MANAGEMENT OF YOUR PERSONAL DATA

The American Hospital of Paris (hereinafter referred to as the "**organization**" or the "**Hospital**") attaches great importance to respecting your private life and protecting your personal data. The Hospital pledges to process your data in compliance with the General Data Protection Regulation (hereinafter referred to as the "**GDPR**") of April 27, 2016, with the French Data Privacy Act No. 78-17 of January 6, 1978 (*loi informatique et libertés)*, and with other applicable legislation.

The purpose of this document is to inform you about how the Hospital, in its capacity as a data controller, processes your personal data. The specific conditions under which your data is processed within the framework of artificial intelligence systems and clinical research activities are also described.

The Hospital is located at :

American Hospital of Paris
63, boulevard Victor Hugo
92202 Neuilly-sur-Seine
France

✓ Why does the Hospital collect and process your personal data ?

The Hospital collects and processes your personal data in order to:

- Organize your **pre-admission**
- Manage your medical **appointments**
- Ensure the continuity of your **care**
- Create and add to your **health record**
- Manage your **prescriptions** for medication, medical devices and tests
- Organize your **transfer** to another structure when necessary, or your return home
- Create, add to and manage your **administrative file**
- Enable the smooth management of **individual treatment stations, beds, rooms and operating suites**
- Perform **billing**
- Enable the **collection** of Hospital fees
- Steer and carry out **Hospital activities**
- Perform **quality audits** on the management of administrative and medical records
- Evaluate your **satisfaction** level regarding patient amenities and the care provided
- Send written **fundraising appeals**
- Send information about latest Hospital **news**, **events** and **projects**
- Use tools based on **artificial intelligence**
- Participate in **medical research** in connection with clinical studies and trials

Your medical data is consolidated in a secure, confidential **electronic health record** in order to keep track of your medical history and ensure continuity of care for you or your child.

The Hospital may also process your data using tools based on **artificial intelligence algorithms** (diagnostic assistance, enhanced quality of care, automation of administrative tasks), in compliance with the applicable

legislation. The use of AI within our Hospital is systematically subject to human supervision, in order to guarantee the reliability of results.

Unless you choose to opt out, your data can be pseudonymized (first and last names replaced by an alias or code) or anonymized (impossible to identify source) and used for health-related **medical research**. In this case, your data might be compared to data in other databases such as France's national system of health data, if authorized by the competent authorities.

Lastly, as part of its mission to **continuously improve the quality and safety of care**, the Hospital may use personal data from your medical file to evaluate professional practices, analyze adverse events or perform quality audits.

Your data is processed under the strict supervision of authorized personnel in compliance with medical confidentiality standards. When possible, your data is anonymized or pseudonymized.

✓ What are the legal grounds for data processing by the Hospital?

For each purpose listed above, the Hospital processes your personal data in accordance with a predefined legal basis that includes :

- **Consent**: You consented to the processing of your personal data for one or more specific purposes:
  You may withdraw your consent at any time, without providing a reason, by contacting the person or department to whom you gave your consent, or the Data Protection Officer (DPO, contact details below).
  Example: this legal basis makes it possible to share certain information with your primary physician, or enables you to participate in interventional clinical research (research not involving human subjects, reference methodology MR001).

- **Legal obligation**: processing is performed to meet one of the Hospital's legal obligations.
  Example: this legal basis makes it possible to create and retain your patient record in accordance with the retention periods defined in the French public health code, or to track your requests to exercise your rights based on the GDPR.

- **Legitimate interest** of the Hospital: specifically, improving services and monitoring relationships with patients.
  When this legal basis is used, you may opt out at any time by clicking on the "unsubscribe" link provided in an email.
  Example: this legal basis provides the grounds for sending satisfaction surveys, latest Hospital news and events, and fundraising appeals.

✓ What categories of data are most likely to be processed by the organization?

The following types of personal data may be collected :

Identification data such as your last name, first name, email address, mailing address, phone number and photograph

Data about your **personal and professional life** such as your marital status and occupation

Financial data such as your banking coordinates

Health data such as your medical history, diseases, medications, lab results, prescriptions, height, weight and which Hospital department treated you

Fields marked with an asterisk in the forms you fill out are mandatory. If you decide not to share the information requested, this could prevent you from enjoying the full benefit of certain services provided by the Hospital.

If you are providing data on behalf of another person, you pledge to do so with their consent and after informing them of the conditions under which their data is processed.
Example: your health care agent's identification data (last name, first name, phone number)

✓ How long is your data retained?

Your personal data is retained in compliance with the applicable legislation; the retention period is limited to the strict minimum necessary to achieve the goal that its processing is meant to achieve.

Personal data other than health data is retained for a duration defined by the Hospital based on the following criteria: What is the goal of processing? Are you likely to return to our Hospital soon? Might the Hospital undergo an inspection by a supervisory body? Is there a dispute underway between you and the Hospital?

	Type of data	Goal(s)	Legal basis	Retention period
Medical record	Identification data Health data	Provide your medical care	Legal obligation	**20 years** as from your last visit to the Hospital as an inpatient or outpatient or at least until your **28th birthday** or for **10 years** following your death
Administrative record	Identification data Health data	Correctly identify you Organize your pre-admission Manage your medical appointments	Legal obligation	Only for the amount of time strictly necessary to ensure your care. This retention period is identical to that defined for your medical record, as the two records are inextricably linked.

Hospital invoice	Identification data Financial data	Enable billing for hospitalization expenses and physician fees Enable electronic transfer to your local Assurance Maladie office for reimbursements	Legal obligation	**10 years** as from the invoice issue date
Video surveillance	Identification data	Ensure the security of patients and property	Legitimate interest	**30 days**
Hospital news and events	Identification and contact data	Send information about latest Hospital news, events and projects	Legitimate interest	Until the person in question unsubscribes or opts out, **or for 3 years following the last contact with the person**
Internal satisfaction	Identification data Health data	Send satisfaction surveys	Legitimate interest	Until the person in question unsubscribes or opts out, **or for 3 years following the last contact with the person**
Donation requests	Identification data	Send written fundraising appeals	Legitimate interest	Until the person in question unsubscribes or opts out, **or for 3 years following the last contact with the person**
Quality and audits	Identification data Health data	Improve the quality and safety of care Evaluate professional practices Analyze adverse events	Legitimate interest	For the duration of the quality analysis/audit Data is subsequently anonymized
Information request form (website)	Identification and contact data	Respond to inquiries	Consent	Only for the amount of time strictly necessary to fulfill the request, and for **a maximum of two years**
Request to exercise rights	Identification data	Re-contact the person in question to meet their request to exercise a right	Legal obligation	Only for the amount of time strictly necessary to fulfill the request, and for **a maximum of two years**
Job application	Identification data Professional and personal data	Contact job applicants	Consent	Until the position has been filled and for **three months** following completion of the application process
Clinical research (reference methodology MR-001 and certain MR-002 clinical studies)	Identification data Personal life data Health data	Participate in clinical research	Consent	MR-001: until the product studied is released on the market or for up to **two years after the last publication of the research findings** or, in the absence of publication, until the final research report has been signed.

				MR-002: until the **final study report** or until the IVD has been registered with the competent authorities
Clinical research (certain MR-002 clinical studies, MR-003, MR-004, MR-005)	Identification data Health data	Participate in clinical research	Legitimate interest	MR-002: as stated above MR-003: until **the product studied is released on the market** or until the publication of the research findings MR-004: for up to **two years after the last publication** of the research findings or, in the absence of publication, until the final research report has been signed MR-005: only for the time **necessary** for the processing

✓ Who can access your data?

Professionals who work at the Hospital can access only the personal data (not including health data) they need for the purpose of the processing.
Example: to issue a cost estimate prior to your hospitalization, patient advisors have access to some of your data relating to your health insurance and supplemental health insurance coverage. To manage your appointments, secretaries need to access your name, email address and phone number.

Only the **health care professionals on your or your child's care team may access your health data**. Professionals on the same care team may share amongst themselves only the information that is strictly necessary for the purposes of coordination and continuity of care, prevention, medical-social and social monitoring of patients.

To improve the quality of your care pathway, the Hospital may also, with your express consent, need to share this data with health care professionals outside the American Hospital of Paris who are also involved in your care (*example*: your primary physician).

Some of your data may be shared with **authorized third parties** (*example*: Assurance Maladie and supplemental health insurers, police or judicial authorities).

Some data can also be accessed by our **service providers** (sub-contractors) on the Hospital's instructions (*example*: video surveillance tools, management of your patient record, IT service providers). In this case, access to your data is strictly regulated and restricted via a contract that complies with GDPR obligations.

Lastly, unless you have opted out, your data can be shared with our partners as part of **prospective or retrospective clinical research activities**, which respect the reference methodologies defined by the Commission Nationale de l'Informatique et des Libertés (hereinafter referred to as the "**CNIL**"), France's national commission for information technology and civil liberties. You must give your express written consent prior to participating in clinical research involving human subjects (MR001) and certain MR002 clinical studies.

In all cases, professionals access your data strictly for the needs of their assignment and are always required to comply with the relevant confidentiality rules.
The American Hospital of Paris retains your personal data within the European Union (or the EEA). If the Hospital transfers data outside the European Union as part of a service offered by one of its sub-contractors or partners, it will ensure the data transfer complies with the mechanisms specifically designed to protect this type of transfer (Data Processing Agreement, Standard Contractual Clauses, adequacy decisions).

✓ How do physicians practicing at the American Hospital of Paris process your data?

Just like the Hospital, the physicians who work there process your personal data in compliance with the French Data Privacy Act of January 6, 1978 (*loi informatique et libertés*) and with the GDPR.

Depending on your situation and the data processing performed, physicians are considered to be either an independent **data controller** acting for their own needs, or a **joint controller** acting jointly with the Hospital.

Each physician is responsible for processing your personal data for the purpose of **collecting their fees**.

For hospitalizations and consultations, the Hospital and its physicians are joint controllers.

This is the scenario described in the GDPR in which two entities – here, the Hospital and its physicians – are jointly responsible for the processing of your data because they jointly determined the objectives and means of said processing. In tangible terms, the Hospital and its physicians are jointly responsible for the processing of your personal data for the following purposes:

- Your **admission** to the Hospital and the management of your consultation appointments
- **Tracking of your medical history** and updating of your **electronic health record**
- **Prescriptions** for tests, medications and medical devices
- **Referrals** to one or more colleagues, when necessary
- Your **transfer** to another structure when necessary
- M**anagement of** individual treatment stations, beds, rooms and operating suites
- **All decisions** and measures taken as part of your care
- **Retention and archiving** of patient records

As joint controllers, the Hospital and its physicians must comply with all GDPR requirements. Therefore, they must process only the data that is appropriate, relevant and necessary with regard to the abovementioned purposes, and must do so in a fair, lawful and transparent manner. The Hospital and its physicians have signed an agreement precisely defining their respective roles and relationships with regard to the transfer of your personal data and the management of your rights associated with that data.

✓ What are your rights and how can they be exercised?

You have the right to access your data, request its amendment and erasure; restrict its processing, object to it being used in certain cases, and request its transfer. If you wish to exercise these rights, please contact the Hospital's Data Protection Officer (DPO) or your Hospital physician at:

By email: dpo@ahparis.org

By mail: American Hospital of Paris DPO
63, Boulevard Victor Hugo, 92200 Neuilly-Sur-Seine
France

Via the CNIL: You may also lodge a claim with the Commission Nationale de l'Informatique et des Libertés (CNIL), France's national commission for information technology and civil liberties, if you deem that your rights have been breached, via their online form or by mail (Plaintes | CNIL).

Electronic Health Record (Dossier Médical Partagé (DMP))

The electronic health record (hereinafter referred to as "**DMP**") is a secure space for storing your personal medical data such as prescriptions, hospital reports, and lab results. It enables patients to share their personal and medical information with their health care professionals.

First introduced in 2022, a DMP is automatically created for any patient covered by the French national health insurance (Assurance Maladie) when the patient creates their personal profile in a space called "Mon espace santé". All patients, whether they are under or over 18, can have a DMP as long as they do not opt out when creating their profile.

Professionals and health care organizations are required by law to add to their patients' electronic health record after every procedure or consultation, unless the patient has opted out for legitimate reasons.

The American Hospital of Paris complies with this requirement for patients who did not opt out when their profile was created. The Hospital therefore adds to your DMP certain documents relating to your care, including:

- Hospitalization reports
- Lab and imaging test results
- Discharge summary and other related documents
- Medical observations

These documents can only be seen by the authorized health care professionals involved in your care.

You may block a given professional's ability to access and add to your DMP at any time (Section R. 1111-46 of the French public health code). At any time you may also restore this same professional's ability to access and add to your DMP.

You may, for legitimate reasons, opt out of information being added to your DMP (Section R.1111-47 of the French public health code) by informing a Hospital professional.
Example of a legitimate reason: a patient objects to the addition of a document mentioning a hormonal treatment.

Your data:

- Is hosted in France by a certified health data hosting organization (Hébergement de Données de Santé – HDS)
- Can only be accessed using a health care professional card (carte de professionnel de santé – CPS)
- Cannot be modified after it has been added to the DMP

To exercise your right to access, amend, erase, restrict and/or object to processing as well as your right to data portability, please contact the director or DPO of your local Assurance Maladie office.

American Hospital of Paris

Specific information on the use of artificial intelligence in patient care

The Hospital may use artificial intelligence (AI) technology as part of its patient care and more generally for the overall management of Hospital activities.

✓ Why does the American Hospital of Paris use AI?

AI technology is implemented in order to offer you the best possible care.

AI tools make it possible to:

- Improve the precision and efficacy of medical diagnoses made by health care professionals
- Identify the most appropriate treatments and make informed medical decisions
- More generally speaking, help manage and steer Hospital activity and optimize financial planning

For example:

- AI can be used in the analysis of medical images such as x-rays, MRIs and CT scans
- AI algorithms can help doctors detect or predict abnormalities and disease by identifying tumors, fractures and other pathological conditions

✓ What types of safeguards does the Hospital offer?

The Hospital attaches great importance to the ethics of using AI in health care.

The Hospital's use of AI is systematically subject to human supervision, in order to guarantee the precision and reliability of results.

This means that final decisions regarding your diagnosis, treatment and all other medical decisions are always made by qualified health care professionals who use AI-induced recommendations as a decision-making tool.

In addition, robust security measures are implemented within the Hospital and by our partners in order to guarantee the confidentiality of your personal data and protect it against any unauthorized access, loss or accidental disclosure. We always ensure that the AI systems used in our organization strictly comply with the ethical and regulatory standards in force (*example*: ethical seal of approval criteria, audit and traceability mechanisms, algorithm transparency, non-discrimination/equity measures).

If you have any questions about the Hospital's use of AI, please speak to the physician who provided your care. They will be able to explain to you in detail if and how AI is used in their department, the expected benefits of such us and any consequences that may arise from opting out of such use. If you have difficulty exercising your rights, please contact the Organization's Data Protection Officer (dpo@ahparis.org).

Specific information about your rights regarding the use of your personal data for medical research

Data collected by the Hospital is used to conduct research aimed at improving the quality of care, through research performed either in-house by a care team (single center) or externally (multicenter).

Some research also implies the development and improvement of artificial intelligence algorithms.

Regarding the Hospital's partnerships (in particular with medical training and research centers and the Paris public hospital network), only pseudonymized or anonymized data can be shared with external partners involved in the research.

The findings of these research projects (results, scores, algorithms, aggregated data) may be included in scientific publications.

At any time and without providing a reason, you may choose to opt out of your data being used for research by contacting the CEO of the American Hospital of Paris. This will have no impact whatsoever on the quality of the medical care you receive or on your relationship with the Hospital physician. You may also write to the Hospital's Data Protection Officer (dpo@ahparis.org).