PRIVACY NOTICE
Last Updated: November 2024

This Privacy Notice explains what personal data The Kenya Hospital Association (**trading as The Nairobi Hospital** and hereafter "**TNH**", "**we**" or "**us**") as a data controller will collect, hold, use, share and discard data about you (the "**data subject**").

We are required to notify you of this information, under data protection legislation.

Please ensure that you read this Notice and any other similar Notice we may provide to you from time to time when we collect or process personal data about you.

We may update this Notice from time to time without notification to you.

This privacy notice tells you what to expect us to do with your personal information.

The Data Protection Principles We Uphold

TNH will:

- Process your data lawfully, fairly and in a transparent manner (**Lawfulness, Fairness and Transparency**);
- Collect your personal data only for specified, explicit and legitimate purposes, and will not process it in a way that is incompatible with those legitimate purposes (**Purpose Limitation**);

- Only process the personal data that is adequate, relevant and necessary for the relevant purposes (**Data Minimisation**);
- Keep accurate and up to date personal data, and take reasonable steps to ensure that inaccurate personal data are deleted or corrected without delay (**Accuracy**);
- Keep personal data for no longer than is necessary for the purposes for which the data are processed (**Storage Limitation**);
- Process data securely to protect it against unauthorised or unlawful processing, and against accidental loss, destruction or damage throughout its life cycle by implementing appropriate technical and organisational measures (**Confidentiality and Integrity**); and
- Be responsible for the protection of your data and be able to show compliance with relevant laws (**Accountability**).

Our Lawful Bases for Processing Your Data

We must have lawful reasons to process your personal data. The lawful bases we rely on are as follows:

Consent	You give us explicit permission which is clear and informed to process your data for a specific reason. All your data protection rights may apply, except the right to object. To be clear, you have the right to **withdraw your consent at any time**.
Contract	We have to process the data in order to enter into or carry out a contract with you. All your data protection rights may apply except the right to object.
Legal Obligation	We have to process your data in order to comply with the law.

	All your data protection rights may apply, except the right to erasure, the right to object and the right to data portability.
Legitimate Interests	We process your data because it benefits you, our organisation or someone else, without causing an undue risk of harm to anyone. All your data protection rights may apply, except the right to data portability.
Vital Interests	We apply this basis when your physical or mental health or wellbeing is at urgent or serious risk, often life-threatening. All your data protection rights may apply, except the right to object and the right to data portability.
Public Interest	If there is a law that requires us to process some data for the benefit of the public, we are obliged to do so. All your data protection rights may apply, except the right to erasure and the right to data portability.
Historical, statistical, journalistic, literature, and art or scientific research	We will collect data where it is necessary to: (a) advance knowledge on health and diseases; (b) preserve and study historical events; and (c) monitor trends to predict and control any disease outbreaks.

Data We Collect and Hold

We collect your **Personal Data** which is any information relating to an identified or identifiable natural person/individual.

As a hospital, we **may** collect data to provide certain goods and services to you as follows:

- **Identity Data** includes your name, marital status, title, date of birth, gender, identification card (ID), passport, birth certificate and any other biographical information you may provide us.
- **Contact Data** includes home address, email address and telephone numbers of both the data subject and their next of kin, emergency contact(s) or guardian(s).
- **Financial Data** includes bank account data, payment card details, insurance policy details.
- **Transaction Data** includes details about payments to and from you and other details of events, products or services you have purchased from us or gifts you have donated to us.
- **Technical Data** includes internet protocol (IP) address, website usage through cookies and other technology on the devices you use when you visit the hospital website.
- **Marketing and Communications Data** includes your preferences in receiving marketing from us and our third parties and your communication preferences.
- **Sensitive Personal Data** includes details about your race or ethnic origin, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, health data (including medical conditions, allergies, medical requirements, medical history and test results) and genetic and biometric data.
- **Safety Data** which includes photographs, video footage, data collected during incident investigation, as well as reports and accident book records.

Where we need to collect personal data to perform a contract we have or are trying to enter with you, and you decline to provide that information, we may not be able to perform that contract.

How We Collect Your Data

- Directly from you – when you fill admission forms, contracts, correspond with us, opt to receive marketing information, visit our website, apply to be a consultant, apply for employment/internship.
- Next of Kin, Guardians, Family Members, Surrogates or Guarantors.
- Other healthcare providers – when sharing medical records about you.
- Social services.
- Schools, colleges, universities or other education organisations – when you join or transfer into the College.
- CCTV footage or other recordings – from our cameras which are installed to ensure security.
- Insurance companies and corporates – when dealing with payment details.
- Previous employers – when you join the hospital for references.
- Suppliers and service providers – procurement process.
- Hospital Q Management system.

When We Disclose/Release Your Data

We may also need to disclose/release some of the above categories of personal data to third parties as follows:

- Other healthcare providers like medical consultants.
- Insurance companies, brokers and other intermediaries.
- Relevant legal or regulatory authorities.
- Future or previous employers according to human resource practice.
- Suppliers and service providers.
- Next of Kin – where there is a threat to life.

We make efforts to ensure that data recipients have similar standards of data protection.

We may also be required to disclose/release some personal data to the Office of the Data Protection Commissioner as required to comply with the law.

How Long We Keep Your Data

We hold your data both at our offices for physical records and in the cloud for digital records. We do not keep your data for longer than is necessary and only for the purposes for which it is processed.

How long we keep your data will depend on the nature of the data collected.

Your Rights

You have a right to:

- know how we will use your personal data;
- access the personal data we hold about you;
- have your data rectified if the information we hold is inaccurate, incomplete or requires to be updated;
- restrict the processing of your data – the data we hold will only be processed for the purpose for which it was collected;
- ask that we erase or delete the data we hold about you;
- object to the processing of your personal data;
- request transfer of your personal data (data portability); and
- not to be subjected to a decision made only through automated processing.

You can exercise your rights at any time by contacting the Data Protection Officer.

Keeping Your Personal Data Secure

We always take the utmost care to protect your personal data.

We have appropriate technical and security measures to prevent personal data from being accidentally lost, used inappropriately, or accessed by unauthorised persons.

We anonymise your data to ensure your protection.

We limit access to your personal data to those who have a genuine business need to know it. Only authorised officers or agents or representatives will handle your data and are subject to a duty of confidentiality.

We have procedures in place to deal with any suspected data security breach. We will notify you and the Office of the Data Protection Commissioner where we are legally required to do so.

Contact Us

We hope that our Data Protection Officer can provide further information and resolve any query or concern you raise about our use of your data.

Please contact us at dpo@nbihosp.org.