LONDON HEART CLINIC

DATA PROTECTION POLICY AND PROCESS

Policy No	C023
Responsible Person	Anika Jivraj
Date Issued	Jun 2024
Next Review Date	Every two years
Authorised by	
Version No	02

Title	**Data Protection Policy**
Author	
Responsible Person	Anika Jivraj
Authorised	Anika Jivraj
Issue Date	June 2024
Review Date	Every two years unless review required earlier
Policy No and Version	C023 Version 02
References	1. **UK General Data Protection Regulation (UK GDPR)** 2. **Data Protection Act 2018**, 3. **Freedom of Information Act 2000**, 4. **The Privacy and Electronic Communications Regulations (PECR) 2003**, 5. **Human Rights Act 1998**, 6. **Health and Social Care Act 2008**, 7. **NHS Data Security and Protection Toolkit** (for relevant healthcare data) 8. **Information Commissioner's Office (ICO) Guidance**
Appendix	
Scope	All individuals in the employ of this establishment *('employ' means any person who is employed, self-employed, volunteer, working under practising privileges or contract of service with this establishment)*

Policy Statement

London Heart Clinic (LHC) is committed to protecting the privacy and confidentiality of personal data in compliance with the **UK General Data Protection Regulation (UK GDPR)**, **Data Protection Act 2018**, and other relevant legislation. This policy outlines how LHC collects, processes, stores, and secures personal data to ensure that it is handled lawfully, fairly, and transparently.

Key Principles

1. Lawfulness, Fairness, and Transparency

LHC ensures that personal data is:

- **Collected and processed lawfully, fairly, and in a transparent manner** in relation to individuals.
- **Processed based on legitimate grounds**, including patient care, staff management, and legal or regulatory obligations.
- Patients and staff will be informed about how their data will be used, ensuring clarity and transparency in all data-related processes.

---

2. Data Minimisation

LHC collects only the **minimum amount of personal data** necessary to fulfil its purposes. Personal data is only collected where it is relevant and necessary for:

- **Patient care** (e.g., medical history, diagnostic information).
- **Staff management** (e.g., employment details, payroll information).
- **Business operations** (e.g., supplier and contractor details).

LHC avoids excessive or irrelevant data collection and reviews its data processing activities regularly to ensure compliance with this principle.

---

3. Accuracy

LHC takes reasonable steps to ensure that personal data is:

- **Accurate**, complete, and kept up to date where necessary.
- Staff and patients are encouraged to inform the clinic of any changes to their personal data to ensure accuracy.
- Data inaccuracies are corrected or deleted without undue delay when identified.

---

4. Purpose Limitation

LHC ensures that personal data is:

- Collected for **specified, explicit, and legitimate purposes**.
- **Not processed in ways incompatible** with those purposes, except where required by law or with explicit consent.
- For example, data collected for patient care will only be used for that purpose unless additional consent is provided or a legal obligation arises.

---

5. Data Retention

Personal data is:

- **Retained only for as long as necessary** to fulfil the purposes for which it was collected, in accordance with legal, regulatory, or clinical obligations.
- Regular reviews of data retention periods are conducted to ensure that no unnecessary data is retained.
- **Patient records** will be retained for the period specified by the relevant healthcare legislation and guidance.
- When personal data is no longer required, it is securely deleted or anonymised.

---

6. Security and Confidentiality

LHC employs appropriate technical and organisational measures to ensure the **security and confidentiality** of personal data, including:

- **Encryption**: Sensitive data, such as patient health records, is encrypted both in transit and at rest.
- **Access controls**: Access to personal data is restricted to authorised personnel only, based on job responsibilities.
- **Regular audits and monitoring**: Systems are regularly reviewed for vulnerabilities, and security measures are updated in line with evolving threats.
- Staff are trained to handle personal data responsibly and report any breaches or security risks promptly.

---

7. Individual Rights

LHC upholds the rights of individuals under the **UK GDPR**, including:

- **Right to access**: Individuals can request access to their personal data held by LHC.
- **Right to rectification**: Individuals can request the correction of inaccurate or incomplete data.
- **Right to erasure**: Individuals may request the deletion of personal data when it is no longer necessary for the purposes for which it was collected, provided no legal obligation exists for its retention.
- **Right to restrict processing**: Individuals may request restrictions on how their data is processed in certain circumstances.
- **Right to data portability**: Individuals can request a copy of their data in a structured, commonly used format.
- **Right to object**: Individuals can object to the processing of their data in certain circumstances, such as for direct marketing purposes.
- All requests are handled promptly and within the statutory timeframe of **one month**, in accordance with the **UK GDPR**.

---

8. Data Breach Reporting

LHC has robust procedures in place for identifying, reporting, and managing personal data breaches. If a breach occurs:

- **Internal Reporting**: Staff are required to report data breaches immediately to the Data Protection Officer (DPO).
- **Investigation**: The DPO will assess the breach to determine the risk to individuals and ensure appropriate mitigation.
- **Notification to Authorities**: In the event of a breach that poses a risk to individuals' rights and freedoms, LHC will

notify the **Information Commissioner's Office (ICO)** within **72 hours** of becoming aware of the breach.
- **Notification to Individuals**: If the breach is likely to result in a high risk to the rights and freedoms of individuals, LHC will also inform the affected individuals without undue delay.
- All breaches, regardless of their severity, are documented in LHC's **Breach Register**, which is reviewed regularly to improve data protection measures.

---

9. Third-Party Data Sharing

LHC only shares personal data with third parties when:
- **Necessary for patient care** (e.g., sharing medical data with other healthcare providers).
- **Required by law** (e.g., for regulatory reporting).
- **Contracted services** (e.g., payroll processing for employees or IT services).
- All third-party providers must comply with LHC's data protection policies and sign appropriate **data-sharing agreements** to ensure compliance with the **UK GDPR** and **Data Protection Act 2018**.

---

10. Data Protection Officer (DPO)

LHC has appointed a **Data Protection Officer (DPO)** to oversee data protection compliance. The DPO is responsible for:
- **Monitoring adherence** to data protection laws and this policy.
- **Providing training** and guidance to staff on data protection matters.
- **Responding to data subjects' requests** and ensuring that individual rights are upheld.
- **Liaising with the ICO** and other regulatory bodies when necessary.
- The DPO also leads regular reviews and audits to ensure continuous compliance with current data protection legislation.

Staff Responsibilities

All LHC staff are responsible for:
- **Handling personal data in compliance** with this policy and relevant data protection laws.
- **Reporting any data breaches** immediately to the DPO.
- **Ensuring data accuracy** and safeguarding confidential information.
- Failure to comply with this policy may result in disciplinary action, including dismissal.

Training and Awareness

All LHC staff will receive **mandatory data protection training** as part of their induction and **regular refresher courses**. This ensures that all employees are aware of their responsibilities under the **UK GDPR** and can effectively protect personal data.

Monitoring and Review

This policy will be reviewed **every two years** or sooner if there are significant legislative or organisational changes. Updates will be made to ensure continued compliance with the **UK GDPR**, **Data Protection Act 2018**, and any relevant regulations.

By adhering to this policy, LHC ensures the secure and lawful processing of personal data, safeguarding both patients' and staff's rights to privacy and confidentiality