DATA PROTECTION NOTICE

Contents

Introduction

This data protection notice (‘**Notice’**) sets out what personal data we collect from you and/or generate about you including how we collect or generate, use, store and process them when you visit our hospital and/or any of our laboratories and obtain services, and when we visit you at your home and/or any place nominated by you to provide services. Your privacy is important to us and we are committed to safeguarding the privacy of your personal data. It is important that you read this notice carefully and understand how and why we process your personal data.

In this notice, we, Hemas Hospitals (Private) Limited and Hemas Capital Hospital (Private) Limited, will be referred to as “**Hemas**”, “**us**” or “**we**”, or the “**Company**” which is part of the Hemas Group of Companies. According to the Personal Data Protection Act No.9 of 2022 (‘PDPA’) we may sometimes act in the capacities of a “**controller**”, “**joint-controller**” or a “**processor**” which may be determined according to the particular context of processing your personal data. A patient or visitor will be referred to as “you” and be treated as a “data subject” under the PDPA.

What Information is Collected

We may collect the following information when you are admitted to our hospital, visit our premises, receive treatment or other services from us, participate in our research, awareness activities or donor programs or when we provide medical services through homecare visits:

- Your name, date of birth, phone number, email address, postal address, national ID number, passport number (if NIC is not available)
- Your medical history, health related information, medical diagnosis, bodily fluids, medical test results, medications and treatment plans, genetic data, biometric data, photographs.
- Contact Information: Email address, phone number, home address, etc., for communication purposes.
- Health Data: Vital statistics (blood pressure, heart rate), fitness activity (steps, calories burned), and any health metrics entered by users or collected via 3rd party sources.
- Symptoms & Conditions: Data about current symptoms, illnesses, or health conditions, including those tracked over time
- In the event of a device log in, the App Usage Data: How often the app is used, duration of use, features accessed, etc., to improve user experience.
- Geolocation Data: The app may collect information about the user's precise or approximate geographic location, either in the foreground or background, depending on the user's settings. These are used for finding nearby hemas hospitals and track the requested healthcare provider details.
- Occupation and educational background
- Your allergies, meal preferences and special needs
- Your ethnicity, religion, sexual orientation, marital status and gender identity
- Your next of kin, information relating to your children, spouse and family background.
- Your financial information, such as insurance details or payment methods such as credit card data.
- Your feedback and complaints including any video or audio testimonials.
- CCTV footage

Why we collect and use your information.

We may collect the above information for the following purposes:

- To provide you with safe, effective and efficient health care services
- To evaluate your eligibility to participate in any donor program as a doner.
- To carry out required medical diagnosis and provide treatment.
- To inform you about our services, reports and future appointments.
- To communicate information relating to your treatment, any medical test/assessment you have undertaken or any other service you have sought from us.
- To communicate with health care professionals involved in your care
- To monitor and improve the quality and delivery of our services
- To train and educate our staff and medical and nursing students
- To conduct research and innovation that benefits patients and society at large.
- To comply with our legal and regulatory obligations

- To respond to law enforcement requests, assist criminal investigations and prosecutions to the extent permitted by law.
- To safeguard public health
- To secure our premises, property and personnel
- To respond to or defend any legal claim before a court of law or tribunal

Legal basis for processing your personal data.

We comply with the 'PDPA when we process your personal data. Depending on the respective purpose, we may rely on one or more of the following lawful basis:

- Your consent, when we have specifically sought your consent to process your personal data for specific purpose(s). In the case of children under the age of 18, consent may relate to parents or legal guardians.
- Contract performance, when we have an agreement with you to provide our services. This includes processing for any pre-contractual purposes as well.
- Legal obligation, when we are required by law or a court order to process your personal data.
- Public interest, when we are required to perform certain processing activities in the public interest as defined by law.
- Our legitimate interests, when have a lawful and reasonable reasons to process your personal data, provided such interests do not override your rights and interests.
- When we have to respond to an emergency that threatens your life, health or safety or that of another person.

When we process special categories of personal data (i.e. information relating to your health, sexual orientation, ethnicity, race, gender, etc. as defined in the PDPA) we may pursue the following legal basis:

- Your consent, when we have specifically sought your consent to process your personal data for specific purpose(s). In the case of children under the age of 18, consent may relate to parents or legal guardians.
- For preventive or occupational medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where such data is processed by a health professional licensed or authorised by law in Sri Lanka.
- Public health purposes ensuring public safety, monitoring and public alert systems relating to impending health or other emergencies, the prevention or control of communicable diseases and other serious threats to public health and the management of public healthcare services in so far as it is provided for in any law.
- When we have to respond to an emergency that threatens your life, health or safety or that of another person where you are physically or legally incapable of giving consent.
- Processing personal data which is manifestly made public by you.
- For the establishment, exercise or defence of legal claims before a court or tribunal or such similar forum, and to be shared with insurance companies for claims
- When necessary for to achieve a public interest purpose as laid down by law.
- For archiving purposes in the public interest, scientific research or historical research purposes or statistical purposes in accordance with law in a manner that is proportionate to the aim pursued, and in accordance with applicable data protection laws.

Sources of Collection

We collect your personal data primarily from you when you make a channelling appointment or admit to the hospital or visit our hospital and/or laboratories for any purpose or when we visit you at your home and/or any place nominated by you to provide services. We may also collect information from your doctors, other hospitals and health care providers, relatives, caregivers, insurance service providers, ambulance operators and public authorities. We may further collect your personal data from our interactions and communications with you including any feedback you may voluntarily provide.

We may also collect personal data from various medical and non-medical devices, including monitoring mechanisms. We may also source personal data from CCTV devices we've implemented at our premises.

Retention Period

We keep your personal data for as long as it is necessary to achieve the purposes for which it was collected. We abide by any specific health information retention periods specified by the Ministry of Health and may retain for longer periods if required to do so by applicable legal obligations, for the purpose of ongoing investigations, to defend legal claims, for the purpose of certain legitimate interests of ours, for archiving purposes in the public interest, scientific research, historical research or statistical purposes subject to such appropriate technical and organisational measures required by law. We will either anonymise or securely dispose your personal data once it is no longer needed.

Sharing with Third Parties

We may need to share your personal data including special categories of personal data with third parties, which are generally identified below, to complete the purposes stated above:

- Insurance Agencies/Companies: we may be required to provide your personal data as requested by insurance agencies/companies who may process your medical claims.
- Other healthcare service providers: this may include laboratory services, other hospitals in the case of patient transfers, ambulance services, pharmacists, physiotherapists, opticians and dentistry.
- Our Suppliers/Service Providers: we may need to engage with a host of suppliers or service providers to carry out various operational work to support the services we provide to you. These suppliers/service providers will be subject to a contractual and legal framework that will stipulate various conditions including but not limited to ensuring the confidentiality and privacy of your personal data. The access they may have shall be limited to a need-to-know basis and in so far as strictly necessary for them to provide their services to us. Accordingly, these suppliers/service providers will provide services in relation to IT infrastructure and support, facility management and security, training and awareness, enterprise resource planning, communication services, finance and accounting, audit, and legal.
- To government or law enforcement authorities: we may share your personal data if we are of the opinion that the applicable laws require use to disclose your personal data with the government including tax and other regulatory bodies, the police or law enforcement authorities.
- Other entities who are involved in your care such as caregivers, next of kin and/or legal representative.
- Recipients in donor programs: subject to anonymity conditions agreed with you (if any) your donor profile may be disclosed to (prospective) donee or your donee profile maybe disclose to the donor as the case maybe in any donor program which you may participate.
- Members of the Hemas Group of Companies: information may be shared with entities within the Hemas Group who provide IT and information security services to us. Information may also be shared with the Hemas Holdings PLC for budgeting, workforce planning, human resources, legal and other centralised functions.

- Prospective buyers or sellers including their advisers: we may be required to share your information in the context of an acquisition, merger, joint venture or any other form of change in control or strategic alliance.

Please note that sharing of any personal data will be strictly limited to what is relevant, necessary and proportionate to the purpose to which sharing is required. We shall not sell or license your information to any third party.

Use of Automated Decisions Making Systems

We may adopt automated decision-making systems in our operational environment. Automated decision-making means making decisions or profiling you purely through automated means without any human intervention. These systems are generally used to support human decision-making processes by analysing your data subject to certain criteria set by us. We may use these systems for evaluation or profiling for internal requirements.

Your Rights

Under the applicable data protection laws, you'd be entitled to the following rights subject to any exceptions permitted under the PDPA:

Access: you may access your personal data or get a confirmation whether we process any of your personal data. You may also request further information pertaining to how, where and why we process your personal data.

Withdraw consent: if we have sought your consent for any of the purposes listed above, then you may be in a position to withdraw your consent for those particular purpose(s). When you withdraw your consent, we will not be able to process your information thereafter and may affect the delivery, availability and extent of our services to you.

However, your withdrawal will not invalidate any processing which we've done prior to such withdrawal.

Object to processing: if we are processing your personal data pursuant to a legitimate interest of ours or due to public interest, then you may request us to refrain from processing your personal data for said purposes. However, your objection will not invalidate any processing which we've done prior to such objection.

Rectification & update: We rely on your input and assistance to ensure the accuracy of the personal data which you have provided to us, and you have an obligation to provide us with correct and updated personal data particularly when that information is sought directly from you. Meanwhile you have the right to request rectification of any inaccurate data or completion of incomplete personal data which we process.

Erasure: if you think that we are processing your personal data in contravention to the PDPA, or you have withdrawn your consent regarding any processing that was founded upon your consent, then you may request us to erase your personal data. Any request for deletion will be evaluated against our legal obligations to retain the said data.

Review of automated decisions: if any decision that affects your rights are taken by us based on purely automated means without human intervention, in certain circumstances you may have the right to request us to review the said decision.

Right to complaint: if you are not happy with how we process your personal data, or not satisfied with our response to your request under the above mentioned rights, you may make a complaint to the Data Protection Authority, First Floor; Block 5, Bandaranaike Memorial International Conference Hall (BMICH), Bauddhaloka Mawatha, Colombo 07, Sri Lanka. info@dpa.gov.lk

Data Security

We are committed to securing your personal data and safeguarding the confidentiality, integrity and availability of your personal data by using appropriate organisational and technical measures. For this purpose, we have adopted industry-best practices and appropriate information security standards and

protocols to guard against unauthorized or unlawful processing, loss, destruction or damage of your personal data.

Some of these measures include, using secure information systems and networks when we transmit and store your personal data, implementing access restrictions and allow access on need-to-know basis to our staff, regular training and guidance to our staff on privacy and data protection, use of anonymisation and encryption as appropriate, implementing internal procedures to duly detect and respond to data breaches.

International Transfers

Your personal data may be transferred and processed outside of Sri Lanka in one or more countries in certain circumstances. Such circumstances may typically arise when your personal data may be stored/hosted on cloud platforms, in the context of a patient transfer to a foreign hospital or attending to insurance claims of an insurance provider located outside Sri Lanka. Whist we strive to process data in countries where the Sri Lankan Data Protection Authority has given adequacy decisions, for operational reasons, this may not always be possible. Therefore, we have adopted appropriate safeguards to ensure the security and privacy of your information through comprehensive contractual and other means in accordance with the PDPA.

Contact

If you need any clarifications regarding this data protection notice, you may contact your respective data protection officer at dpo@hemashospitals.com or call the general line on 0094117888888

To exercise any of your rights under this data protection notice, please complete the following form and sent it to dpo@hemashospitals.com or call the general line on 0094117888888

Name	
Patient ID / NIC	
Email	
Mobile No.	
Request Type: **[Access | Withdrawal of Consent | Object to Processing | Rectification | Update | f | Review of Automated Decision | Further Information]**	
Additional Information on the Request	

Changes to Data Protection Notice

We may update this data protection notice from time to time to reflect the changes in our services, data protection practices or legal obligations. Any significant changes will be notified by posting the updated notice on our website, or by contacting you directly through registered channels.

Last update: 01/01/2025