Information Governance Policy

Introduction

Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources. It plays a key part in clinical governance, service planning and performance management. It is therefore of paramount importance that information is efficiently managed, and that appropriate policies, procedures, management accountability and structures provide a robust governance framework for information management.

Purpose of the policy

This information governance policy provides an overview of the practice's approach to information governance; a guide to the procedures in use; and details about the IG management structures within the dental practice.

The practice's approach to Information Governance

The practice undertakes to implement information governance effectively and will ensure the following:

· Information will be protected against unauthorised access;

· Confidentiality of information will be assured;

· Integrity of information will be maintained;

· Information will be supported by the highest quality data;

· Regulatory and legislative requirements will be met;

· Business continuity plans will be produced maintained and tested;

· Information governance training will be available to all staff as necessary to their role;

· All breaches of confidentiality and information security, actual or suspected, will be reported and investigated.

Procedures in use in the practice

This Information Governance policy is underpinned by the following procedures:

- Records management procedure that set outs how patient dental records will be created, used, stored and disposed of;
- Access control procedure that sets out procedures for the management of access to computer-based information systems;
- Information handling procedure that sets out procedures around the transfer of confidential information;
- Incident management procedure that sets out the procedures for managing and reporting information incidents;
- Business continuity plan that sets out the procedures in the event of a security failure or disaster affecting computer systems;

Staff guidance in use in the practice

Staff compliance with the procedures is supported by the following guidance material:

- Records management: guidelines on good record keeping;
- Staff confidentiality code of conduct sets out the required standards to maintain the confidentiality of patient information; obligations around the disclosure of information and appropriately obtaining patient consent;
- Access control: guidelines on the appropriate use of computer systems;
- Information handling: guidelines on the secure use of patient information;
- Using mobile computing devices: guidelines on maintaining confidentiality and security when working with portable or removable computer equipment;
- Information incidents: guidelines on identifying and reporting information incidents.

Responsibilities and accountabilities.

The designated Information Governance lead for the practice is Wajahida Anjum Syeda.

The key responsibilities of the lead are:

· Developing and implementing IG procedures and processes for the practice;

· Raising awareness and providing advice and guidelines about IG to all staff;

· Ensuring that any training made available is taken up;

· Coordinating the activities of any other practice staff given data protection, confidentiality, information quality, records management and Freedom of Information responsibilities;

· Ensuring that patient data is kept secure and that all data flows, internal and external are periodically checked against the Caldicott Principles;

· Monitoring information handling in the practice to ensure compliance with law, guidance and practice procedures;

· Ensuring patients are appropriately informed about the practice's information handling activities.

The day to day responsibilities for providing guidance to staff will be undertaken by Wajahida Anjum Syeda who is responsible for ensuring that sufficient resources are provided to support the effective implementation of IG in order to ensure compliance with the law, professional codes of conduct and the NHS information governance assurance framework. All staff, whether permanent, temporary or contracted, and contractors are responsible for ensuring that they are aware of and comply with the requirements of this policy and the procedures and guidelines produced to support it.

This policy has been approved by the undersigned and will be reviewed on an annual basis.

Approved By: Wajahida Anjum Syeda
Date Published: 11/11/2021

Data Protection & Information Security Policy

This practice is committed to complying with 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 and Information Governance Procedures. This policy and all related policies, procedures and risk assessments are reviewed annually.

The person responsible for Data Protection is Wajahida Anjum Syeda

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 do not 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)

Our DPO is Wajahida Anjum Syeda

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:

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 we need to notify.

Right to be informed

We provide 'fair processing information', through our Privacy Notice, 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 contact 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

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

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.

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 another 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 using the Sensitive Information Map, PIA and Risk Assessment.

Information security

Information Governance Procedures 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.

Further information

Information Commissioner www.ico.org.uk

EU – US Privacy Shield www.privacyshield.gov

GDPR Regulation

Approved By: Wajahida Anjum Syeda
Date Published: 11/11/2021