Data Protection and Information Security Policy

This practice is committed to complying with the Data Protection Act 2018, the General Data Protection Regulation (GDPR), GDC, NHS and other data protection requirements relating to our work. We only keep relevant information about employees for the purposes of employment and about patients to provide them with safe and appropriate health care. This policy should be read in conjunction with Data Protection Overview (M 216) and Information Governance Procedures (M 217C). This policy and all related policies, procedures and risk assessments are reviewed annually in iComply.

The person responsible for Data Protection is the Information Governance Lead Kimberley Lewis.

Our lawful basis for processing personal data is:

- Consent of the data subject
- Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract
- [Other]

Our lawful basis for processing special category data is:

- *Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional.*

Consent
The practice offers individuals real choice and control. Our consent procedures put individuals in charge to build customer trust and engagement. Our consent for marketing requires a positive opt-in, we don't use pre-ticked boxes or any other method of default consent. We make it easy for people to withdraw consent, tell them how to and keep contemporaneous evidence of consent. Consent to marketing is never a precondition of a service.

Data protection officer (DPO)
[NHS practice: Our DPO is the Information Governance Lead] [Fully private practice: We do not have a Data Protection Officer as we do not process large volumes of data.]

Pseudonymisation
Pseudonymisation means transforming personal data so that it cannot be attributed to an individual unless there is additional information.

- Pseudonymisation – the data can be tracked back to the original data subject
- Anonymisation – that data cannot be tracked back to the original data subject

Examples of pseudonymisation we use are:

- We never identify patients in research, patient feedback reports or other publically available information
- When we store and transmit electronic data it is encrypted and the encryption key is kept separate from the data

Data breaches
We report certain types of personal data breaches to the relevant supervisory authority within 72 hours of becoming aware of the breach, where feasible. If the breach results in a high risk of adversely affecting individuals' rights and freedoms we also inform those individuals without undue delay. We keep contemporaneous records of any personal data breaches, whether or not we need to notify.

Right to be informed
We provide 'fair processing information', through our Privacy Notice (M 217T), which provides transparency about how we use personal data.

Right of Access
Individuals have the right to access their personal data and supplementary information. The right of access allows individuals to be aware of and verify the lawfulness of the processing. If an individual contacts the practice to access their data they will be provided with, as requested:

- Confirmation that their data is being processed
- Access to their personal data
- Any other supplementary information or rights as found below and in our Privacy Notice (M 217T)

Right to erasure
The right to erasure is also known as 'the right to be forgotten'. The practice will delete personal data on request of an individual where there is no compelling reason for its continued processing. The right to erasure applies to individuals who are not patients at the practice. If the individual is or has been a patient, the clinical records will be retained according to the retention periods in Record Retention (M 215).

Right of rectification
Individuals have the right to have personal data rectified if it is inaccurate or incomplete.

Right to restriction
Individuals have a right to 'block' or suppress the processing of their personal data. If requested we will store their personal data, but stop processing it. We will retain just enough information about the individual to ensure that the restriction is respected in the future.

Right to object
Individuals have the right to object to direct marketing and processing for purposes of scientific research and statistics.

Data portability
An individual can request the practice to transfer their data in electronic or other format.

Privacy by design
We implement technical and organisational measures to integrate data protection into our processing activities. Our data protection and information governance management systems and procedures take Privacy by design as their core attribute to promote privacy and data compliance.

Records
We keep records of processing activities for future reference.

Privacy impact assessment
To identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy we review our Privacy Impact Assessment annually in iComply using the Sensitive Information Map, PIA and Risk Assessment (M 27Q).

Information security
Information Governance Procedures (M 217C) includes the following information security procedures:

- Team members follow the 'Staff Confidentiality Code of Conduct', which clarifies their legal duty to maintain confidentiality, to protect personal information and provides guidance on how and when personal or special category data can be disclosed
- How to manage a data breach, including reporting

- A comprehensive set of procedures, risk assessments and activities to prevent the data we hold being accidentally or deliberately compromised and to respond to a breach in a timely manner
- The requirements and responsibilities if team members use personal equipment such as computer, laptop, tablet or mobile phone for practice business

Review
This policy and the data protection and information governance procedures it relates to are reviewed annually with iComply.

CODE iComply related templates

G 110 – Complaints, Problems and Significant Events
G 110B - Event Register
G 110A - Event Record
G 135 – Backup Procedures and Software Log
G 135A – Computer Backup Log
G 135B – Purchased Software Log
M 215 - Record Keeping,
M 216 - Data protection Overview
M 216A - GDPR and Data Protection Act Action Plan
M 217A – Information Governance Improvement Plan (NHS practices only for online IG Toolkit)
M 217C – Information Governance Procedures
M 217D – Information Governance Lead Job Description
M 217E - Staff Confidentiality Agreement
M 217F - Subcontractors Confidentiality Agreement
M 217G - Information Asset Log
M 217H - Mobile Equipment Log
M 217I - Mobile Equipment Terms and Conditions
M 217K - Compliance Monitoring Form
M 217L – Computer and Software Access Log
M 217M – Physical Security Risk Assessment
M 217N - Business Impact Analysis
M 217P - Patient Leaflet on Personal Information
M 217Q - Sensitive Information Map, PIA and Risk Assessment
M 217RA - Communication Consent Form
M 217RB - Consent for Clinical Photography
M 217RX – Data Requests Record
M 217S – Legitimate Interests Assessment
M 217T – Privacy Notice
M 217UA - Model Contract for Data Processor
M 233-CON - Confidentiality Policy
M 233-CNS - Consent Policy
M 233-SMD - Social Medial Policy
M 255 - Disaster Planning and Emergency Procedures

Further information
Information Commissioner www.ico.org.uk
EU – US Privacy Shield www.privacyshield.gov
GDPR Regulation