Data Privacy Policy - Dr. Simon Chapman

Introduction

I am committed to protecting your privacy and handling your personal data responsibly, in compliance with the Data Protection (Jersey) Law 2018 (DPJL) and the General Data Protection Regulation (GDPR). This policy explains how I collect, use, store, and protect your personal data and outlines your rights under these laws.

Data Controller

As a Data Controller, I am accountable for the personal data you provide when engaging with my private medical practice. This includes information related to your health, consultations, referrals, and follow-up care.

Health Data Retention Policy for Private Patients

I utilise MAXIMs, the Health and Community Services (HCS) Electronic Patient Record (EPR) system, ensuring that all medical records are protected by the same Data Governance protocols as HCS data and patient records. HCS records are governed by the Public Records (Jersey) Law 2002, which requires a statutory duty of care for records management. This data retention policy is aligned with the NHS retention schedule, adopted by HCS Information Governance.

Data Protection Training

Both my secretary and I have completed HCS accredited Data Protection training.

Purpose

This policy establishes standards for managing, retaining, and securely disposing of patient records in compliance with the Records Management Code of Practice 2021, as well as NHS and HCS guidelines.

Scope

This policy applies to all patient health and care records managed within my practice through HCS systems, covering both physical and digital records to ensure statutory retention compliance.

Retention Periods by Record Type

Abiding by the Records Management Code of Practice 2021, the following retention periods are observed:

- **Adult Health Records**: Retained for a minimum of 8 years after the last recorded entry.
- **Children's Health Records**: Retained until the patient's 25th birthday (or 26 if they were 17 at the end of treatment).

Data Security and Confidentiality

All records managed through HCS systems comply with NHS and HCS information governance protocols. Access to patient data is restricted to authorised personnel to ensure confidentiality and integrity of records.

Data Disposal and Destruction

Once retention periods lapse, records are securely destroyed following the Records Management Code of Practice 2021:

- **Electronic Records**: Permanently deleted or securely overwritten in HCS systems.
- **Physical Records**: Securely shredded or destroyed per HCS standards to prevent unauthorised access.

Policy Review

This retention policy will be reviewed periodically in line with HCS Information Governance processes to maintain alignment with regulatory standards.

How Your Data is Collected, Processed, and Stored

I collect your personal data through:

- **Appointments**: Either in person or via other means.
- **Referral Information**: Information provided by referral letters or through interactions with healthcare professionals involved in your care.

Data is securely stored on the MAXIMs Electronic Patient Record (EPR) system, approved for health data management by Jersey General Hospital. Paper records, where necessary, are securely transcribed into the EPR and disposed of via confidential waste processing.

Lawful Basis for Processing

To comply with the DPJL and GDPR, I process your data lawfully, fairly, and transparently, based on the following lawful grounds:

1. **Consent**: Your explicit consent is obtained for referrals to other healthcare professionals. Consent can be withdrawn at any time.
2. **Contractual Obligations**: For health insurance purposes, I may provide consultation data to insurers to facilitate billing and claims.
3. **Vital Interests**: In emergencies, I may process data to protect your life or that of others.
4. **Legal Obligations**: I may be legally required to share data with authorities, such as the police or courts.
5. **Legitimate Interests**: I may process data for legitimate professional activities, such as medical appraisals, ensuring no impact on your rights or freedoms.

Data Sharing

Your data may be shared as follows:

- **Healthcare Professionals**: Other doctors, specialists, or allied health professionals (e.g., physiotherapists or radiologists) involved in your care.
- **Health Insurance Providers**: For billing and claims purposes, with your consent, through Healthcode. Healthcode complies with ISO/IEC 27001 data security standards, meeting DPJL requirements for confidentiality, integrity, and security.

- **Emergency Services**: If a serious risk of harm exists, data may be shared to protect you or others.
- **Legal Authorities**: If required by law (e.g., by the police, courts, or professional bodies).

Any shared data is limited to the minimum necessary information and transmitted securely to protect your privacy.

Data Retention

I retain personal data only as long as necessary for the purpose collected. In accordance with HCS guidelines, data is retained for 8 years following the conclusion of treatment, after which it is securely deleted.

Your Rights Under DPJL and GDPR

You have the following rights regarding your data:

1. **Access**: Request a copy of personal data held about you.
2. **Rectification**: Request corrections to any inaccurate data.
3. **Erasure**: Request data deletion when it is no longer necessary or if consent is withdrawn.
4. **Restriction of Processing**: Request a halt to data processing in specific circumstances.
5. **Objection**: Object to processing, particularly under legitimate interests. In some cases, legal obligations may require continued processing.
6. **Data Portability**: Request data transfer to another healthcare provider, where applicable.

Contact Information

For any questions or to exercise your data rights, please contact:
Dr. Simon Chapman
Email: info@jerseymedic.com
Phone: 01534 442800
Address: Consultant Offices, Emergency Department, Jersey General Hospital, St. Helier, JE1 3QS

Data Protection Impact Assessments (DPIAs)

If significant changes to data processing are introduced, I will conduct a DPIA to ensure your privacy rights are fully protected.

Auditing Data Access

Access to personal data is limited to authorised individuals with legitimate need and is auditable by the HCS Information Governance Department to ensure only necessary access.

Complaints

If you believe your data has been mishandled or if you have concerns regarding data processing, please contact me directly.
Alternatively, you may also contact the Jersey Office of the Information Commissioner:

- **Phone**: +44 1534 716530
- **Website**: Jersey Office of the Information Commissioner

Policy Updates

This Privacy Policy may be updated periodically. For the latest version, please check my website or contact me directly.