hospital (Huderf)

appreciate and attach great importance to the confidence you place in them. The Institution wishes to provide you, as a patient and independently of your income, your insurability, your origins and

philosophical beliefs, with the very best reception, optimal medical and paramedical care as well as adequate assistance with social and administrative matters.

The Institution undertakes to respect confidentiality and your private life. It undertakes to process personal data, notably in relation to your medical care and social and administrative suport, in accordance with the General Data Protection Regulation (GDPR) and the applicable Belgian legislation on the protection of private life.

This information document is for the purpose of setting out how the H.U.B institutions process your data in the framework of their activities. Data processing includes the collection, storage, protection and erasure of data. This document also sets out your rights in regard to your personal data and how you can exercise them.

2. WHO IS CONCERNED BY DATA PROCESSING AND IN WHAT FRAMEWORK

Patients of the Institutions

The Institution processes personal data (hereinafter "the data") of all patients who consult it. These data are collected from the patient or, if applicable, from the patient's legal representative, by Institution staff, by means of an application or on a web page if the patient uses one.

Patient contact persons

The Institution also processes the data of third persons referenced by the patient or the patient's legal representatives. These third persons can be contact persons, legal representatives, the GP or other healthcare professionals who accompany the patient, etc.

For the patient as for third parties, the Institution only processes information that is useful and necessary for achieving the purposes set out in this document.

In what framework does the Institution process these data?

Data concerning you are collected and processed at different moments, notably at the time of:

- Making an appointment (whether made by telephone, via websites, the MyHUB application, or a platform for making online appointments);
- A consultation;
- A hospitalisation;
- Treatment by the Emergency Department (externally by the SMUR [Emergency Medical Assistance Service] or within the Hospital);
- Carrying out an examination prescribed by an external healthcare provider;
- A request for a second opinion coming from an external healthcare provider or centre;
- The subcontracting of certain activities (laboratory analyses, etc.);
- Organising transfers between care institutions or to a reception structure;
- Activities relating to healthcare research;
- Treatment invoicing;
- The compulsory sending of certain data to the responsible institutions (INAMI [National Medical Insurance Association], National Cancer Register, AVIQ [Agency for a Quality Life], etc.)

These data concern your health and are extremely sensitive. The Institution is careful to manage and protect your data effectively while respecting the legal provisions.

In this document you will find information on the data categories the Institution collects, the purposes for which your data are processed, the entities with which they can be shared, measures taken by the Institution to protect your data and the way in which you can exercise your rights regarding your data.

The essential elements of the data protection policy are as follows:

- Data are only processed if this is necessary for realising the Institution's missions which include the provision of care and the legal obligation to maintain an up-to-date Patient File containing information of a medical, administrative, social and financial nature, and also in the framework of our research and teaching missions for which we process de-identified data only;
- Your data are only transmitted to third parties in a context in keeping with the hospital's missions and under no circumstances for commercial purposes;
- Your data are stored in our data centers. If it is necessary to share them externally with a subcontractor (request for second opinion, additional analysis, reading of indicators via connected equipment, clinical trials, etc.) we put into place the appropriate guarantees to accompany this data processing, in accordance with the GDPR;
- Your data are retained for a period that respects the periods laid down by the legislation (for the medical file: a minimum of 30 years and a maximum of 50 years);
- For any questions concerning the processing of your data and the exercising of your rights, please submit your request to the Data Protection Officer at the following address: dpo@hubruxelles.be.

The processing of patients' personal data is notably possible in connection with:

- The provision of healthcare services, as referred to in the law of 22 August 2002 on patients' rights;
- The provisions of the coordinated law on hospitals and other care establishments of 10 July 2008 (articles 20 and 25 in particular);
- The coordinated law of 14 July 1994 on compulsory insurance to cover the costs of medical care;
- Judicial proceedings;
- Care, teaching and research missions, in accordance with the legislation in this field;
- Management of the Institution, in accordance with its obligations or legitimate interests;
- Or, if applicable, the patient's explicit and well informed consent, provided the authorisation to process the patient's data is requested in accordance with articles 6 and 9 of the GDPR.

3. PROCESSING RESPONSIBILITY

The Institution you consult is legally responsible for the processing of your personal data

Hôpital Erasme – Cliniques universitaires de Bruxelles

808, route de Lennik, 1070 Bruxelles

N° entreprise : 0941.792.893

Association Hospitalière de Bruxelles – Centre Hospitalier Universitaire Jules Bordet

90, Rue Meylemeersch, 1070 Anderlecht

N° entreprise : 0257.981.101

Association Hospitalière de Bruxelles - Hôpital Universitaire des Enfants Reine Fabiola

15, Avenue Jean Joseph Crocq, 1020 Bruxelles

N° entreprise : 0260.238.627

Responsibility for and surveillance of your data, as patients and third parties, rests with the managing director, medical director, nursing director and administrative and financial director of the Institution, depending on the processing effected under their respective responsibilities.

In accordance with the General Data Protection Regulation (GDPR), the Institution has appointed a Data Protection Officer. He or she may be contacted with any question concerning the protection of personal data, at the following address dpo@hubruxelles.be.

4. TYPES OF DATA PROCESSED

The Institution collects data that are pertinent to and necessary for your care by the care services (medical, nursing, paramedical), for the compiling of your patient file and the management of your administrative and social file, by the reception services, and for the patient contact, invoicing, accounting and social welfare service.

The Institution processes your medical data (for example: health status, results of examinations, pathologies, antecedents, etc.) and your administrative data (for example: identification data such as first and last names, national register umber, invoicing data, etc.).

The Institution also processes other data necessary for the purposes determined by or laid down in the legislation (for example: data on lifestyle, on family and professional situation, on contact persons or trusted persons or mandatees, on philosophical or religious beliefs, on sexual behaviour, on racial or ethnic origin, etc.).

These data can be collected either directly from you or indirectly from your representative, your prescribing doctor or your GP, from file elements transmitted by another provider, another institution, by you, etc.

Depending on the purposes, the personal data processed by the Institution may concern the following categories:

Personal data :

- Identification data (for example: first name, last name, unique patient number (NISS [social security] no.) contact postal address and/or domicile, telephone number, medical file number, hospitalisation number, registration number, pseudonym, etc.);
- Copy of identity card, passport, or other card attesting to identity;
- Electronic and connection data (for example: email address, IP addresses, logs, terminal identifiers, connection identifiers, etc.);
- Personal characteristics (for example: age or date of birth, gender, nationality, language spoken, civil status, etc.);
- Physical data (for example: height, weight, appearance, etc.)
- Mental, psychiatric data or data relating to consultation with a psychologist (e.g. personality, character, etc.)

- Household composition
- Lifestyle (for example: dependency - alone, in institution, autonomous, bedridden -, assistance – home, family help -, physical exercise, urban, semi-urban, nomadic, sedentary lifestyle, accommodation);
- Consumer habits (for example: diet, dietary habits, addictions, etc.);
- Leisure activities and interests;
- Third party data and data concerning contact persons (for example: representatives, legal proxy, trusted person, care provider, prescribing specialist doctor, GP, etc.);
- Level of education (for example: primary, secondary, higher);
- Professional life (for example: training, experiences, CV, etc.);
- Images (for example: photos, images filmed by surveillance camera, etc.);

Data perceived as "sensitive":

- Financial and administrative data relating to admission and invoicing (for example: bank account number, data concerning membership of mutual or insurance companies, etc.);
- Social data (for example: identification of downstream structures and other rehabilitation centres, intervention by the CPAS (social welfare), ONE (employment office) or any other parastatal body, etc.)
- National register number ;

Special categories of personal data (GDPR Art. 9):

- Health data (for example: weight, height, blood group, diagnosis, results of examinations, personal or family antecedents, appointment, consultation and hospitalisation data, history of pathologies, list of allergies, treatment plan, administration of medicines, nutrition and dietary data, results of neurological images, etc.);
- Biometric data (for example: fingerprints, fundus of the eye, ocular biometry, etc.);
- Genetic data;
- Samples taken;
- Ethnic origin;
- Political opinions;
- Religious or philosophical beliefs or trade union membership;
- Data concerning sex life or sexual orientation of a natural person

5. WHAT IS THE LEGAL BASIS FOR PROCESSING YOUR DATA ?

Depending on the purpose of the processing and type of personal data (whether a special category of personal data according to GDPR, Article 9, or not), the Institution processes the personal data on the legal basis of:

- Respect for a legal obligation (for example: maintaining a medical file, obligatory declaration of diseases, etc.) (GDPR Art.6.1.c; for these examples: GDPR Art.9.2.h; GDPR Art.9.2.i);
- Processing required for the purposes of preventive medicine or industrial medicine (...), medical diagnoses, health and social care (…), or by virtue of a contract entered into with a health professional (…) (GDPR Art.6.1.b; GDPR Art.6.1.e; GDPR Art.9.2.h) ;
- The performance of a contract (for example: the processing of data relating to invoicing of services requested and/or carried out) (GDPR Art.6.1.b) ;
- The performance of a public interest mission incumbent upon the Institution (for example: data processing for the purposes of teaching, scientific research) (GDPR Art.6.1.e) ;

- Processing for the purposes of legitimate interests pursued by the Institution (for example: recording and managing risks and undesirable events, processing relating to technical management, logistics, security of goods, access control, process improvement and optimisation, comparative evaluation, following up legal proceedings, etc.) (GDPR Art.6.1.f) ;
- Protecting the vital interests of the person concerned (for example: processing of Data on patents in a situation of medical emergency) (GDPR Art.6.1.d).

If the processing of personal data cannot be based on one of these foundations, the processing can only take place on receipt of your explicit consent in writing.

6. FOR WHAT PURPOSE(S) ARE YOUR DATA USED?

Your data are processed to permit the organisation of your treatment and the creation of your patient file, as well as the management of your administrative, financial and social follow-up within the Institution and the care network within which it participates.

Your personal data can also be used to enable the Institution to fulfil its obligations such as legal reporting, and its other missions such as clinical teaching and scientific research on the sole basis of pseudonymised data. If you do not want the Institution to process your data in the framework of scientific research you can object to it. You will find more information on the use of data in the framework of scientific research and on how you can object to this data processing under point 16 of this document.

The Institution is particularly careful to ensure that personal data are processed appropriately, limited to the purposes of the treatment and in accordance with the applicable legislation.

The list of purposes for which the Institution processes personal data is as follows:

a) Care activities

- Management of the patient file, serving to permit diagnosis, treatment and the communication of information concerning the provision of medical, nursing and paramedical care to patients under optimal conditions of security;
- Treatment of patients admitted to Emergencies ;
- Social welfare;
- Appointments management;
- Management of prescribing and results of medical and technical examinations;
- Prescribing, issuing and administration of health products and requests for acts;
- Declaration of diseases for which reporting is obligatory;
- Registering of risk groups, with the aim of identifying and monitoring persons with a medical risk;
- Registering of donors, with the aim of creating files with details of persons who wish to be donors, promoting this aim and the use of these files;
- Management of declarations of births and deaths;
- Registering of screening test results or follow-up in official registers or registers of other official bodies (in particular registering cancers with the National Cancer Register, registering of deafness among newborns with the ONE, registering of rare disease monitoring with Sciensano, etc.);

- Management of blood banks, stem cell banks, tissue banks, etc.;
- Collecting consents relating to healthcare;
- Etc.

b) Support activities

– Administrative and financial management of patients for the purposes of invoicing and collection, this implying the communication of information to authorised third parties (mutual companies, insurance and collection companies, etc.)
– Management of contacts relating to the family, proxies, contact and trusted persons designated by the patient, this to improve the patient's treatment and administrative and social follow up;
– Management of contacts and directories concerning GPs, prescribers, dispensers and signatories to ensure treatment follow up;
– Technical management of the information system supporting infrastructures and institutional applications that process personal Data;
– Logistics management permitting patient care, namely stretcher carrying, reception, appointments, dietetics;
– Recording and management of undesirable events relating to patient safety;
– Management of requests submitted by the patient concerning the exercising of patients' rights by virtue of the General Data Protection Regulation (GDPR) and the law of 22 August 2002 concerning patients' rights;
– Management of requests for copies of medical file;
– Complaints and litigation management;
– Management of spiritual support and well-being;
– Security of persons and goods, exercised notably by videosurveillance cameras and access control ;
– Etc.

c) Medico-economic management activities

– Registering of patients' medical and hospitalisation data with a view to the Institution's internal management or objectives imposed by the public authorities;
– Evaluation of the quality of care, resources management and control of hospital activities (notably within the CBAH network – Conference of Academic Hospitals of Belgium);
– Dispatch of appointment reminders by text message or email;
– Etc.

d) Research and teaching activities (*)

Within a university or academic hospital your data can be used in connection with clinical teaching and scientific research. Your health data are essential for the continuous improvement of care and medical techniques and to develop the medicine of the future. These missions require the processing of pertinent, pseudonymised data collected from your file to furnish retrospective studies and registers as well as the analysis of these data by communities of researchers, teachers and students. The use and analysis of data for these activities requires approval by an ethics committee and a scientific research service, both of which are committed to respecting the applicable legislation and patient security.

Prior to such a use your data are pseudonymised so as to protect your identity. Processing relating to research and teaching include:

- Clinical teaching and training of doctors and other healthcare professionals;
- Applied scientific research (retrospective and prospective studies with or without clinical trials, studies of residual human body material (**)) ;
- The development of new technologies;
- Management of the Human Body Material Bank/ Tissue Bank;
- The creation of registers, monocentric or multicentric, epidemiological or of targeted populations presenting a scientific interest in the field of health and care;
- The collecting of consent;
- Etc.

(*) The Institution respects the legislation of 30 July 2018 on data protection. When medical data are analysed retrospectively for the purposes of scientific research and teaching, the Institution favours the processing of aggregated data with de-identification and codification. Explicit consent will be required if it proves necessary to have recourse to granular data that can potentially result in the re-identification of the person. Anonymization is guaranteed for any publication or dissemination. If a risk of re-identification is identified following a publication or dissemination (for case studies concerning rare diseases for example), explicit consent in writing will also be required. The patient can object to this at any time and reverse a previous consent without having to justify this or experience any inconvenience in his or her medical treatment. Any objection will be noted in the medical file. Conversely, the patient can also reverse a refusal at any time.

(**) For prospective studies and clinical trials explicit consent in writing will be submitted to participants.

e) Data Communication

- Medical reports, requests for tests and medical examinations and their results are communicated to healthcare professionals who can attest to a treatment link with the patient in question. This communication can be by direct communication to the provider or by way of a health network for patients who have consented to this. You will find more information on Health Networks under point 10;
- Communication of information necessary for the discharge of patients to bodies in the social and family assistance, medico-social and psycho-pedagogical sectors or upstream reception structures necessary for the reception of patients coming from a downstream structure;
- Exchange of health documents (results of examinations, medical reports, emails, etc.) whether computerised or otherwise from/to the patient and between the various care providers involved in the care for the same patient;
- Communication on the presence and location of the patient and patient's loved ones, unless the patient has objected to this or such a communication would be contrary to the patient's interests.
- Etc.

For any other purposes the consent of the patient or the patient's legal representative will be requested.

It should be noted that a person's right to confidentiality is not absolute and there can be other circumstances in which we have to share information from your patient file with other persons. In such circumstances we are not obliged to have your consent.

Examples of such circumstances could be:

- So as to comply with a judicial decision;
- For the purposes of data conservation (technical backup of data processing system);
- If your information falls within a category that must be reported for reasons of public health or other legal reasons, such as certain contagious diseases;

- To prevent or detect serious crimes;
- If you are subject to the law on mental health there are circumstances when legal guardians or agents must receive information even if you oppose it;
- In the legitimate interest of the Institution, for example, if revealing certain information is necessary for defence in a court of law;
- At the time of internal quality surveys (failing opposition on your part);
- If the information has been the subject of an effective de-identification that makes it impossible for the recipient to re-identify the persons concerned by the habitual means.

9. WHO ARE THE PERSONS WITH ACCESS TO YOUR DATA?

Persons involved in ensuring a smooth care pathway within the Institution (notably in terms of treatment, administration and social welfare) or who undertake tasks entrusted to them by the Institution may process your personal data, within the limits necessary for their missions and for the specific purposes of the treatment.

Access to and processing of your data is carried out solely by authorised personnel (direct or indirect collaborator such as Institution partner under a contract or convention). Users only have access to the data they need to undertake their tasks, according to the principle of "necessary and sufficient" ("nothing except..."). These persons undertake to respect professional secrecy, the regulations and provisions relating to data protection via a contractual obligation and via the code or deontology of their profession.

The Institution's direct and indirect collaborators or members of the care network of which the Institution is a part as well as partner institutions have access to your data, within the limits of their missions and tasks, as follows:

<u>The Supervisor</u>

This is the supervising practitioner appointed from among doctor members of the Institution's medical management. He or she is responsible for supervising all aspects of the care and treatment administered to a patient by the medical and nursing team (care team).

<u>Medical and nursing team (care team)</u>

This is the nominative list of doctors, specialist assistant doctors, specialist candidate doctors, hospital pharmacy staff, members of the care and paramedical teams and type 1 auxiliary staff who are associated with the tasks required or carried out in connection with the care and treatment of a patient, under the supervision of the Supervisor. The care is of a medical, nursing, health and social nature.

<u>The health professionals</u>

In accordance with the coordinated law on the exercising of healthcare professions of 10 May 2015, the term "health profession" designates persons in charge of patients, that is, doctors (doctors with management role, consultant doctors, associated doctors), specialist assistants, Specialist Candidate Assistant Doctors (MACCS), dentists, hospital pharmacists, other health professionals, namely nurses, auxiliary nurses, hygienists, physiotherapists, midwives, biologist pharmacists, clinical psychologists and any other practitioner who can give orders, give consultations and/or carry out acts or interventions for treatment, pharmaceutical or care purposes. The term excludes specifically visiting doctors (the GP or other doctor who may visit the patient) as well as researcher doctors, scientific officers intervening solely for research or teaching missions

<u>Type 1 Auxiliary Staff</u>

Type 1 Auxiliary Staff designates persons delegated by a supervisor to provide medical, nursing and social care for patients. This category of personnel is a part of the medical and nursing team and includes paramedics (hospital dieticians, ergotherapists, hearing care specialists, speech therapists, opticians, orthoptists, prosthesists, podiatrists, bandagists and medical imaging and laboratory technicians, etc.), interns (doctor, physiotherapist, midwife, nurse, dietician, etc.), and medical secretaries, social workers, stretcher bearers, care coordinators and data managers in clinical research.

Type 2 Auxiliary Staff

Type 2 Auxiliary Staff designates any internal or external collaborator who is required to access information concerning the patient for the needs of his or her mission. These are administrative staff (patient administration and reception, consultation secretary, planning, invoicing, DI-RHM/RCM [medical abstract/register of nursing interventions] codifying), patient mediators, archivists, voluntary staff, educators/facilitators, spiritual accompaniers, administrative nursing assistants, researchers (doctors, students), scientific officers, data manager, internal auditor, staff assigned to data protection, data protection office, data security adviser.

Type 3 auxiliary staff

Type 3 auxiliary staff designates support staff, that is, equipment technicians, data processing staff, staff attached to logistics services.

Other

Third persons associated by convention and subject to professional secrecy in the framework of the mission conferred by a control authority. Any health professional who has access to documents published on the health networks (for example RSW, RSB/Abrumet, etc.) or care networks (see dedicated section) in the framework of their treatment relation.

10. WHO DO WE SHARE YOUR DATA WITH?

Within the limits of articles 6 and 9 of the GDPR and insofar as this is necessary for the purposes referred to in this Policy, various categories of recipients can legitimately receive the communication of certain of your data, each according to his own purposes:

- Yourself as a patient or your representatives
- Your insurance bodies
- National Institute of Sickness-Disability Insurance (INAMI)
- The public authorities
- Providers of external services
- The Institution's insurer in the event of litigation with the patient
- The Institution's subcontractors
- The Institution's partners within care networks and groups of which the Institution is a part (see below)
- Other recipients in the framework of a transfer authorised by law or the patient's consent

Your data can only be shared with third parties or with bodies outside the Institution in connection with your treatment (sharing of data with other hospitals, doctors who do not practice within the Institution, etc.), in connection with one of the Institution's missions, in compliance with a legal obligation to transmit data to which the Institution is subject (for example, pursuant to a law,

regulation or legal proceedings), and this in connection with the purposes stated in this policy, with your consent if required.

When data are exchanged, the Institution guarantees that appropriate technical and organisational measures will be put into place, such as the concluding of a contract and the use of secured means of communication.
The categories of recipients with which the Institution is likely to share data are the following:

- The patients concerned or their representatives within the limits of the provisions referred to in the law of 22 August 2002 concerning patients' rights;
- At the patient's request, after the patient has been informed and provided his or her explicit consent, any authorised person;
- Social security organisations, insurance companies and other social assistance organisations provided this is imposed by or pursuant to the law or authorised by the patient.
    - o In this connection, when you request practice of the third-party payment system with your supplementary hospitalisation insurance, you authorise the hospital to transmit detailed invoices to your insurer, by electronic means. These invoices set out: hospitalisation costs with admission and discharge dates, type of hospitalisation, admission and transfer service; fees and various costs, including the INAMI code(s), that are not reimbursed of care services provided, fixed fees, implantable devices; amounts payable by the insuring body and by the patient; also transmitted are details of the service provider(s), the prescriber(s), the pharmaceutical specialities administered, communiqué(s);

- The National Institute of Sickness and Invalidity Insurance as imposed by or pursuant to the law or authorised by the patient;
- Public bodies that are authorised by a decision of the authorities (in particular the ONE, Sciensano, etc.) ;
- The patient's external care providers in the framework of patient care (for example: SMUR, ambulance, adapted transport for patients, bandagists, pharmacies);
- Other bodies provided this is laid down by or is pursuant to a law (for example for organ donation) or authorised by the patient;
- The insurer of the hospital's professional liability or that of the practitioner designated by the hospital, through the intermediary of the hospital's insurance broker and this without requiring the patient's authorisation provided this communication is necessary to arrive at an amicable resolution, to defend a right before the courts or to initiate, exercise or support legal proceedings;
- External subcontractors or third parties to which the Institution has recourse to process personal data and for which appropriate guarantees are in place regarding the protection of personal data (for example: home transport service, dispatch of text message confirming appointments, investigation service, debt collection company, mediation services, etc.);
- Auditors or monitors, under the authority of the sponsor of a clinical trial or an Ethics Committee, whose mission is to audit clinical trials and studies carried out on the basis of the data collected or studies or trials.
- Auditors and inspectors of any competent health authority.
- Partners of the Institution within the care networks in which the Institution participates

With the exception of the cases cited above, only anonymised or codified data with no re-identification may be exchanged with other persons and bodies.
When we share your information we implement the appropriate legal, technical and operational measures. There will be a contract and/or an information sharing agreement in place. We will only share your information if we are convinced that adequate agreements exist and that the means of communication with third parties and/or organisations are adequately secured.

Hospital groups and care networks

Networking hospitals favours closer and more frequent cooperation between university hospitals, both specialised and local. Continuous dialogue between all the actors concerned, including care providers outside the hospital, is essential. (Order of Doctors, source https://ordomedic.be/fr/avis/medecine-hospitaliere/hopitaux/reseautage-clinique-entrehopitaux-principes-deontologiques)

The Brussels University Hospital (H.UB) is a grouping of three hospitals, namely:

- The Brussels University Clinics– Erasmus Hospital, this including:
  - The Trauma and Rehabilitation Centre (CTR) ;
  - The Geriatric Rehabilitation Centre (CRG) ;
  - The Lothier Polyclinic;
- The Brussels Hospital Association –Jules Bordet University Hospital;
- The Brussels Hospital Association – Queen Fabiola University Children's Hospital (Huderf)

These three partner institutions work together to provide you with the best possible reception and care. They process and share the information they possess on you in accordance with the present policy and in compliance with all the applicable laws and standards.

These three institutions also participate in the CHORUS care network that brings together:

- The University Clinics – Erasmus Hospital;
- The Jules Bordet Institute;
- The Queen Fabiola University Children's Hospital;
- The CHU-Brugmann ;
- The CHU Saint-Pierre ;
- The Edith Cavell Inter-Regional Hospital (CHIREC) ;
- The Iris Sud Hospitals.

These networks are regulated by the consolidated coordinated law of 10 July 2008 on hospitals and other care establishments concerning inter-hospital networking.

Within these networks the partner institutions make available the information they possess on you to the professionals they employ via the shared care file. This sharing takes place in the framework of accessibility to care and the provision and/or continuity of care. The institutions' priority remains the quality and continuity of care in the interests of the patient and of society.

Networking information is designed to enable professionals at the institutions who are involved in your care or your social follow-up to consult your files, thereby assisting them in understanding your needs and in taking the best decisions with you and for you. This means that:

- You will not have to give your details repeatedly very time you need care;
- Clinicians and nursing and paramedical teams will be able to see what medicines you are taking and if you have any allergies, thereby making your treatment safer;
- They will also be able to take the best decisions regarding your care in full knowledge of recent antecedents and elements such as results of tests, analyses and prescription details;
- You will obtain more effective treatment as the clinicians and teams who care for you will not have to wait for other partner organisations to communicate your information.

What information will health and care professionals be able to see?

We are setting out below the information that the health, social service and administrative professionals employed by partner organisations will be able to consult via the shared file. We have categorised them under the headings of "administrative management", "health care" and "social follow-up" in order to show the type of information that each entity of the partner organisation will be able to consult depending on its strictly specific missions and needs.

Administrative management (common data)

- Identification data and details such as your name, photo, address, date of birth, NISS [social security] number, eid card no., and administrative numbers;
- Telephone, first and last name of persons to be contacted in the event of an emergency in particular;
- Persons to be contacted in the event of an emergency;
- The name of the providers of care and services that you have received;

Medical care and continuity of care

- Identification data and details such as your name, photo, address, date of birth and NISS number;
- Persons to be contacted, in the event of an emergency in particular;
- Providers of care and services you have received;
- Your medication and care plans;
- Any alert, allergy or risk that is pertinent for your care;
- Your medical and pregnancy history;
- Details of births and neonatology;
- Information concerning any operations you have had;
- Care files you have received as a hospitalised patient or outpatient;
- Your appointments;
- Documents such as summaries of discharges, clinical letters, care plans, risk evaluations and references;
- Results of investigations, scans and laboratory tests;
- Reports such as radiology analyses and X-ray reports;
- Examinations, such as to check blood pressure;
- Trials or studies which you could participate in;
- Information on social service assessments;
- Details of support care, including details of your end of life preferences, etc.

Social follow-up

- Identity information and details such as your name, photo, address, date of birth and NISS number;
- Persons to be contacted in the event of an emergency;
- Information on social service assessments;
- Providers of care and services you have received;
- Any protection information designed to protect you;
- Your medication and care plans;
- Your appointments;
- A summary of the care you have received or are receiving within partner institutions;
- Details of support care, including details of your end of life preferences, etc.

Each partner organisation is responsible for the information it consults or makes available for consultation via the shared care file. This includes personal files and special category information

they have in their files. All the partners who are authorised to consult your information must respect the law to ensure they always process your personal information in a manner that is legal. The data actually processed depends on the care or services you need. The legal bases for this sharing are:

- The provision of health/social care (Art 6.1.b, e or a and 9.2.h of the GDPR) when you register with an institution participating in the networks;
- Protecting vital interests ("life or death" situation") (Art 6.1.d and 9.2.c of the GDPR) when you go to emergencies or are unconscious;
- The protection of vulnerable adults and children (Art 6.1.c or d, 9.2.g of the GDPR) when the situation demands specific care.

The health networks

With the aim of improving continuity of care and to facilitate cooperation between the care providers in the interests of better patient follow-up, four health networks have been set up in Belgium:

- The Brussels Health Network (or Abrumet)
- The Walloon Health Network
- Two local networks in Flanders:
    - The Cozo for the Ghent and Antwerp regions,
    - VznkuL for the Leuven region.

To ensure that it is possible to share information throughout Belgium these four networks are interconnected and also connected to the federal portal www.masante.belgique.be.

As a Brussels structure, the H.U.B shares pertinent information on the Brussels Health Network to permit continuity of care (hereinafter "the Network").

To benefit from this Network's services, care providers and patients must give their consent for electronic data to be shared in the framework of continuity of care.

Only care providers with a treatment link with the patient can access their medical data and this subject to the patient's prior agreement.

Information rendered accessible on the Network continues to be stored at the Institution, only the document reference being published so as to make it possible to consult the information 24/7.

The Institution does not share the complete patient file but only those documents deemed pertinent for your continuity of care, such as the results of examinations, medical reports, emails, etc.

After the document reference is published on the Network, a waiting period of 7 days applies before the content can be accessed. This enables the care provider to contact the patient if the care provider considers this necessary. This waiting period can be extended at the service provider's request if a longer period proves necessary to contact or meet the patient.

This sharing of information on the Network is in order to improve the continuity of care and in accordance with the legal basis for data processing for the needs of preventive medicine, medical diagnosis and health and social care or treatment (GDPR Art.9.2.h).

To find out more about the Brussels Health Network : https://brusselshealthnetwork.be/

11. WHAT SECURITY MEASURES ARE IMPLEMENTED TO SAFEGUARD YOUR DATA?

The Institution, as the data controller, and any of its subcontractors, implement and maintain sufficient technical and organisational measures to protect personal data against any forbidden or illegal access, communication, modification, loss or accidental destruction.

The retention, storage, consultation and communication of your data is effected in accordance with good practice and the minimal standards imposed on the healthcare sector by the competent authorities.

The Institution has put into place appropriate procedures to manage any presumed breach of personal data. In accordance with the GDPR (Article 34), the Institution will inform you in the case of a data breach and if a high risk for your rights and freedoms is identified. In the event of such a breach the Institution will also notify the Data Protection Authority (GDPR Art.33) as well as any other competent body.

The principal security measures taken by the Institution are the following:

- Appointment of a data security adviser;
- Protection, by physical security measures, of the sites where the data are kept (identified and protected areas, limited access, processing protection devices, protection against physical dangers such was fire, water damage, etc.);
- Protection of secured areas to ensure that only authorised persons have access to them (physical access controls);
- Restricted access to the data and data processing means. Restrictions and checks are carried out in accordance with the limited and authorised logical access of Institution personnel. Each user has a personal and confidential identifier and password (logical access control);
- Implementation of a password policy that includes a unique authentication service as well as the obligation to periodically change the password;
- Implementation of traceability mechanisms for the identification, collection, processing, retention and deletion of data liable to serve as proof;
- Implementation of periodic checks on event logs with a view to detecting infractions and breaches;
- Recourse to encryption in connection with the use of fixed supports whenever possible and at the time of electronic communications with a view to protecting confidentiality (encryption);
- Reduction or elimination of the identifying nature of personal data when processing permits (pseudonymisation or anonymisation) ;
- Protection of data and data processing means against malicious software (protection against malware codes);
- Management of security incidents according to a specific procedure;
- Implementation of a data safeguarding and restoration policy;
- Implementation of measures designed to protect data on communication networks (network security);
- Implementation of measures designed to protect data when they are transferred to an external entity (data transfer);
- Increasing awareness of data protection among members of staff.

Restriction of access by external recipients who have a secure access that allows them to access solely the data and environments necessary for their mission.

13. FOR HOW LONG ARE YOUR DATA RETAINED?

Notwithstanding any legal or regulatory provisions, notably in regard to data storage, the following data retention periods apply. These periods commence with the patient's discharge or final treatment:

- Data included in the Patient File are retained for a minimum of 30 years and a maximum of 50 years;
- Data concerning the organisation of hospitalisation are retained for 10 years;
- Data concerning the patient's administrative formalities are retained for 10 years;
- Data concerning clinical trials are retained for a minimum of 25 years after completion of the trial in accordance with the applicable legislation;
- The mediation service data are retained for one year after the file is closed;
- Data concerning complaints and litigation management are retained for one year after resolution of any legal action;
- Data concerning financial and accounting management are retained for between seven and 10 years depending on the applicable legal provisions;
- Images filmed by surveillance cameras are retained for one month unless they serve as proof in connection with investigations or for establishing, exercising or defending legal rights.

If the retention period expires the personal data are erased within a period of one year unless their retention is required on the basis of a legal provision or if it is considered important from a medical point of view or to defend the legitimate interests of the hospital, of the patient or of the patient's legal successors and also if there is an agreement between the patient and the Institution on the data retention.

If the data retained are processed in such a way that the identification of persons can be reasonably considered to be impossible they can be retained for an unlimited period in a de-identified form.

14. WHAT ARE YOUR RIGHTS AND HOW TO EXERCISE THEM?

Pursuant to the legislation on the protection of personal data, you have a number of rights in relation to your data: right of access, right of correction, right of erasure, right to limit processing, right to data portability, right to object, right not to be subject to a fully automated decision (artificial intelligence), right to lodge a complaint with the Data Protection Authority.

In the case of a request to exercise a right, the Institution will provide you, within 30 days, with information regarding the measures taken following your request. If necessary, this period can be extended by two months to allow for the complexity and number of requests. In which case the Institution will give you the reason for this extension within one month of receipt of the request (GDPR Art.12.3).

The response time will start when the request is received in due form, that is, when the request is clearly formulated and any reasonable doubts regarding your identity have been removed. When making a request to exercise a right it is imperative to address the request in writing, by mail or email, accompanied by a rector verso of your identity card as proof of your identity (GDPR Art.12.6).

Electronic address: dpo@hubruxelles.be

Postal address:

For the attention of the Data Protection Officer
Data Security/DSI (route 1532)

Jules Bordet Institute
90, Rue Meylemeersch
1070 ANDERLECHT

For your data security a secure shared space can be created at your request via the address dpo@hubruxelles.be. At this site you can upload your identity in total security.

If your request is submitted in electronic form, the information you receive in return will also be communicated by electronic means. (GDPR Art.12.3).

In the case of clearly unfounded or excessive requests, notably because they are repeated requests, the Institution may request the payment of reasonable costs to cover the administrative costs incurred in providing you with information, communicating or taking the measures requested. The Institution may also refuse to act on your requests but in that case it will be bound to demonstrate the evidently unfounded or excessive nature of the request (GDPR Art. 12.5).

If you are not satisfied with the way the Institution processes your data you can contact:

- The Data Protection Officer (DPO), an independent body within the Institution, at the address dpo@hubruxelles.be.
- The Data Protection Authority (DPA), to obtain additional information or to submit a complaint
    - Postal address: Rue de la Presse 35, 1000 Bruxelles
    - Tel +32 (0)2 274 48 00, Fax +32 (0)2 274 48 35
    - E-mail : contact@apd-gba.be

The MyHUB application enables you to access and correct your administrative data registered with the Institution. The application enables you to yourself modify your telephone number, email address, contact person and GP details.

Right of access to your data (GDPR Art.15)

Exercising the right of access enables you to know whether your data are being processed and to obtain the communication in a comprehensible format. It also enables you to check that the data are correct and to rectify or erase them if necessary.

The patient or the patient's legal representative can thus exercise their right of access in relation to the following information:

- The categories of data collected;
- The purposes for which these data are being used;
- The categories of recipients who have been able to access these data;
- The time during which data are retained or the criteria that determine this period;
- The existence of other rights (right of rectification, erasure, limitation, objection);
- Any information concerning the source of the data collected if they are not collected directly from you;
- The existence of any automated decision-making, including in the case of profiling, and the underlying logic, significance and consequences of such a decision for you;
- The possible transfer of your data to third country (non-member of the EU) or to an international organisation;
- The possibility of notifying the Data Protection Authority

Right to rectification (GDPR Art.16), restriction of processing (GDPR Art.18) and erasure of your data (GDPR Art.17)

You can request the **rectification** of incorrect or incomplete data concerning you. The right to rectification makes it possible to correct incorrect data concerning you (for example: incorrect age or address) or to complete data relating to the processing purpose.

In regard to medical data, the correct nature of the data must be examined. The data must be rectified or completed if and only if the doctor notes that they are incorrect or incomplete.

As your data controller, the Institution must also communicate to other data recipients details of the rectifications made unless such a communication would require disproportionate efforts.

The right to the **restriction** of processing of your data is foreseen by the GDPR. If you contest the correctness of the data used by the Institution or you oppose the processing of your data, the GDPR authorises the Institution to carry out a check or to examine your request during a certain period. After this period, you have the right to request the Institution to freeze the use of your data that will then no longer be used but will be retained.

Conversely, you can request directly the limited processing of certain data in the case when the Institution itself wants to erase them (for example: images filmed by a surveillance camera). This will enable you to retain the data, for the purposes of exercising a right for example.

In certain cases you have the right to require the Institution **to erase** your personal data as soon as possible.

However, the **right to erasure** does not apply if the Institution is legally obliged to retain the data or insofar as the processing is necessary for reasons of general interest in the field of public health and for dispensing health care and insofar as the data controller is bound to professional secrecy, or if the processing is necessary for the purposes of scientific research.

The right to erasure applies in the case of one of the following reasons:

- If the data are no longer necessary for the purposes for which they were collected;
- If the person concerned withdraws the consent on which the processing is based and there is no other legal basis for the processing;
- If the person concerned opposes the processing and there is no imperious legitimate reason for the processing or the person concerned opposes processing for prospection purposes
- If the personal data have been the subject of illegal processing;
- If the personal data must be erased to respect a legal obligation foreseen by EU or Belgian law;
- If the personal data were collected in relation to the offer of information society services.

Right to data portability (GDPR Art.20)

You have the right to receive the personal data you provided to the Institution in a structured, commonly used and machine-friendly format, and you have the right to transmit these data when the processing is based on consent and it is carried out by automated means.

Regarding your medical data, you may request at any time the transfer of your data in connection with our treatment follow-up.

Right to object to the processing of your data (GDPR Art.21)

You have the right to object to the use of your data for reasons relating to your personal situation when we use them for your legitimate interest or when the processing is based on the public interest or profiling. We will then cease processing your data unless we can demonstrate that there are legitimate and compelling reasons for the processing which override your interests, rights and freedoms or when the data are necessary for the establishment, exercise or defence of legal claims.

Right not to be the subject of automated decision-making (GDPR Art.22)

A fully automated decision is a decision taken in regard to an individual by means of algorithms applied to the personal data without any human intervention in the process.

In the healthcare sector, and in particular in the context of your care, each decision concerning you is validated by a healthcare professional.

15. REQUESTING ACCESS TO OR A COPY OF YOUR MEDICAL FILE

In accordance with the law on patients' rights of 22 August 2002 you have the right:

- To consult your medical file (Art.9§2);
- To request a copy of your medical file or of a part of it (Art.9§3);

Consultation of your medical file is organised as soon as possible and no later than 15 days after receiving your request. You can request to be assisted by a trusted person or ask this trusted person to exercise your right of consultation on your behalf.

Requests for a copy of your medical file or for a part of it are organised within the same maximum period of 15 days from receipt of your request. This copy is strictly personal and confidential. If the professional practitioner has clear indications that the patient is under pressure to communicate a copy of their medical file to third parties, the practitioner can, as a safeguard measure, refuse to provide this copy.

To request consultation of or a copy of your medical file you can send a written request to one of the addresses set out below, depending on your Institution. In the interests of your health data security, proof of your identity will be requested.

- For the Erasmus Hospital: DGM@hubruxelles.be
- For the Jules Bordet Institute: copiedossier@hubruxelles.be
- For the Queen Fabiola University Children's Hospital: courriermedical.huderf@hubruxelles.be

In the case of a **request for a deceased patient**, the law is more restrictive (Law on patients' rights of 22 August 2002, Art.9§4). There is a right of consultation only. This access to the medical file is authorised for the partners, spouses, legal cohabitants or relatives up to the second degree included and provided this has not been opposed by the patient. There must be sufficient and specified

grounds for the request and the consultation must be carried out by the intermediary of a professional practitioner designated by the requester.

16. YOUR HEALTH DATA AND SCIENTIFIC RESEARCH

In accordance with the coordinated law on hospitals and other care establishments of 10 July 2008 (Art.4), the Erasmus Hospital, as a university hospital, is legally mandated to pursue a mission of applied scientific research.

As university hospitals and structures specialised in their respective fields, the Jules Bordet Institute and the Queen Fabiola University Children's Hospital are also mandated to pursue a scientific research activity and endeavour to improve the quality of care and the effectiveness of treatment.

Your data are crucial to help achieve a continuous improvement in care and medical techniques in developing the medicine of the future. Pertinent and encoded data from your file can provide valuable input for the retrospective studies and registers within the H.U.B institutions. The legal bases for the processing of your data in this connection are (i) processing necessary to execute a public interest mission (GDPR Art.6.1.e) and (ii) processing necessary for the purposes of scientific research (GDPR, Art.9.2.j). Additional information on the purposes for which your data will be used in connection with research are available under point 7d.

In the same way, and in accordance with the law of 19 December 2008 on obtaining and using human body material for human medical purposes or for the purposes of scientific research, the Institution may have cause to retain Residual Human Body Material obtained in connection with your care at the time of an act of diagnosis or treatment. This material is residual as following its collection the aims pursued have been achieved and the said residue is redundant and could be destroyed. The Institution retains this material for subsequent purposes of scientific research.

You can object to the processing of your data for the purposes of scientific research as well as the retention of Residual Human Body Material collected in the course of your treatment. There are a number of ways of doing so:

- A document is available at your Institution's reception that you can fill out to indicate your objection;
- On the MyHUB application you can also fill out a form objecting to this data processing
- You can indicate your objection by email, attaching poof of identity, to be sent to dpo@hubruxelles.be

As retaining and using Human Body Material involves a processing of personal data, objecting to data processing for the purposes of scientific research will also imply an objection to retaining and using Human Body Material.

17. CHANGE TO THE PRESENT POLICY

This Private Life Policy for the attention of H.U.B patients enters into force from the date mentioned at the top of this page. It may be updated regularly so as to most effectively reflect the way the Institution processes your personal data.

18. TERMS AND DEFINITIONS

General Data Protection Regulation or GDPR: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/CE (accessible via the following link : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679);

Belgian law on the protection of private life: law of 30 July 2018 on the protection of natural persons with regard to the processing of personal data (accessible via the following link): https://www.autoriteprotectiondonnees.be/publications/loi-cadre.pdf);

Personal data (hereinafter "The Data": Any information or group of information that identifies or renders identifiable a natural person. This can be an identifier such as a name, identification number, location data, an online identifier, etc. It can also be one or more specific elements relating to the person's health or physical, physiological, genetic, mental, economic, cultural or social identity;

Processing: 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;

Data subject: The identified or identifiable natural person whose personal Data are processed;

Controller: The natural or legal person (public body, company, non-profit organisation, etc.) which determines the purposes and means of the processing. In practice and in general this is the legal person embodied by one or more legal representatives.

Sub-Contractor : The natural or legal person who processes the Data on behalf of another body ("the controller"), in connection with a service. For example, the sub-contracting of laboratory analyses, dispatch of mail, etc.

Recipient: The person authorised to receive the Data recorded in a file or a processing by virtue of their functions;

Third party: A natural or legal person, a public authority, a service or a body other than the data subject, the controller, the sub-contractor and persons who, placed under the direct authority of the controller or the sub-contractor, are authorised to process the personal Data. For example, the IMAMI, The mutual companies, the GP, etc.

Data concerning health: Data concerning physical or mental health, past, present or future, of a natural person (including the provision of healthcare) which reveal information about the person's health status. This may be information concerning a natural person collected when registering to benefit from health services or when these services are provided, information obtained at the time of a test or examination of a part of the body or of a bodily substance as well as information concerning an illness, handicap, risk of illness, medical history, clinical treatment or physiological or biomedical status of the person concerned;

Patients : Any natural person to whom care is administered. Donors and receivers are also considered to be a "Patient", notably in the context of an organ transplant, stem cell transplant, insemination, as well as healthy volunteers in relation to clinical trials;

Supervisor: The independent public body charged with overseeing application of the GDPR. In Belgium, this mission is assumed by the Data Protection Authority.

Personal Data breach: Any security incident, whether of ill-intentioned origin or not, and whether intentional or not, which has the effect of compromising the integrity, confidentiality or availability of personal Data;

Pseudonymisation: A security measure that aims to reduce the identifying nature of data while retaining a link between the Data and the individual to which they relate. Pseudonymised Data render it impossible to identify a person directly but make it possible to trace the identity of data subjects solely by means of additional information (for example: a code, an alias, a visit or hospitalisation number, or a sample) that must be stored securely;

Anonymisation: Processing that involves using a set of techniques so as to render it impossible, in practice, to identify the person by any means and this irreversibly.

De-identification: A processing that consists of removing sufficient elements so that the data subject can no longer be identified. The objective is to ensure that the data processed can no longer be used to identify the natural person as a result of recourse to "all means likely to be reasonably implemented" either by the controller or by a third party;

Public health: A notion designating "all elements relating to health, namely health status, including morbidity and disability, the determinants having an effect on the health status, health care needs resources allocated to health care, the provision of, and universal access to, health care, as well as health care expenditure and financing, and the causes of mortality."

***