ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Εθνικόν και Καποδιστριακόν Πανεπιστήμιον Αθηνών
ΙΔΡΥΘΕΝ ΤΟ 1837

ΑΡΕΤΑΙΕΙΟ ΝΟΣΟΚΟΜΕΙΟ

Privacy Notice Addressed to Patients about the Processing of their Personal Data

The **'National and Kapodistrian University of Athens – Aretaieio Hospital'** (hereinafter referred to as the **'Hospital'** or **'we'**) respects the importance of protecting your personal data and their lawful and fair processing. Acting as Data Controller, the Hospital hereby informs you about the collecting, using, handling and storing of your data, adopting additional measures to ensure that it fully complies with the requirements of the General Data Protection Regulation (EU) 2016/679 (hereinafter referred to as the 'GDPR').

1. Our commitments

The Hospital undertakes the following commitments regarding the protection of your personal data:

- ✓ We retain correct and updated information regarding your personal data to provide you with our services and fulfill our legal obligations in relation to you.
- ✓ We keep your data safe and accurate.
- ✓ We retain your information as long as necessary to fulfill our obligations, and as provided by law, on a case-by-case basis.
- ✓ We collect, store, and use the information provided by you as required by the data protection standards and by the laws governing the protection of your data and your rights.
- ✓ We inform you if there is a destruction, alteration, loss (breach) of your personal data, which may result in a high risk regarding your rights and freedoms. The information can be provided personally and/or, if it concerns many people, on the Hospital's website.
- ✓ We fully comply with the GDPR, which requires that we handle your personal data in a fair, legal and transparent manner.

2. Categories of personal data

In order to provide health services to you, we may collect your personal data directly from you, as a patient, or from your companion/relative, or from Public Services or Third Parties (e.g. the National Organization For Health Care Services-EOPYY, the National and Kapodistrian University of Athens, doctors, other hospitals, laboratories, etc.). In particular, the categories of your personal data that we may process during your hospitalization are the following:

- Basic data (e.g. name, surname, date of birth, phone number, etc.)
- Unique identifiers (e.g. ID Number, VAT Number, Social Insurance Number, etc.)

- Health data (e.g. health condition, diagnosis, type of medical examination requested, medical history, sonographies, medication, Social Insurance Number, personalized patient nutrition, laboratory tests, date of surgery, surgical products, results of the sample analysis, etc.)
- Insurance data (e.g. insurance registration number, insurance agency, uninsured status, etc.)
- Identification data (e.g. patient registration number, patient reference number, file number, etc.)
- Sample data (e.g. blood sample, urine sample, etc.)
- Image data (e.g. x-ray, Computed Tomography-CT scan, sonographies, Magnetic resonance imaging-MRI scan, surgery pictures, etc.)
- Financial data (e.g. hospitalization costs, examination costs, IBAN, etc.)
- Social background data (e.g. marital status)
- Employment data (e.g. occupation of the patient)

3. Purposes of processing your data and legal bases of processing

The personal data collected by the Hospital are being processed exclusively for the purpose of:

a) The provision of health services to both out-patients and in-patients and their clinical management

b) The monitoring of your condition after your treatment

c) The management of your nutrition

d) The handling of your requests for certificates and the management of such certificates

e) The management of your financial debts

f) The provision of documents to the insurance funds

g) The provision of patients counselling

h) The optimal operation of the Hospital's infrastructure (e.g. management of the reception, the call center and the parking area)

i) The storage of data for educational and medical research purposes

j) The costing of the hospitalizations/archiving

k) The drafting of hospitalization certificates and/or hospitalization costs

l) The registration of newborns

m) The adoption of decisions by the Hospital's Governing Body ('Eforeia')

n) The management of applications and registration

o) The management of exclusive nurses

p) The management of the Hospital's medical equipment

q) The management of supplies

Regarding the processing of the non-sensitive personal data, the following legal bases apply in relation to the abovementioned purposes:

1. The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Hospital, in the context of the Hospital's given powers and public interests, as they arise from its Organisation as a public body, for the purposes of processing with reference points a), b), c), d), e), f), g), h), i), j), k), m), n), p) and q).

2. The processing is necessary for the Hospital's compliance with legal obligations to which it is subject, as they arise from the legislation applicable to the Hospital's function, for the purposes of processing with reference points k), l), n) and o).

3. The processing is necessary to protect the vital interests of the data subject or of another natural person, for the purpose of processing with reference point a).

Regarding the processing of sensitive personal data (health data), the following legal bases apply in relation to the abovementioned purposes:

1. The processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 9.3 of the GDPR, for the purposes of processing with reference points a), b), c), d), e), f), g), h), k), m), n), o) and q).

2. The processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Hospital as Controller or of the data subject in the field of employment and social security and social protection law, in accordance with applicable law, for the purposes of processing with reference points j) and m).

3. The processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, in particular professional secrecy, for the purposes of processing with reference points n) and p).

4. The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard your fundamental rights and interests, for the purposes of processing with reference points i) and l).

It is noted that:

- ✓ Your personal data are not further processed beyond the above purposes. If it becomes necessary to further process your data for purposes other than those listed above, we will inform you accordingly.
- ✓ Your personal data are subject to the obligation of professional secrecy.

4. Data retention period

Your medical file is retained for a period of twenty (20) years from the date of your last visit. However, your personal data may be stored for a different period, proportional to the relevant processing purpose.

5. Recipients of your data

Recipients of your personal data are the necessary, in any case, employees of the Hospital, who have been fully and appropriately informed on the secure processing of your personal data.

Furthermore, recipients of your data are:

- Natural and legal entities, to which the Hospital entrusts the execution of specific tasks on its behalf such as medical equipment companies, providers of technological equipment maintenance services, providers of application maintenance services, audio transcript companies, providers of security services, collaborating laboratories and external partners for consultation. These partners, which act as data processors, have been informed and committed in advance to the confidentiality of your data, and they know and follow our instructions regarding the processing of personal data taking all the appropriate and necessary measures to protect them.
- Doctors, other hospitals, researchers, universities-Special Account for Research Funds (ELKE), the National Public Health Organization, courier companies, insurance funds (e.g. the National Organization For Health Care Services-EOPYY), suppliers of materials, various Centers-Institutions (competent for specific diseases), which act as independent Controllers by virtue of the nature and manner of providing their services.
- Supervisory, auditing, independent, judicial, public and/or other authorities and bodies within the framework of their statutory powers and duties (such as the Ministry of Health, the Tax Office, etc.) when the data transfer to them is required or established by law.
- Lawyers, law firms, bailiffs, experts, in case of legal actions in the context of safeguarding our rights and interests, or if this is required by legislative provisions or court decisions or regulatory decisions issued by the Hellenic Personal Data Protection Authority or by other independent authorities.
- Any other recipient to which the transfer derives from a legal obligation of the Hospital, or which has a right provided by law to receive your data.

6. Transfers of personal data to third countries or international organizations outside the European Economic Area (E.E.A.)

Your data are being processed only within Greece, and they are not transferred outside E.E.A.

7. Your Rights

According to the GDPR, you, as a data subject, have the following rights that can be exercised on a case-by-case basis:

- **The Right to access your personal data**
  You have the right to receive from the Hospital as data controller confirmation as to whether or not your personal data are subject to processing, as well as to have access to the

information related to the manner of the processing of your personal data (e.g. processing purpose, categories of data, recipients, retention period etc.) as well as receive a copy of your data.

- **The Right to rectification**
  You have the right to request from the Hospital to correct inaccurate data without undue delay, as well as the right to have incomplete personal data completed, even by submitting a supplementary statement.
- **The Right to restriction of processing**
  You have the right to ensure that the Hospital restricts the processing of your data exclusively to their storage, under the conditions provided by the GDPR.
- **The Right to object to the processing of personal data**
  You have the right to object to the processing of your data, at any time and for reasons related to your status.
- **The Right to erasure ('right to be forgotten')**
  You have the right to request from the Hospital the deletion of your personal data when the processing is unlawful or is no longer required to achieve the above purposes. However, under the GDPR, this right may not be applicable to data processing in the field of healthcare provision services, in cases of complying with a legal obligation or fulfilling a task performed in the public interest or in the exercise of official authority vested in the Hospital and/or for reasons of public interest in the area of public health in accordance with Article 9.2 h) and i) and 9.3 of the GDPR.
- **The Right to data portability**
  You have the right to receive the personal data that you have provided to us in a structured, commonly used, and machine-readable format as well as the right to transfer such data to another data controller without any objection from the controller to which the personal data were originally provided. However, under the GDPR, this right does not apply to the processing carried out in cases of complying with a legal obligation or fulfilling a task performed in the public interest or in the exercise of official authority vested in the Hospital, and thus, if you exercise this right, it may not be fulfilled.
- **The Right to withdraw your consent**
  In cases where the processing of your data is based on your previous consent, you have the right to withdraw your consent so that the processing will not continue in the future. Please note that in the context of the above purposes, your consent is not requested for the processing of your data, and thus, the right to withdraw consent does not apply. It is also noted that consent to the processing of personal data is different from the consent you may be asked to give regarding the performance of medical acts.

Please note that the Hospital may not be able to fulfill your abovementioned rights, to the extent that the legal conditions for their fulfillment are not met or there are exceptions deriving from the provisions of the GDPR.

8. Exercising your Rights

If you wish to receive further information regarding the processing of your personal data or exercise any of your abovementioned rights, you may contact the Hospital:

- Via post to the address: Vasilissis Sofias 76, Postal Code 11528, Athens, referring to the Data Protection Officer (DPO)

- Via email to the Data Protection Officer (DPO) of the Hospital, at the email address dpo@aretaieio.uoa.gr.

Our response to your request will take place within (1) one month of its receipt and it does not incur any cost for you. The above period may be prolonged for a period of two (2) additional months, due to the complexity or the number of the requests. In such case, you will be duly informed about the time extension and the reasons for it as soon as possible and at the latest within a month after receiving your request.

In case you consider that: a) your request has not been sufficiently and lawfully satisfied or b) your right to the protection of your personal data has been violated by our processing, you have the right to lodge a complaint with the supervisory authority, i.e. the Hellenic Data Protection Authority (address: Kifissias 1-3, Postal Code: 115 23, Athens, https://www.dpa.gr/, telephone number: 210 6475600, email address: contact@dpa.gr).

End of text