POLICY DOCUMENT

1.0 DOCUMENT DESCRIPTION

Status	Active
Number	GCH/MOI/POL/4/1
Title	Healthcare Privacy Policy
Type	Policy
Author	Chief Information Officer
Approved by	ICT Committee
Version	1
Active Date	February 1, 2014
Reviewed	March 11, 2024
Next Review Date	February 1, 2026
Accessed by	All Staff
Availability	Electronic copies
Custodian	Chief Information Officer

1. IMPORTANT INFORMATION

1.1. At Gertrude's Children's Hospital ("**Hospital**", "**we**", "**us**", "**our**"), our primary goal is to deliver exceptional paediatric healthcare services. To accomplish this, it is necessary for us to collect, use, disclose, transfer, and retain (in other words, **process**) information relating to you, whether you are a patient, family member, caregiver, or visitor, for purposes of the care we have provided or plan to provide.

1.2. This Privacy Policy lets you know what happens to any **personal data** that you may give us or that we may collect from you (or about you or the patient). This Policy is issued by the Hospital as a healthcare provider, and covers the data we hold about our future, current, and former patients, their families, and other individuals who may use our services.

1.3. This Privacy Policy will also inform you about your privacy rights and how the law protects you in accordance with the provisions of the Data Protection Act, 2019 (the **Act**).

1.4. This Privacy Policy does not form part of any contract we have with you to provide services.

1.5. It is crucial that you read this Privacy Policy alongside any other relevant privacy policies or notices that we may provide on specific occasions when collecting or processing your personal data, or the personal data you provide. This ensures that you have a comprehensive understanding of how and why we utilize your information. This Privacy Policy complements such other privacy policies and notices and is not intended to supersede them.

1.6. We will regularly review our Privacy Policy. This version was last updated on February 2024.

2. WHO WE ARE

2.1. The Hospital is a "***data controller***" in relation to the processing activities described below. This means that we determine the purpose and means of processing your personal data (or personal data you provide).

2.2. The Hospital is registered as a "*data controller*" with the Office of the Data Protection Commissioner.

2.3. Our Data Protection Committee (DPC) is responsible for our data protection function. You can find contact details for our DPC Department team at the end of this Privacy Policy.

3. THE TYPES OF PERSONAL DATA THAT WE COLLECT AND PROCESS

3.1. "**Personal data**" means any information that can be used to identify an individual natural person. Please note that there are "**special categories**" of personal data that are more sensitive and require a higher level of protection. The personal data we collect will vary according to the circumstances surrounding our relationship with you.

3.2. We will collect, use, store, transfer or otherwise process personal data about you (or persons connected to you including):

(a) **Personal details about parents/ care-givers/ guardians**: name, title, gender, nationality, marital status, date of birth, age, national identification/passport number, addresses, telephone numbers, personal email addresses, ID photograph, place of work, details of the third party with parental responsibility over the patient, emergency contact information,

bank account details, medical insurance information, and information about other family members related to the patient.

(b) **Health details about parents/ care-givers/ guardians:** details of your or your family's previous and current medical history that is relevant for the patient's treatment.

(c) **Personal details about patients**: name, address, date of birth, place of birth, gender, age, race, religious or other beliefs, medical insurance information and information about any disability.

(d) **Health details about patients:** current and previous medical conditions, details and records of treatment and care/ notes, health reports including any allergies or health conditions; related information from research/ clinical trials; results of x-rays, scans, blood tests, or any investigation, genetic information, biometric information, vaccination history and status, and any previous contact that the patient has had with the Hospital through appointments, attendance, or inpatient stays.

(e) **Third parties connected to the patients:** any relevant information about third parties who care for the patient and know them well, such as health professionals, social workers providing social care services, relatives, and care-givers as well as information about any sponsors who will be funding the patient's treatment.

(f) **Monitoring information** such as:

(i) information about your use of our information and communications systems, including your website and system interaction (cookies, internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and similar technologies),

(ii) information about your use of the Hospital's facilities,

(iii) information received in response to any surveys or complaint claims,

(iv) information gathered through CCTV and building access information.

(g) **Marketing and communications data**: your preferences for receiving marketing from us and our third parties and your communication preferences.

3.3. Please note that by providing us with any personal data about a third party, you will be confirming

(a) that you have obtained the necessary consent from those third parties to the use of their personal data, and

(b) that the third parties are aware of your actions.

4. WHAT HAPPENS IF YOU FAIL TO PROVIDE THE REQUESTED PERSONAL DATA?

If you do not provide us with the requested personal data, we may be unable,

(a) to perform the contract that we have with you (such as providing the patient with healthcare services), or

(b) to comply with our legal obligations as a healthcare provider.

5. HOW DO WE COLLECT YOUR PERSONAL DATA (OR PERSONAL DATA YOU PROVIDE)?

5.1. We may collect or receive your personal data (or personal data relating to your personal relations) in a number of different ways:

(a) Where you provide the personal data directly to us, for example:

(i) corresponding with us by phone or email or any virtual platform;

(ii) completing forms provided by the Hospital such as the inpatient admission form and the relevant insurance cover form,

(iii) during the course of your relationship with us when accessing or using any of our services,

(iv) using or registering to use our website (https://www.gerties.org/).

(b) From another healthcare professional you or the patient has seen when the healthcare professional refers the patient to the Hospital for treatment,

(c) From third parties, such as other hospitals, outsourced service providers such as the Hospital's independent consultants, laboratory and diagnostic entities, insurance providers, mental health provides, referral agencies, sponsors, and government departments and agencies,

(d) From publicly available sources including but not limited to internet search engines, public records and registers and social media accounts (e.g., *Facebook*, *LinkedIn*, and *Twitter*),

(e) By generating additional information about you or the patient during the period of the patient's treatment with the Hospital, and

(f) Where you provide the personal data indirectly to us through monitoring devices or by other means (for example, building and location access control and monitoring systems, CCTV, telephone logs and recordings, instant message logs and email and internet access logs), if and to the extent authorised by applicable laws.

5.2. Generally, you have no obligation to provide us with your personal data (or personal data you provide), but if you do not provide us with the information we need, we may be unable to provide you with services.

5.3. We will seek to minimise the amount of information we request for, to only that which is needed to perform the relevant function or service at the time.

6. HOW DO WE USE YOUR PERSONAL DATA (OR PERSONAL DATA YOU PROVIDE)?

6.1. Subject to applicable law including the Act, we may store and process your personal data (or personal data you provide) to support the delivery of appropriate healthcare and treatment as well as for the following purposes:

(a) **Supervision and administration of the patient's treatment by the Hospital including:**

(i) To help inform decisions that we make about the patient's care and treatment.

(ii) To ensure that the patient's treatment is safe and effective.

(iii) To work effectively with other organisations who may be involved in the patient's care and treatment.

(iv) To remind you about appointments and send you correspondence.

(v) To respond to your inquiries, challenges or requests for feedback received in relation to our care and treatment.

(vi) To monitor programmes that require us to ensure equality of opportunity and diversity.

(b) **Continual administration and oversight of the Hospital's operations including:**

(i) To support the health of the general public and ensure our services can meet future needs.

(ii) To review our care and treatment to ensure it is of the highest standard possible as well as evaluate our current care policies and procedures.

(iii) To train healthcare professionals.

(iv) To conduct clinical research and audits to enable us to understand more about disease risks and causes, improve diagnosis, develop new treatments, and prevent disease.

(v) To prepare statistics on hospital performance.

(vi) To evaluate government policies and to comply with our legal and regulatory obligations as well as following guidance and best practice issued by healthcare bodies.

(vii) To support the funding of our operations.

(viii) To respond to any inquiries, challenges or requests for feedback received in relation to our care and treatment.

(ix) To operate security, governance, audit and quality assurance processes and arrangements.

(x) To compile statistics and conduct research for internal and statutory reporting purposes, for business improvement, and to support changes to service delivery.

(xi) To fulfil and monitor our responsibilities under the various laws of Kenya.

(xii) To communicate effectively with you by post, email, and phone. Where appropriate you will be given the opportunity to opt-out of receiving some communications from us.

(xiii) To comply with our obligations to funders and sponsors (including our disclosure obligations under their terms and conditions and policies).

(xiv) To manage and maintain your information in hard copy records, files, and systems, including technical support and maintenance of the Hospital's systems and managing electronic and hard copy records in line with our retention schedules.

(xv) For business contingency planning and in response to active incidents.

(c) **Compliance monitoring, security and systems use including:**

(i) Measuring the performance of our IT systems by monitoring your usage of our systems; this includes analysing time, locations, and activities whilst users are logged into our network.

(ii) Auditing, monitoring, investigation, and compliance monitoring activities in relation to our policies, codes of conduct, applicable law, the prevention, and detection of criminal activity and to protect our assets and premises.

(d) **Responding to legal and regulatory requests including:**

Complying with lawful requests by public authorities or where otherwise required or authorised by applicable laws, court orders, government regulations, or regulatory authorities (up to and including without limitation data protection, and tax), whether within or outside this country.

7. LEGAL BASIS FOR PROCESSING YOUR PERSONAL DATA (OR PERSONAL DATA YOU PROVIDE)

7.1. We will only collect, use, and share your personal data (or personal data you provide) where we are satisfied that one of the following legal grounds apply to a specific processing activity:

(a) The processing is necessary for us to comply with a **legal obligation** to which we are subject, for example, complying with public health requirements, defending a legal claim, complying with statutory record keeping and reporting requirements for health and safety obligations.

(b) The processing is necessary for the **performance of a contract** to which you are a party or to take steps, at your request, prior to entering into such a contract, for example collecting your personal data (or personal data you provide) to provide care and treatment to the patient and the associated billing, accounting, audit, and payment verification.

(c) The processing is based on your **consent**. Where consent is required for the processing in question, it will be sought from you separately to ensure that it is freely given, informed and explicit.

In the limited circumstances where you have consented to the processing of your personal data (or personal data you provide) for a specific purpose, you have the right to withdraw your consent at any time. Please note that withdrawing your consent, does not render unlawful our prior handling of your personal data (or personal data you provide) or the processing which is based on other legal justifications.

(d) The processing is necessary for the **legitimate interests** pursued by us or by a third party, except where such interests are overridden by your interests or rights and freedoms which require protection of personal data. We believe that we have a legitimate interest in processing personal data for the purposes set out above, and to support the achievement of our immediate and long-term business goals and outcomes.

(e) The processing is necessary to **protect your interests** (or **someone else's interests**).

(f) The processing is necessary to perform a task carried out in the **public interest or for official purposes**.

7.2. Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal data (or personal data you provide).

7.3. In summary, we will process your personal data (or personal data you provide) for the purposes and on the basis of the legal bases set out in the table below:

Purpose of Processing	Personal Data	Lawful Basis for Processing
Supervision and administration of the patient's treatment by the Hospital	• Personal details about parents/ care-givers/ guardians • Health details about parents/ care-givers/ guardians • Personal details about patients • Health details about patients • Third parties related to the patients • Monitoring information • Marketing and communications data	Contractual performance Legitimate interest Compliance with a legal obligation
Continual administration and oversight of the Hospital's operations	• Personal details about parents/ care-givers/ guardians • Health details about parents/ care-givers/ guardians • Personal details about patients • Health details about patients • Third parties related to the patients • Monitoring information • Marketing and communications data	Contractual performance Legitimate interest Compliance with a legal obligation Consent
Compliance monitoring, security and systems use	• Personal details about parents/ care-givers/ guardians • Personal details about patients • Monitoring information	Contractual performance Legitimate interest Consent Compliance with a legal obligation
Responding to legal and regulatory requests	• Personal details about parents/ care-givers/ guardians • Personal details about patients • Health details about patients • Third parties related to the patients	Contractual performance Compliance with a legal obligation Legitimate interest

8. CHANGE OF PURPOSE

8.1. We will use your personal data (or personal data you provide) solely for the purposes for which it was collected, unless we reasonably believe that we need to use it for another reason that is compatible with the original purpose.

8.2. If we need to use your personal data (or personal data you provide) for an unrelated purpose, we will notify you, explain our legal basis for the change and obtain your consent to process your personal data (or personal data you provide) for that unrelated purpose.

8.3. Please note that we may process your personal data (or personal data you provide) without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

9. COOKIES

9.1. Please note that in order to improve our internet service to you, we will occasionally use a “cookie” and/or other similar technologies which may place certain information on your computer’s hard drive when you visit our website or any of the Hospital’s affiliated websites.

9.2. A cookie is a small amount of data that our web server sends to your web browser when you visit certain parts of our site.

9.3. We use cookies to do many different jobs, like letting you navigate between pages efficiently, identifying you after you have logged in by storing a temporary reference number in the cookie, allowing you to access stored information if you register for any of our online platforms, and generally improving your online experience.

9.4. Cookies do not enable us to gather personal information about you unless you give the information to our server. Most Internet browser software allows the blocking of all cookies or enables you to receive a warning before a cookie is stored.

10. WHO DO WE SHARE YOUR PERSONAL DATA (OR PERSONAL DATA YOU PROVIDE) WITH?

10.1. We will disclose your personal data (or personal data you provide) to:

(a) other relatives, care-givers, guardians, or representatives of the patient who are involved in the patient’s care,

(b) healthcare professionals and providers involved in the patient’s care,

(c) public health agencies and authorities.

(d) other hospitals involved in the patient's care,

(e) referrals such as to specialists,

(f) funders and sponsors of the Hospital,

(g) sponsors of a patient’s care at the hospital,

(h) our external service providers where we outsource certain services such as the Hospital’s independent consultants, IT service providers, payment processors such as banks, administrative service providers and third-party debt recovery agencies,

(i) research organisations,

(j) laboratory and diagnostic entities involved in the patient’s care,

(k) pharmacies involved in the patient’s care,

(l) insurance companies related to a patient,

(m) any other relevant professional or statutory regulatory bodies such as the Kenya Medical Practitioners Pharmacists and Dentists' Union (KMPDU),

(n) third parties such as external accountants, auditors, external legal teams, regulators, and other professional bodies. We will do this so that we can comply with any legal obligations,

(o) third parties for our legitimate interests such as where we restructure or buy or sell our business or its assets or have a merger or a re-organization,

(p) public authorities or governments when required by law, public interest, national security, regulation, legal process, or enforceable governmental request,

(q) establish, exercise, or defend our legal rights including providing information to others and/or in connection with any ongoing or prospective legal proceedings.

10.2. In all the cases cited above, we require all parties we share your personal data (or personal data you provide) with to respect the security of your personal data (or personal data you provide) and treat it in accordance with the law. Please note that we do not allow our external service providers to use your personal data (or personal data you provide) for their own purposes and only permit them to process your personal data (or personal data you provide) for specified purposes and in accordance with our instructions.

10.3. Please note that if you request us, in writing, to share your personal data (or personal data you provide) with third parties, we will follow your request to share the relevant information. However, we do not have control over how those third parties will use your information. Before you make your request, we recommend that you (or the person acting on your behalf) consider the data protection practices of that third party by reading their privacy policies or contacting them.

11. CROSS BORDER TRANSFER OF PERSONAL DATA

11.1. We may transfer your personal data (or personal data you provide) to other hospitals, research, and diagnostic facilities, regulatory, prosecuting, tax and governmental authorities, courts and other tribunals, and other entities located in countries outside Kenya including countries which have different data protection standards to those which apply in Kenya.

11.2. When we transfer your personal data (or personal data you provide) outside Kenya to other entities, we will ensure that they protect your personal data (or personal data you provide) in accordance with the requirements under the Data Protection Legislation and that it is kept secure and receives at least a similar level of protection as that which it receives in Kenya.

12. DATA SECURITY

12.1. We have put in place appropriate physical and technical measures to safeguard your personal data (or personal data you provide) from being accidentally lost, used, or accessed in an unauthorised way.

12.2. Our IT systems are provided either in-house or by specific suppliers who are required to manage the data securely in a manner compliant with the Data Protection Legislation. We also have perimeter and internal protection of our IT systems and monitor access and security in a proactive manner. Only individuals with legitimate reasons are allowed access to areas storing personal data.

12.3. In addition, we will limit access to your personal data (or personal data you provide) to those employees, consultants, agents, and other third parties that require it for legitimate business purposes. They will only process your personal data (or personal data you provide) on our instructions and they are subject to a duty of confidentiality.

12.4. We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach if required by law.

13. COMMERCIAL USE OF YOUR PERSONAL DATA (OR PERSONAL DATA YOU PROVIDE)

13.1. Subject to obtaining your consent and in accordance with your communications preferences, we may use your personal data (or personal data you provide) to send you marketing information on our new facilities, services, and treatments which we think may be of interest to you.

13.2. You are free at any time to change your mind and withdraw consent for marketing activities. Please contact dpc@gerties.org.This will not affect the healthcare services we provide to you.

14. THE RETENTION AND STORAGE OF YOUR PERSONAL DATA (OR PERSONAL DATA YOU PROVIDE)

14.1. We will only retain your personal data (or personal data you provide) for as long as necessary to accomplish the purposes for which it was collected, including complying with any legal, accounting, or reporting requirements.

14.2. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data (or personal data you provide), the purposes for which we process your personal data (or personal data you provide) and whether those purposes can be achieved through alternative means, and the applicable legal requirements.

14.3. In some circumstances we may anonymise your personal data (or personal data you provide) so that it can no longer be linked to you, in which case we may use such anonymised information without notifying you further. Once our relationship is completed, your personal data (or personal data you provide to us) will be retained and securely destroyed in accordance with our personal data retention schedule.

15. YOUR LEGAL RIGHTS

15.1. Subject to certain exceptions and limitations under the law, you have a number of legal rights in relation to the personal data that we hold about you (or persons connected to you). These rights include the right to:

(i) **be informed** of the use to which your personal data (or personal data you provide) is to be used;

(ii) **request access** to your personal data (or personal data you provide) and receive a copy of the personal data we hold about you;

(iii) **request correction and erasure** of the personal data that we hold about you;

(iv) **request the restriction of processing** of your personal data (or personal data you provide). This enables you to ask us to suspend the processing of your personal data (or personal data you provide);

(v) **request us to transfer personal data** either to you or to another company in a commonly used electronic format. This is known as the right to data portability;

(vi) **object to the processing of your personal data (or personal data you provide)**;

(vii) **object and opt-out** of our direct marketing services; and

(viii) **request not to be subject to automated decision making**. This enables you to ask us not to make a decision about you that affects your legal position (or has some other significant effect on you) based purely on automated processing of your data.

15.2. To exercise any of these rights, please write to our DPC via the contact details given below.

15.3. We will respond to your request without undue delay and no later than the time periods stipulated by the applicable Data Protection Legislation.

16. CONTACT US AND FURTHER INFORMATION

16.1. If you have any questions about this Privacy Policy or how we handle your personal data (or personal data you provide), please contact dpc@gerties.org.

16.2. We will respond to your questions and concerns in a timely manner and in compliance with the relevant laws.

17. CHANGES TO THIS PRIVACY POLICY

17.1. We reserve the right to update this Privacy Policy at any time and we shall notify you of the changes through electronic mail or such other means of communication which may be available to us.

17.2. We may also notify you in other ways from time to time about the processing of your personal data (or personal data you provide).