Woosehill Medical Centre

Information Governance Policy

Woosehill Medical Centre
01/05/2024

V1.2 November 2022

Contents

1. Introduction and Purpose

The role of the **Woosehill Medical Centre** (the Practice) is to deliver General Practitioner services to members of the public. In doing so, the Practice will uphold the NHS Constitution. This policy is important because it will help the people who work for the Practice to understand how to look after the information they need to do their jobs, and to protect this information on behalf of patients.

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

Information Governance looks at the way the NHS handles information about patients, staff, contractors and the healthcare provided, with particular consideration of personal and confidential information. Without access to information, it would be impossible to provide quality healthcare and good corporate governance. A robust governance framework needs to be in place to manage this vital asset, providing a consistent way to deal with the many different information handling requirements including:

- Information Governance Management
- Confidentiality and Data Protection Legislation assurance
- Corporate Information assurance
- Information Security assurance
- Secondary Use assurance

The aims of this document are to maximise the value of practical assets by ensuring that information is:

- Held securely and confidentially
- Obtained fairly and efficiently
- Recorded accurately and reliably
- Used effectively and ethically
- Shared appropriately and lawfully

To protect the practice's information assets from all threats, whether internal or external, deliberate or accidental, the Practice will ensure that:

- 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 security training will be available to all staff

2. Scope and Definitions

Scope

The scope of this document covers:

- All permanent employees of the Practice and;
- Staff working on behalf of the Practice (including contractors, temporary staff, and secondees).

The Practice recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The Practice fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard information. The Practice also recognises the need to share information in a controlled manner. The Practice believes that accurate, timely and relevant information is essential to deliver the highest quality health care. As such, it is the responsibility of managers and staff to ensure and promote the quality of information and to actively use information in decision making processes.

Definitions

In order to assist staff with understanding their responsibilities under this policy, the following types of information and their definitions are applicable in all relevant policies and documents.

Personal Data (derived from the UK GDPR)	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
'Special Categories' of Personal Data (derived from the UK GDPR)	'Special Categories' of Personal Data is different from Personal Data and consists of information relating to: (a) The racial or ethnic origin of the data subject (b) Their political opinions (c) Their religious beliefs or other beliefs of a similar nature (d) Whether a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1998 (e) Genetic data (f) Biometric data for the purpose of uniquely identifying a natural person (g) Their physical or mental health or condition (h) Their sexual life
Personal Confidential Data	Personal and Special Categories of Personal Data owed a duty of confidentiality (under the common law). This term describes personal information about identified or identifiable individuals, which should be kept private or secret. The definition includes dead as well as living people and 'confidential' includes information 'given in confidence' and 'that which is owed a duty of confidence'. The term is used in the Caldicott 2 Review: Information: to share or not to share (published March 2013).

Commercially confidential Information	Business/Commercial information, including that subject to statutory or regulatory obligations, which may be damaging to the Practice or a commercial partner if improperly accessed or shared. Also as defined in the Freedom of Information Act 2000 and the Environmental Information Regulations.
Sensitive Data (Derived from UK GDPR)	'Sensitive Data' is different from Personal or Special Category data as it is derived from Article 10 of the UK GDPR and is information relating to "data relating to criminal convictions and offences or related security measures"

3. Legal Compliance

The Practice regards all identifiable personal information as confidential except where national policy on accountability and openness requires otherwise.

The Practice will maintain policies to ensure compliance with Data Protection Legislation. This includes the UK General Data Protection Regulation (UK GDPR), the Data Protection Act (DPA) 2018, the Law Enforcement Directive (Directive (EU) 2016/680) (LED) and any applicable national Laws implementing them as amended from time to time.

In addition, consideration will also be given to all applicable Law concerning privacy, confidentiality, the processing and sharing of personal data, including the Human Rights Act 1998, the Health and Social Care Act 2012 as amended by the Health and Social Care (Safety and Quality) Act 2015, the common law duty of confidentiality and the Privacy and Electronic Communications (EC Directive) Regulations.

The Practice, when acting as a Controller, will identify and record a condition for processing, as identified by the UK GDPR under Articles 6 and 9 (where appropriate), for each activity it undertakes. When relying on Article 6, 1 (e) ' processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller', the Practice will identify the official authority (legal basis) and record this on relevant records of processing.

4. Roles and Responsibilities

The Practice has a responsibility for ensuring that it meets its corporate and legal responsibilities and for the adoption of internal and external governance requirements. The Practice is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

Senior Practice Management Team

It is the role of the Senior Practice Management Team to define the Practice policy in respect of Information Governance, taking into account legislative and NHS requirements. The Senior Practice Management Team is also responsible for:

- ensuring that sufficient resources are provided to support the requirements of the policy

- appropriate mechanisms are in place to support service delivery and continuity

Practice Manager

The Practice Manager is responsible for overseeing day to day Information Governance issues; developing and maintaining policies, standards, procedures and guidance; coordinating Information Governance in the Practice and raising awareness of Information Governance.

All staff have responsibility for complying with this policy and with Data Protection Legislation; the following roles have specific responsibilities:

Caldicott Guardian

The Caldicott Guardian is the person within the Practice with overall responsibility for protecting the confidentiality of personal data and special categories of personal data (described as Personal Confidential Data (PCD)) in line with the National Data Guardian reports, and for ensuring it is shared appropriately and in a secure manner. This role has the responsibility to advise the Practice on confidentiality issues.

Data Protection Officer

The Data Protection Officer (DPO) is the person that has been identified by the Practice that has the responsibilities as set out in the UK GDPR guidance. This includes monitoring compliance with IG legislation, providing advice and recommendations on Data Protection Impact Assessments, giving due regard to the risks associated with the processing of data undertaken by the practice and acting as the contact point with the ICO.

5. Processes/Requirements

The Practice will ensure that it meets its national requirements in respect of its submission of the annual self-assessment Data Security and Protection Toolkit (DSPT).

Non-confidential information about the Practice and its services will be available to the public through a variety of media.

The Practice will maintain policies to ensure compliance with the Freedom of Information Act.

The Practice will maintain clear procedures and arrangements for handling requests for information from the public. Please refer to the Practice's Subject Access Request Policy in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act (DPA) 2018.

The Practice will maintain policies to ensure compliance with the Records Management Code of Practice 2021. NHSX_Records_Management_CoP_V7.pdf (england.nhs.uk) Please refer to The Practice Records Management Policy.

6. Information Security

The Practice will maintain policies for the effective and secure management of its information assets and resources.

The Practice will promote effective confidentiality and security practice to its staff through policies, procedures and training. [Please refer to the Practice Information Security, Remote Working and Portable Devices and Network Security policies].

The Practice will adhere to the NHS Digital Guide to the Notification of Data Security and Protection Incidents[1] and as part of this, will review and maintain incident reporting procedures and monitor and investigate all reported instances of actual or potential breaches. Under Data Protection Legislation, where an incident is likely to result in a risk to the rights and freedoms of the Data Subject/individuals the Information Commissioner's Office (ICO) must be informed no later than 72 hours after the practice becomes aware of the incident. Please refer to the Practice Incident Reporting Policy.

7. Information Quality Assurance

The Practice will maintain policies and procedures for information quality assurance and the effective management of records.

The Practice will undertake or commission annual assessments and audits of its information quality and records management arrangements. Staff are expected to take ownership of, and seek to improve, the quality of information within the Practice. Wherever possible, information quality should be assured at the point of collection.

Data standards will be set through clear and consistent definition of data items, in accordance with national standards.

8. Implementing new services

The Data Protection Officer should be consulted during the design phase of any new service, process or information asset and contribute to the statutory Data Protection Impact Assessment (DPIA) process when new processing of personal data or special categories of personal data is being considered. Responsibilities and procedures for the management and operation of all information assets should be defined and agreed by the Senior Practice Management Team.

All staff members who may be responsible for introducing changes to services, processes or information assets must be effectively informed about the requirement to complete a statutory DPIA in advance of proceeding with the proposed change.

The Practice will maintain a DPIA process that includes an approved template, guidance and supporting checklists.

[1] https://www.dsptoolkit.nhs.uk/Help/incident-reporting

9. Training

All new starters to the Practice inclusive of temporary, bank staff and contractors must undertake Data Security induction training via an approved training platform to evidence compliance with the Data Protection Legislation and the DSPT assertions as part of the induction process. Extra training will be given to those dealing with requests for information. A register will be maintained of all staff who have completed the annual data security online training.

10. Monitoring and Review

This policy will be monitored by the **Partners and Management Team** to ensure any legislative changes that occur before the review date are incorporated.

Compliance with Practice policies is stipulated in staff contracts of employment. If staff members are unable to follow Practice policies or the policy requirements cannot be applied in a specific set of circumstances, this must be immediately reported to the Line Manager, who should take appropriate action. Any non-compliance with Practice policies or failure to report non-compliance may be treated as a disciplinary offence.

This policy will be reviewed **01/05/2025** by the **Partners and Management Team** or sooner if required by law.

11. References and Associated Codes of Practice

- NHS Digital Codes of Practice
- Department of Health Code of Practice
- CQC Code of Practice
- Health and Social Care (Safety and Quality) Act 2015
- NHS England Confidentiality Policy
- All Practice policies, procedures and guidance relating to the management and processing of information within the organisation

END of POLICY

Document Control

This document was created by NHS South Central and West Commissioning Support Unit (SCW) and as such the Intellectual Property Rights of this document belong to SCW.

Document Name	Version	Status	Author
Information Governance Policy Primary Care template	1.2	Published	NHS SCW Information Governance Services
Document objectives	This policy supports Practice staff in compliance with Data Protection legislation, achieving best practice in the area of Information Governance and in meeting the requirements of the Data Security and Protection Toolkit		
Target audience	All staff		
Monitoring arrangements and indicators	This policy will be monitored by NHS SCW Information Governance Services to ensure any legislative changes that occur before the review date are incorporated.		
Review frequency	SCW reviews customer documents in line with our planned schedule		
SCW Planned Review date	01 November 2023		
Date uploaded to SCW Website	March 2023		
Approved & ratified by practice	Woosehill Medical Centre	01/05/2024	
Date issued by practice	01/05/2024		
GP Review date	01/05/2025		

Change record

Date	Author	Version	Page/s	Reason for Change
28.08.2020	SCW	1	All	Review for Website publication
26.10.2021	SCW	1.1	All	Update UK GDPR in all sections
01.11.2022	SCW	1.2	All	All links updated