

## **LUTON HOSPITAL PRIVACY POLICY**

Clear information about how we handle personal data

**LAST UPDATED**  
22 July 2026

**WEBSITE**  
[www.lutonhospital.co.ke](http://www.lutonhospital.co.ke)

**PRIVACY CONTACT**  
[info@lutonhospital.co.ke](mailto:info@lutonhospital.co.ke)



## Table of Contents

|                                                      |    |
|------------------------------------------------------|----|
| DEFINITIONS AND ABBREVIATIONS .....                  | 3  |
| PRIVACY AT A GLANCE.....                             | 4  |
| 1. WHO WE ARE AND THE SCOPE OF THIS POLICY .....     | 5  |
| 2. PERSONAL DATA AND SENSITIVE PERSONAL DATA .....   | 5  |
| 3. PERSONAL DATA WE COLLECT .....                    | 5  |
| 3.1 IDENTITY AND CONTACT INFORMATION .....           | 5  |
| 3.2 APPOINTMENT AND ENQUIRY INFORMATION .....        | 5  |
| 3.3 HEALTH AND MEDICAL INFORMATION .....             | 6  |
| 3.4 PAYMENT, INSURANCE AND COVER INFORMATION.....    | 6  |
| 3.5 COMMUNICATIONS AND DOCUMENTS.....                | 6  |
| 3.6 WEBSITE AND DEVICE INFORMATION .....             | 6  |
| 3.7 INFORMATION ABOUT ANOTHER PERSON .....           | 6  |
| 4. HOW WE COLLECT PERSONAL DATA.....                 | 6  |
| 5. WHY WE PROCESS PERSONAL DATA .....                | 7  |
| 6. LEGAL GROUNDS FOR PROCESSING.....                 | 7  |
| 7. IF YOU DO NOT PROVIDE REQUESTED INFORMATION ..... | 8  |
| 8. CHILDREN AND PERSONS WHO NEED ASSISTANCE .....    | 8  |
| 9. WHEN WE DISCLOSE PERSONAL DATA.....               | 8  |
| 10. INTERNATIONAL TRANSFERS .....                    | 9  |
| 11. COOKIES AND SIMILAR TECHNOLOGIES.....            | 9  |
| 12. DIRECT MARKETING.....                            | 9  |
| 13. AUTOMATED DECISION-MAKING.....                   | 10 |
| 14. DATA SECURITY AND CONFIDENTIALITY.....           | 10 |
| 15. PERSONAL-DATA BREACHES .....                     | 10 |
| 16. DATA RETENTION .....                             | 10 |
| 17. YOUR DATA-PROTECTION RIGHTS .....                | 11 |
| 18. HOW TO EXERCISE YOUR RIGHTS.....                 | 11 |
| 19. COMPLAINTS.....                                  | 12 |
| 20. THIRD-PARTY LINKS AND SERVICES .....             | 12 |
| 21. CHANGES TO THIS POLICY .....                     | 12 |
| 22. CONTACT US.....                                  | 12 |
| 23.GENERAL INFORMATION .....                         | 12 |
| REFERENCES.....                                      | 13 |



## Definitions and Abbreviations

| Term / Abbreviation                                           | Definition                                                                                                                                                                                                                                                                                                     |
|---------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Personal Data</b>                                          | Any information relating to an identified or identifiable natural person (data subject). Identifiable means the person can be identified, directly or indirectly, by reference to name, ID number, location data, online identifier, or other factors. (DPA 2019, s.2) [1]                                     |
| <b>Sensitive Personal Data / Special-Category Health Data</b> | Data revealing race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details, sex, or sexual orientation. Health data constitutes sensitive personal data under DPA 2019 s.46 [1] and the Digital Health Regulations 2025 [3]. |
| <b>Data Controller</b>                                        | The Hospital, acting as the natural or legal person who determines the purposes and means of processing personal data. (DPA 2019, s.2) [1]                                                                                                                                                                     |
| <b>Data Processor</b>                                         | Any natural or legal person, public authority, agency, or body that processes personal data on behalf of the Hospital under a written data processing agreement.                                                                                                                                               |
| <b>ODPC</b>                                                   | Office of the Data Protection Commissioner the independent regulatory authority established under DPA 2019 s.5 [1].                                                                                                                                                                                            |
| <b>Processing</b>                                             | collecting, recording, organising, storing, retrieving, using, sharing, transmitting, restricting, deleting or destroying personal data.                                                                                                                                                                       |
| <b>Breach / Personal Data Breach</b>                          | A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed. (DPA 2019, s.43) [1]                                                                                                |
| <b>SHA</b>                                                    | Social Health Authority insurers that may receive patient data under permitted disclosures.                                                                                                                                                                                                                    |



Luton Medical Hospital Limited respects your privacy and is committed to handling personal data lawfully, fairly, transparently and securely. This Privacy Policy explains how we collect, use, disclose, retain and protect personal data when you:

- visit or use **[www.lutonhospital.co.ke](http://www.lutonhospital.co.ke)**;
- submit an appointment request or another online form;
- contact us by telephone, email, WhatsApp or another available channel;
- receive or enquire about healthcare or related services from us; or
- otherwise interact with us in connection with our services.

Please read this Policy together with any more specific privacy notice provided when we collect personal data. A specific notice will supplement this Policy and will take priority for the processing activity it describes.

### Privacy at a glance

|                     |                                                                                                                                                                        |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Data controller     | <b>Luton Medical Hospital Limited</b>                                                                                                                                  |
| Data we may collect | Identity and contact details; appointment, health and medical information; payment or cover information; communications, documents and limited technical website data. |
| Main purposes       | Responding to enquiries, arranging and providing healthcare, administering payment or cover, communicating, safeguarding systems and meeting legal duties.             |
| Your rights         | Information, access, rectification, erasure, restriction, objection, portability, consent withdrawal and safeguards for qualifying automated decisions.                |
| Privacy contact     | <a href="mailto:info@lutonhospital.co.ke">info@lutonhospital.co.ke</a>                                                                                                 |
| Postal address      | P.O. Box 34444-00100, China Centre, Ngong Road, Nairobi, Kenya                                                                                                         |
| Telephone           | +254 111 003 400; +254 726 510 000; +254 711 300 900                                                                                                                   |



## 1. Who we are and the scope of this Policy

Luton Medical Hospital Limited is the data controller for personal data where it determines why and how that data is processed. In some arrangements, another organisation may be an independent or joint controller and should provide its own privacy information.

This Policy covers the hospital's principal website, online appointment requests and communications linked to our services. A separately operated portal, pharmacy platform, insurer, payment provider or third-party website may publish an additional privacy notice. The linked Luton Hospital Pharmacy site currently publishes a separate privacy policy.

This Policy does not replace the confidentiality duties owed by healthcare professionals or any specific consent, clinical, employment, research, CCTV, patient, pharmacy or other privacy notice that applies to a particular activity.

## 2. Personal data and sensitive personal data

"Personal data" is information relating to an identified or identifiable person. "Sensitive personal data" includes information that Kenyan law gives additional protection, including health data, genetic data, biometric data used for identification, a person's family details, sex or sexual orientation, and other legally protected categories.

Health information may reveal a person's physical or mental health, medical history, symptoms, diagnosis, treatment, medication, disability, laboratory or imaging results, health-cover details or the fact that a person is seeking healthcare. We apply additional care when processing health and other sensitive personal data.

## 3. Personal data we collect

The information we collect depends on how you interact with us and what service you request. It may include the following categories.

### 3.1 Identity and contact information

This may include your full name, date of birth, sex, national identification or passport information where lawfully required, postal or physical address, telephone number, email address, next-of-kin or emergency contact details, and information about a parent, guardian or authorised representative.

### 3.2 Appointment and enquiry information

The hospital's online appointment-request form currently asks for the service or department, appointment type, preferred date and time, full name, telephone number, email address, payment or cover type, SHA or insurance number, an attachment, and the reason for the visit. The form is used to request an appointment; submission does not itself confirm availability or create a confirmed appointment.



Please provide only information that is relevant to your request. Do not upload more medical, identity or financial information than the form asks for.

### 3.3 Health and medical information

Where necessary for healthcare or related services, we may process symptoms, medical history, diagnoses, prescriptions, treatment and care plans, clinical notes, test and imaging information, allergies, disability information, referral details, discharge information and other data relating to health or care.

### 3.4 Payment, insurance and cover information

Where applicable, we may process billing details, invoices, receipts, payment status, insurance or corporate-cover information, SHA details, authorisations and claim-related information. If a separate payment service is used, that provider may process payment credentials under its own privacy notice.

### 3.5 Communications and documents

We may process the content of enquiries, complaints, feedback and other communications, together with documents or attachments you choose to send. If you communicate through email, telephone, WhatsApp or another channel, the channel provider's own terms and privacy practices may also apply.

### 3.6 Website and device information

When you use our website, our systems or authorised service providers may process limited technical information needed to deliver, secure and maintain the service. Depending on the technology in use, this may include Internet Protocol address, browser and device type, operating system, referring page, pages visited, date and time, error logs and security events.

### 3.7 Information about another person

If you provide another person's personal data, you must have lawful authority to do so and should make this Policy available to that person where appropriate. This includes information about a child, dependant, next of kin or emergency contact.

## 4. How we collect personal data

We may collect personal data:

- **directly from you**, including through online forms, telephone calls, email, WhatsApp, in-person interactions and documents you provide;
- **from a parent, guardian or authorised representative** acting for you;
- **from healthcare professionals or organisations involved in your care**, where lawful and necessary;



- **from an insurer, SHA, employer or corporate-cover administrator**, where relevant to authorisation, billing or claims;
- **from public authorities or other persons**, where disclosure is required or permitted by law; and
- **automatically through the website**, where necessary technologies or lawfully enabled optional technologies are in use.

## 5. Why we process personal data

We process only the personal data reasonably required for a lawful and specified purpose. Depending on the circumstances, those purposes may include:

1. receiving, assessing and responding to enquiries and appointment requests;
2. identifying a patient or service user and maintaining accurate records;
3. arranging, coordinating and providing healthcare or related services;
4. communicating about appointments, care, service availability, follow-up or administration;
5. verifying SHA, insurance, corporate-cover or payment information and administering billing or claims;
6. responding to emergencies and protecting a person's vital interests;
7. managing complaints, incidents, quality assurance, clinical governance, audit and service improvement;
8. preventing and investigating fraud, misuse, unlawful activity, cyber threats and threats to safety;
9. operating, securing, maintaining and troubleshooting our website, communications and information systems;
10. establishing, exercising or defending legal claims;
11. complying with legal, regulatory, professional, public-health, reporting and recordkeeping duties; and
12. producing anonymised or aggregated information that no longer identifies an individual.

We do not disclose personal health data for market-research purposes. The Digital Health (Health Information Management Procedures) Regulations, 2025 prohibit a health data controller from disclosing personal health data for market research.

## 6. Legal grounds for processing

We will rely on one or more lawful grounds appropriate to the activity. These may include:

- **your consent**, where consent is required and has been freely given for a specific purpose;
- **steps requested before entering into a contract or performance of a contract** with you;
- **compliance with a legal obligation** imposed on the hospital;
- **protection of vital interests**, including urgent circumstances involving life or health;
- **performance of a task carried out in the public interest**, where applicable;



- **our legitimate interests or those of another person**, where those interests are not overridden by your rights and freedoms; and
- **additional grounds permitted for health or other sensitive personal data**, including grounds connected with healthcare, public health, legal claims or another basis authorised by law.

The applicable ground depends on the specific data and purpose. Consent is not always the legal basis for healthcare processing, and withdrawing consent does not affect processing already lawfully completed or processing required on another lawful ground. These grounds are governed principally by the Data Protection Act, 2019.

### 7. If you do not provide requested information

You are not required to provide personal data merely to browse public pages of our website. However, if information is necessary to identify you, assess an appointment request, provide safe care, verify cover, process payment or meet a legal duty, we may be unable to complete the requested service without it. We will seek to explain when information is required and, where practical, what may happen if it is not provided.

### 8. Children and persons who need assistance

Healthcare services may involve children or persons who cannot independently exercise all data-protection choices. Where required, we will seek information or authorisation from a parent, guardian or other person lawfully authorised to act. We may process information without such authorisation where the law permits or requires it, including to protect vital interests or provide urgent care.

A parent, guardian or representative should provide only information necessary for the person's care or request and should tell us in what capacity they are acting. We may take reasonable steps to verify authority before disclosing records or acting on a rights request.

### 9. When we disclose personal data

We may disclose the minimum personal data reasonably necessary to recipients who have a lawful need to receive it. Depending on the service and only where applicable, recipient categories may include:

- healthcare professionals and authorised staff involved in care or administration;
- laboratories, imaging centres, referral facilities or other healthcare providers involved in a service requested for you;
- SHA, insurers, employers or corporate-cover administrators for verification, authorisation, billing or claims;
- professional advisers, auditors and insurers acting under appropriate duties;
- authorised providers supporting hosting, communications, cybersecurity, records, maintenance or other hospital systems;





- payment, pharmacy or delivery providers where you use the relevant service;
- regulators, courts, law-enforcement agencies, public-health bodies and other public authorities where disclosure is legally required or permitted; and
- another person where you have authorised the disclosure or requested that we send information to that person.

We expect processors acting on our instructions to handle personal data only for authorised purposes, apply appropriate safeguards and comply with applicable data-protection obligations. Health data controllers are required to maintain records of engaged health-data processors and apply role-based access in relevant systems.

We do not sell personal data. We do not disclose personal health data for market research.

## 10. International transfers

Some authorised service providers may process or support personal data from outside Kenya. Where a transfer outside Kenya occurs, we will apply the requirements and safeguards required by Kenyan law. These may include confirming that appropriate protection exists, using contractual or other legally recognised safeguards, or obtaining consent where that is the proper legal basis.

We do not state that all website or service data is stored only in Kenya unless that has been confirmed for the relevant system.

## 11. Cookies and similar technologies

Our website may use strictly necessary cookies or similar technologies needed for functions such as security, network management, accessibility and reliable page delivery.

Optional analytics, advertising or similar technologies will be enabled only where they have been assessed and can be used lawfully. Where optional technologies are used, the website's cookie notice or consent interface should identify their categories, purposes, providers and durations and provide the controls required by law.

You can use browser settings to block or delete cookies, although blocking strictly necessary technologies may affect website operation. We do not name a specific analytics, advertising or tracking provider in this Policy because the hospital's current technology-vendor inventory has not been confirmed.

## 12. Direct marketing

We may send direct marketing only where there is a lawful basis to do so and any required consent has been obtained. You may opt out at any time by using an unsubscribe method in the message or contacting us.

We will not make access to necessary healthcare conditional on agreeing to unrelated marketing. We do not use personal health data for market research.



### 13. Automated decision-making

If we use solely automated processing to make a decision that produces legal or similarly significant effects, we will provide the information and safeguards required by law. These may include a way to request human intervention, express your view and contest the decision. Routine routing, form validation or appointment administration does not necessarily amount to a legally significant automated decision.

### 14. Data security and confidentiality

We are responsible for applying technical, organisational and physical safeguards appropriate to the nature of the data, the processing and the risks involved. Safeguards may include measures relating to authorised access, confidentiality, staff responsibilities, secure handling, system maintenance, incident management and oversight of service providers.

Access to personal data should be limited to persons who need it for an authorised purpose and who are subject to confidentiality or professional duties. No method of storage or transmission is completely secure, and users should avoid sending unnecessary sensitive information through ordinary email or messaging services.

### 15. Personal-data breaches

We maintain procedures for assessing and responding to suspected personal-data breaches. Where the legal threshold is met, the hospital will notify the Office of the Data Protection Commissioner within 72 hours after becoming aware of the breach and will notify affected persons where the law requires it.

Where a health-data incident is also reportable under digital-health law, we will notify the Digital Health Agency or another competent authority as required.

### 16. Data retention

We keep personal data only for as long as it is reasonably needed for the purpose for which it was collected and for any applicable legal, clinical, professional, accounting, reporting, insurance, claims or dispute-resolution requirement.

Retention periods may differ for appointment requests, communications, clinical records, prescriptions, billing and cover information, complaints, security logs and website data. When deciding how long to keep information, we consider:

- the nature, sensitivity and volume of the data;
- the purpose of processing and whether it can be achieved in another way;
- patient-safety and continuity-of-care needs;
- legal and professional recordkeeping duties;
- limitation periods and the possibility of claims or complaints; and
- security and privacy risks.



When retention is no longer justified, data will be securely deleted, destroyed or anonymised, subject to technical limits and lawful exceptions.

## 17. Your data-protection rights

Subject to applicable conditions, exemptions and verification requirements, you may have the right to:

- 13. **be informed** about how your personal data is used;
- 14. **request access** to personal data held about you and receive a copy;
- 15. **request correction** of inaccurate or incomplete personal data;
- 16. **request erasure** where there is a lawful basis for deletion;
- 17. **request restriction** of processing in qualifying circumstances;
- 18. **object** to processing based on particular grounds, including direct marketing;
- 19. **request data portability** where the legal requirements are met;
- 20. **withdraw consent** for future processing that depends on consent; and
- 21. **seek safeguards concerning qualifying automated decisions** .

Under the Data Protection (General) Regulations, 2021, an access request is generally to be fulfilled within seven days and free of charge. Rectification, erasure and restriction requests are generally to be addressed within 14 days, subject to the applicable legal conditions and exceptions. A refusal to rectify is to be communicated in writing within seven days with reasons.

These rights are not absolute. For example, we may need to retain information to provide safe care, comply with law, protect another person's rights, or establish or defend a legal claim.

## 18. How to exercise your rights

Send a clear request to [info@lutonhospital.co.ke](mailto:info@lutonhospital.co.ke) or write to:

### Privacy and Data Protection Contact

**Luton Medical Hospital Limited**

**P.O. Box 34444–00100**

**China Centre, Ngong Road**

**Nairobi, Kenya**

You may also telephone **+254 111 003 400**, **+254 726 510 000** or **+254 711 300 900** for guidance on submitting a request.

Please describe the right you wish to exercise and the data or interaction concerned. We may request information reasonably necessary to verify identity, authority and the scope of the request. We will not request more verification data than necessary.

We will respond within the period required by law. If we cannot comply in full, we will explain the reason where permitted and tell you about any available complaint or review route.



## 19. Complaints

Please contact us first if you have a privacy concern so that we can investigate and respond.

You also have the right to lodge a complaint with the **Office of the Data Protection Commissioner of Kenya (ODPC)**. The Data Protection Act, 2019 establishes the Commissioner's complaint and enforcement role. Current official information and complaint channels are available at <https://www.odpc.go.ke/>.

## 20. Third-party links and services

Our website may link to websites, portals, maps, social-media pages, messaging services, payment services or other services controlled by third parties. Their privacy practices are governed by their own notices. We encourage you to read those notices before providing personal data.

A link does not mean that we control the third party's data practices. However, where a third party processes personal data on our instructions, we remain responsible for meeting the obligations that apply to us as controller.

## 21. Changes to this Policy

We may update this Policy to reflect changes in law, technology or our services. The latest version will be posted on our website with its effective or "last updated" date. If a change materially affects how we use personal data, we will take reasonable steps to provide additional notice where required.

## 22. Contact us

For questions, requests or complaints about this Policy or our handling of personal data, contact:

### Privacy and Data Protection Contact

**Luton Medical Hospital Limited**

**P.O. Box 34444-00100, China Centre, Ngong Road, Nairobi, Kenya**

**Email:** [info@lutonhospital.co.ke](mailto:info@lutonhospital.co.ke)

**Telephone:** +254 111 003 400; +254 726 510 000; +254 711 300 900

**Website:** <https://www.lutonhospital.co.ke>

## 23. General Information

This Privacy Policy is intended to provide general information regarding the Hospital's processing of personal data. It does not replace any specific privacy notice, patient consent form, employment notice or legal obligation applicable to a particular service.



## References

- [1] Luton Hospital — Appointment Booking. <https://lutonhospital.co.ke/booking>
- [2] Luton Hospital Pharmacy — Privacy Policy.  
<https://pharmacy.lutonhospital.co.ke/index.php/privacy-policy>
- [3] Office of the Data Protection Commissioner — Data Protection (General) Regulations, 2021.  
<https://www.odpc.go.ke/wp-content/uploads/2024/03/THE-DATA-PROTECTION-GENERAL-REGULATIONS-2021-1.pdf>
- [4] Kenya Data Protection Act, 2019. <https://www.kentrade.go.ke/wp-content/uploads/2022/09/Data-Protection-Act-1.pdf>
- [5] Kenya Law — Digital Health (Health Information Management Procedures) Regulations, 2025. <https://new.kenyalaw.org/akn/ke/act/ln/2025/76/eng@2025-04-11>

