REGULATIONS GOVERNING THE PROCESSING OF PERSONAL DATA OF PATIENTS OF THE IRIS HOSPITAL NETWORK

I. INTRODUCTION

The Iris network hospitals and all members of their personnel have the stated desire to ensure that you, the patient, is able to expect the greatest possible security regarding the processing of your data by virtue of a set of technical and organizational measures. This documents seeks to set out the methods used for the collection, recording, retention, modification, deletion, consultation and dissemination of personal data on patients, including medical data.

Compliance with medical confidentiality and protection of your private life in regard to any information – medical or otherwise – obtained on the occasion of a consultation or hospitalisation are important bases for the trust you place in us.

Our hospitals principally process your identification data for the purposes of your administrative follow-up and your health data in connection with the provision of care. Under no circumstances are your data processed for commercial purposes.

If you have any questions regarding your personal data, you can address these in writing to the hospital's General Medical Officer or Data Protection Officer at the following address: Institut Jules Bordet 1 Rue Heger Bordet B1000 Bruxelles

II. DEFINITIONS

Personal data: All information relating to an identified or identifiable natural person (hereinafter "person concerned"); is deemed to be an "identifiable natural person" a natural person who can be identified, directly or indirectly, notably by reference to an identifier, such as name, ID number, localisation data, login ID, one of more elements specific to his or her physical, physiological, genetic, psychological, economic, cultural or social identity.

Personal medical data: All information of a personal nature concerning the physical or mental health of a physical person, including the provision of healthcare services, that reveals details of the state of health of this person.

Processing: Any operation or set of operations whether or not carried out with the assistance of automated processes and applied to data or sets of data of a personal nature, such as collecting, recording, organisation, structuring, retention, adaptation or modification, retrieval, consultation, use, communication by transmission, dissemination or any form of making available, comparison or interconnection, limitation, deletion or destruction.

File: Any structured set of personal data accessible according to determined criteria, whether these data be centralised, decentralised or divided on a functional or geographical basis.

Automated processing: All operations carried out in full or in part with the assistance of automated processes and relating to the recording and retention of personal data as well as the modification, deletion, consultation and dissemination of these data.

Data controller: The natural person or legal entity, public authority, service or any other body that, alone or together with others, determines the purpose and means of the processing; when the purposes and the means of this processing are determined by European Union law or the law of a Member State, the data controller may be designated by or specific characteristics applicable to his designation may be laid down by the law of the European Union or the law of a Member State.

Data manager: Person to whom the organisation and implementation of the processing is entrusted.

Subcontractor: The natural person or legal entity, public authority, service or other body that processes the personal data on behalf of the data controller.

Data protection officer (DPO): The data protection officer fulfils the missions imposed by the European General Data Protection Regulation (EU 2016/679).

Patient: Any person who entrusts himself or herself to the hospital with a view to the provision of medical, nursing, psychological or paramedical services. By extension, are also understood by this donors of human body material entrusted to the hospital.

Recipient: The natural person or legal entity, public authority, service or any other body that receives the communication of personal data, whether or not a third party. However, the public authorities that may receive the communication of personal data in the framework of a particular survey mission in accordance with the law of the European Union or the law of a Member State are not considered to be recipients; the processing of these data by the public authorities in question must comply with the applicable regulations regarding data protection according to the purposes of the processing.

Consent of the person concerned: Any expression of a freely given specific, informed and unambiguous desire by which the person concerned accepts, through a declaration or clear affirmative act, that personal data relating to him or her may be the subject of processing.

III. FIELD OF APPLICATION

These regulations are applicable to the processing of personal data concerning patients treated or admitted by an Iris network hospital. They also apply to the processing of data concerning persons whose material is conserved at the HBM (Human Body Material) banks of the Iris network hospitals.

IV. PURPOSE OF PROCESSING AND LEGAL BASIS

The processing of personal data and in particular of medical data concerning patients is permitted in connection with the following purposes:

- Patient care: Every institution is legally bound to keep a patient (medical) file that can be consulted by doctors and a patient (nurse) file that can be consulted by nurses and paramedical staff;
- Patient administration: Monitoring of the hospital stay and treatment of patients, including outpatients, for administrative, accounting and invoicing purposes; ;

- Hospitalisation management;
- Management of human body material banks containing material taken from patients and donors;
- Scientific research ;
- Processing of personal data with a view to guaranteeing the security of persons or goods;
- Recording of medical data of a personal nature imposed by the legally competent authorities;
- Teaching;
- Management of complaints, mediation and disputes;
- Management for statistical purposes;
- Connection to the institution's information systems.

The basis for the above-mentioned processing is

- Execution of a mission of public interest conferred upon the hospital;
- Respect of a legal obligation;
- Legitimate interests pursued by the hospital. In this case we will check that your interests, freedoms and fundamental rights do not take precedence over our interests;
- Performance of a contract;
- Your consent.

Personal data that are not to be used for the above-mentioned purposes may not be collected or processed.

V. IDENTITY OF DATA CONTROLLER

The data controller is the hospital where you are treated.

VI. IDENTITY OF DOCTOR EXERCISING RESPONSIBILITY FOR AND SURVEILLANCE OF YOUR HEALTH DATA PROCESSING

The personal medical data may only be processed under the surveillance and responsibility of the institution's Chief Medical Officer.

VII. PARTICULARS OF DATA PROTECION OFFICER

Particulars of data protection officer (DPO):
dpo@hopital concerned
+ postal address

VIII. CATEGORIES OF PERSONS HAVING ACCESS TO OR AUTHORISED TO PROCESS PATIENT DATA

a) Hospital personnel:

- All doctors and medical students charged with preventive care, diagnosis and treatment of patients; administrative staff duly authorized by doctors to carry out specific tasks linked to their activities;
- Pharmacists and pharmacist assistants in the framework of processes to issue patients with medicines; administrative staff duly authorized by pharmacists to carry out specific tasks linked to their activities;

- Nurses, auxiliary nurses, paramedics, psychologists, medico-technical service technicians, laboratory technicians, who are privy to the medical confidentiality for their functions relating to prevention or care, as well as their interns;
- Physicists in the framework of their own missions linked to care or radioprotection;
- All the doctors, nurses, paramedics, psychologists and medico-technical service technicians in the framework of their teaching missions;
- Medical secretaries duly authorised for the administrative organisation of care and drawing up and communicating reports;
- Social workers who are privy to the medical confidentiality in the framework of their social mission;
- Medical record personnel for the retention, availability flows, and copying of medical information;
- The administrative personnel at reception for the organisation of patient care pathways;
- Personnel responsible for charging-invoicing and disputes for the purposes of managing information on patients in the framework of their mission;
- Researchers in the framework of research having received a favourable opinion from the Ethics Committee;
- The Chief Medical Officer in the framework of his specific missions;
- The IT personnel in the framework of their missions to put into place and maintain software tools and hardware, and to protect data security;
- The mediator designated by the law of 22.08.2002, in the framework of his missions;
- Members of the quality cell, in the framework of their missions
- The hospital hygiene team, in the framework of their specific missions;
- The RHM team, in the framework of their specific missions;
- The data protection officer in the framework of his control missions.

b) External persons:

- The patient concerned while respecting the provisions of the law of 22/08/2002 concerning patient rights;
- Practitioners of the art of healing in a treatment relationship with the patient or appointed by the patient;
- Dispensers of external care, in the framework of care continuity;
- Insuring bodies, within the applicable regulatory and legal frameworks;
- The INAMI [Federal Institute for Health Insurance] within the applicable regulatory and legal frameworks;
- The Federal Public Health Service, within the applicable regulatory and legal frameworks;
- The Institute of Public Health, within the applicable regulatory and legal frameworks;
- The National Cancer Register and the E-Health applications, within the applicable regulatory and legal frameworks;
- Iris-Faitière, in the framework of its approving authority;
- If the situation arises, and in the cases defined by law, the judicial authorities or administrative bodies;
- The other bodies authorised by law (e.g.: organ donating);
- At the request or with the agreement of the patient, any authorised person (e.g.: research, private insurance).

IX. NATURE OF THE DATA PROCESSED AND THE MANNER IN WHICH THEY ARE OBTAINED

Personal data regarding patients are subdivided into:

1. Medical data of a personal nature concerning the treatment provided to patients in the strict sense of the term
2. Administrative data of a personal nature used for the purposes of identification, admission, invoicing, disputes management.
3. Data of a personal nature destined for research.

Nature of data processed	Manner in which the data are obtained
A. Identification data • Name, address, telephone, e-mail • Identifier attributed by treatment manager	By patient administration on admission, at consultation reception or accident and emergency department, from official ID documents
B. Financial details • Identification of insuring bodies and insurance cover and solvency assessment	By patient administration on admission, at consultation reception, by services concerned (invoicing, social service, etc.) Occasionally by care or financial personnel By authorised e-Health sources
C. Personal characteristics • Age, gender, date of birth, place of birth, civil status, nationality, national register	By patient administration on admission, at consultation reception or at accident and emergency department
D. Physical data (height, weight, etc.)	By the doctor(s) responsible for treating the patient, in cooperation with persons privy to medical confidentiality: intern, nurses, paramedical staff, pharmacist, etc.
E. Lifestyle	By the doctor(s) responsible for treating the patient, in cooperation with persons privy to medical confidentiality: intern, nurses, paramedical staff, pharmacist, etc.
F. Psychological data (personality, character, etc.)	By the doctor(s) responsible for treating the patient, in cooperation with persons privy to medical confidentiality: intern, nurses, paramedical staff, pharmacist, etc.
G. Household composition	By patient administration on admission, at consultation reception or at accident and emergency department
H. Racial or ethnic data	By the doctor(s) responsible for treating the patient, in cooperation with persons privy to medical confidentiality: intern, nurses, paramedical staff, pharmacist, etc. By members of the social service and intercultural mediators
I. Data relating to sexual behaviour	By the doctor(s) responsible for treating the patient, in cooperation with persons privy to

	medical confidentiality: intern, nurses, paramedical staff, pharmacist, etc. By members of the social service and intercultural mediators
J. Philosophical or religious convictions	By patient administration on admission By dietitians
K. Medical data • Concerning the physical state of health: patient file, medical report, diagnosis, treatment, test results, handicaps or infirmities, diet, other particular health requirements concerning treatment, travel or accommodation • Medical data concerning the mental state of health: patient file, medical report, information on diagnosis, treatment, test results • Medical data concerning risk situations and behaviour • Genetic data in connection with Human Body Material bank, screening, heredity examination, etc. • Data relating to treatment: data concerning resources and procedures used for medical and paramedical care of patients	By the doctor(s) responsible for treating the patient, in cooperation with persons privy to medical confidentiality: intern, nurses, paramedical staff, pharmacist, etc. By members of the social service and intercultural mediators
L. Judicial data concerning judicial measures	By patient administration on admission or consultation reception By members of social service
M. Identification data of reference person	By patient administration on admission or consultation reception By complaints mediator concerning law on patients' rights
N. Identification data of patient's doctor	By the patient or third parties justified by continuity of care or administrative follow-up By persons directly involved in patient care and duly authorised By members of social service and intercultural mediators
Access to national register	By members of disputes department By members of social service By members of the Medically Assisted Reproduction service

X. PROCEDURES FOR SAFEGUARDING AUTOMATED DATA

Every possible measure is taken to ensure that the data collected are as exact and complete as possible. All technical and organisational measures are also taken to avoid the loss or manipulation of the personal data contained in patient files, as well as to prevent any illicit consultation, changes to or communication of these data.

The safeguarding procedures consist of:

- A backup of information recorded locally, under the responsibility of each user;
- A systematic backup of centralised files and databases by the hospital IT department (administrative data and medical data transmitted temporarily) and by the medical IT departments (laboratory data, imaging, history of summaries, etc.), held for the purposes of data security (confidentiality, integrity, accessibility);
- The backups are obtained on IT supports (tapes, cassettes) that are kept at protected locations
- Data to be deleted have been or will be microfilmed/digitised, in accordance with the legal obligation to retain a patient's file for 30 years. Microfilmed/digitised data are the responsibility of the Chief Medical Officer. These safeguarding procedures are destined to prevent the accidental or illicit destruction of data, the accidental loss of data or illicit access to them, or their illicit modification or dissemination.

XI. DATA RETENTION

Notwithstanding any legal or regulatory provisions, notably in regard to archiving, the following data retention periods apply:

a) Seven years for invoicing data originating in patient files and that have the value of an accounting document;
b) At least 30 years after the last contact with the patient for medical data of a personal nature retained in accordance with the law on hospitals;
c) Five years for all other data contained in patient files

When the data retention time limit as stated above expires, in so far as possible the personal data will be deleted or destroyed within the subsequent 12 months. However, these data may prove necessary for historical, scientific or statistical purposes pursuant to the law of 30 July 2018 on the protection of natural persons in regard to the processing of private data.

However, this destruction will not take place, following the motivated request by the Chief Medical Officer, if it is reasonably established that the retention of personal data concerning patients presents a certain interest for them or other persons (e.g. genetic data) or if the retention is imposed by a legal stipulation or if there is an agreement on the matter between the patient and the Chief Medical Officer.

The data concerned can be retained for an unlimited period in an anonymous form, that is, in such a way that it would be reasonably considered impossible to re-identify the person through data association.

XII. PATIENT RIGHTS

When collecting personal data the patient is informed of the option open to him or her to obtain a free copy of this document and of his or her associated rights

Any patient, on establishing his identity, has a right:

- Of access to his or her data.

Note: If the request relates to a copy of his or her medical file, the request must be addressed to the hospital's Chief Medical Officer in writing accompanied by proof of identity. These data will then be transmitted to the patient no later than 15 days following receipt of this request, on an electronic or paper support. An amount set by the provisions of the RD of 2 February 2007 can be requested from the patient to cover the administrative costs, without this amount exceeding 25 euros.

- To the rectification of his or her data if they prove to be inaccurate or incomplete.
- To oppose the processing of his or her data except if there is a legal restriction.
- To data portability, that is, the transfer of his or her data in the framework of the monitoring of treatment.
- To request the deletion of his or her data except if there is a legal restriction.

N.B.: In order to comply with the law and in the framework of continuity of treatment, certain of the abovementioned rights are limited in regard to health data (for example, they cannot be modified or deleted).

To exercise his or her rights, the patient must write to the data controller at the following address: Institut Jules Bordet 1 Rue Heger Bordet B1000 Bruxelles

At any time the patient also has the right to submit a complaint to the data protection authority (https://www.autoriteprotectiondonnees.be/, contact(at)apd-gba.be).

Regarding the request for access to or a copy of the medical file, the patient must write to the Chief Medical Officer at the following address: Institut Jules Bordet 1 Rue Heger Bordet B1000 Bruxelles