PRECISION SURGERY
CLINIC

Precision Surgery Clinic Information Governance Policy

1. Introduction

Precision Surgery Clinic is committed to safeguarding the confidentiality, integrity, and availability of all identifiable data we hold about patients, staff, and other stakeholders. This policy outlines the principles and procedures governing how we manage personal information in accordance with the Data Protection Act 2018 and other relevant legislation.

2. Arrangements for Ensuring Data Security

2.1 Access Controls:

- Access to personal data is restricted to authorized personnel on a "need-to-know" basis.
- User accounts with unique passwords and multi-factor authentication are mandatory for accessing data systems.
- Access logs are monitored for suspicious activity.

2.2 Data Security Standards:

- We implement appropriate technical and organizational measures to protect data from unauthorized access, disclosure, alteration, or destruction.
- This includes firewalls, encryption, regular backups, and vulnerability assessments.
- We comply with relevant data security standards like GDPR and ICO.

2.3 Internal Validation:

- Regular audits and reviews are conducted to assess the effectiveness of our data security controls.
- Data management practices are evaluated for compliance with this policy and relevant legislation.
- Internal testing and mock breaches are conducted to identify and address vulnerabilities.

2.4 External Validation:

- We engage third-party security experts to conduct independent penetration testing and security assessments periodically.
- We may consider independent data protection accreditations to demonstrate our commitment to data security.

3. Learning from Data Security Breaches

- We have a defined incident response plan to mitigate the impact of data security breaches.
- This plan includes steps for containing the breach, notifying relevant authorities, and communicating with affected individuals.
- We conduct post-breach reviews to identify root causes and implement corrective actions to prevent future occurrences.

4. Compliance with Data Sharing Requirements

- We share data with other healthcare providers and institutions as necessary for patient care, but only with the patient's explicit consent or on legal grounds.
- We comply with data-sharing agreements that specify the purposes and limitations of data sharing.
- We notify relevant authorities of data breaches that may pose a risk to individuals' rights and freedoms.

5. Data Use and Analysis

- We only use personal data for legitimate and lawful purposes, in accordance with the data protection principles.
- Data analysis is conducted for service improvement, research, and other purposes while safeguarding individual privacy.
- Anonymised or pseudonymised data may be used for research and statistical purposes where appropriate.

6. Working with and Sharing Data with Other Services

- We share data with other healthcare services involved in a patient's care, such as GP out-of-hours services, referral hospitals, and discharge facilities.
- We have data-sharing agreements in place with these services, outlining the specific data shared, security measures, and purpose of sharing.
- We only share data with the patient's consent or when legally required.

7. Contingency and Emergency Plans

- We have contingency plans in place to ensure the availability and integrity of data in case of emergencies, such as natural disasters or power outages.
- These plans include backup and recovery procedures to restore data and minimize disruption to services.
- We regularly test and update our contingency plans to ensure their effectiveness.

8. Confidentiality and Patient Choice

- We assure patients that their information is treated confidentially and in accordance with the Data Protection Act.
- We provide patients with information about their rights regarding their data, including the right to access, rectify, erase, and restrict processing.
- We have transparent mechanisms for patients to exercise their choices regarding their data, such as opting out of specific data-sharing arrangements.

9. Communication and Training

- We communicate this policy to all staff and ensure they understand their responsibilities for data protection.
- We provide regular training to staff on data security practices, data handling procedures, and patient confidentiality.
- We raise awareness of data protection among patients and encourage them to ask questions about how their data is used.

10. Review and Revision

This policy will be reviewed and revised regularly to reflect changes in legislation, best practices, and the clinic's operational context.

11. Commitment

Precision Surgery Clinic is committed to being a responsible data controller and ensuring the highest standards of data protection. We strive to build trust with our patients and stakeholders by upholding their privacy rights and safeguarding their personal information.