Information Governance Policy

Approved by: Mr Alex Davies

Version: Version 2024,1.0

Last Updated: 07/03/20204

Review date: 07/03/2025

Gwasanaeth Cefnogi
Swyddog Diogelu Data
Data Protection Officer
Support Service

Contents

1. Document history

1.1. Revision history

Date	Version	Author	Revision Summary
07/03/2024	2024-1.0	Mr Alex Davies	This policy has been based upon Version 3.0 of the DPO Support Service Template

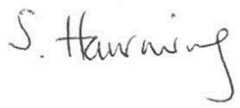
1.2. Reviewers

This document requires the following reviews:

Date	Version	Name	Position

1.3. Authorisation

Signing of this document indicates acceptance of its contents.

Approver's Name:	Caldicott Guardian
Role:	GP Partner
Signature:	 Dr Steve Harrowing Senior Partner Caldicott Guardian 07/03/2024

2. Introduction

This Policy has been developed in line with the All Wales Information Governance Policy.

Information Governance is a framework for handling personal information in a confidential and secure manner to appropriate ethical and quality standards. It provides a consistent way for employees to deal with the many different information handling requirements including:

- Information governance management
- Clinical information assurance for safe patient care
- Confidentiality and data protection assurance
- Corporate information assurance
- Information security assurance
- Secondary use assurance
- Respecting data subjects' rights regarding the processing of their personal data

The arrangements set out in this document and other related policies and procedures are intended to achieve this demonstrable compliance.

3. Scope

This policy applies to all staff of THE VALE OF NEATH PRACTICE.

The term 'staff' includes all health professionals, partners, staff members, locums, students, trainees, secondees, volunteers, contracted third parties and any persons undertaking duties on behalf of THE VALE OF NEATH PRACTICE.

This policy should be read in conjunction and reviewed in-line with the following:

Records Management Policy
Information Security Policy
Data Quality Policy

Breaches of this policy will be reported via the Practice's incident reporting processes and dealt with in line with the Practice's Disciplinary Policy where appropriate.

4. Policy Objectives

The aim of this policy is to provide all employees of the Practice with a framework to ensure all personal data is acquired, stored, processed and transferred in accordance with the law and associated standards. These include the Data Protection Act 2018, UK General Data Protection Regulation 2016 (UK GDPR), the common law duty of confidentiality, NHS standards such as the Caldicott Principles, and associated guidance issued by Welsh Government, the Information Commissioner's Office, and other professional bodies.

The objectives of the Policy are to:

- Set out the legal, regulatory and professional requirements, and
- Provide staff with the guidance to understand their responsibilities for ensuring the confidentiality and security of personal data

This policy supports staff to demonstrate that personal information is:

- Held securely and confidentially
- Processed fairly and legally
- Obtained for specific purpose(s)
- Recorded accurately and kept up to date
- Used only when necessary and ethically, and
- Lawfully disclosed and shared

To minimise risks of any threats and to protect information assets, these being internal or external, deliberate or accidental, the Practice will ensure:

- Measures will be in place to protect information from unauthorised access
- Confidentiality of information is prioritised and assured
- Integrity of information will be maintained
- All regulatory and legislative requirements will be met
- All data will be maintained and supported by the highest quality data
- Business continuity plans will be maintained, tested and adhered to
- Information Governance training will be provided to all staff, and
- All Information Governance breaches and near misses will be investigated, and relevant breaches will be reported to the Data Protection Officer and Information Commissioner's Office

5. Roles and Responsibilities

5.1. Senior Responsible Person

The Senior Responsible Person within the Practice is responsible for ensuring the highest level of organisational commitment to this policy and the availability of resources to support its implementation. Where appropriate, the Senior Responsible Person may delegate specific responsibilities to other individuals who have responsibility for information governance within the Practice.

The Senior Responsible Person will ensure that all staff are aware of this policy, understand their responsibilities in complying with the requirements of this policy and are up to date with mandatory information governance training.

Additionally, the Senior Responsible Person will ensure the key roles outlined below are established within the Practice's management structure.

The Senior Responsible Person within THE VALE OF NEATH PRACTICE is Caldicott Guardian.

5.2. Information Governance Lead

The Information Governance (IG) Lead is responsible for liaising with and supporting the Data Protection Officer and Caldicott Guardian in coordinating and implementing the confidentiality and data protection work programme within the Practice.

Where necessary, the IG Lead will supervise and direct the work of others to aid the Practice in meeting its information governance responsibilities.

The IG Lead will act as the first point of contact for information governance queries within the Practice.

The Information Governance Lead within THE VALE OF NEATH PRACTICE is Caldicott Guardian.

5.3. Data Protection Officer

The Data Protection Officer (DPO) provides independent risk-based advice to support the Practice in its decision making in the appropriateness of processing personal and special categories of data within the Principles and Data Subject Rights laid down in the UK General Data Protection Regulation (UK GDPR).

The DPO role is to 'inform and advise' and not 'to do', they are a trusted advisor whom the Practice should actively seek advice from.

The Data Protection Officer for THE VALE OF NEATH PRACTICE is the Digital Health and Care Wales (DHCW) Data Protection Officer Support Service.

The DPO can be contacted by emailing DHCWGMPDPO@wales.nhs.uk.

5.4. Caldicott Guardian

The Caldicott Guardian has responsibility for ensuring that patient information is used legally, ethically, and appropriately, and that confidentiality is always maintained. Caldicott Guardians should be able to provide leadership and informed guidance on complex matters involving confidentiality and information sharing.

The Caldicott Guardian will apply the eight principles and act as "the conscience of the Practice" regarding information sharing.

The Caldicott Guardian within THE VALE OF NEATH PRACTICE is Dr Steve Harrowing.

5.5. All Staff

All staff have a responsibility for information governance and maintaining appropriate security for their own work area.

All staff must familiarise themselves with the policy content and ensure the policy requirements are implemented and followed within their own work area. Mandatory information governance training must be undertaken at least every two years.

6. Policy

6.1. Data Protection and Compliance

Data protection legislation is about the rights and freedoms of living individuals and in particular their right to privacy in respect of their personal data. The Data Protection Act 2018 (DPA) and the UK General Data Protection Regulation 2016 (UK GDPR) stipulate that those who record and use any personal data must be open, clear and transparent about why personal data is being collected and how the personal data is going to be used, stored and shared.

Whilst the emphasis on this policy is on the protection of personal data, the Practice will also process business sensitive data and the provision for the security of this data will also be governed by this policy as appropriate.

6.1.1. Personal Data

For the purpose of this policy, the use of the term 'personal data' relates to any information that can identify or assist in the identification of any living person(s).

Examples of key identifiable personal data include, but are not limited to; name, address, postcode, date of birth, NHS number, National Insurance number, images, video and audio recordings, IP addresses and e-mail addresses.

6.1.2. Special Category Data

Special category data is defined by data protection legislation as any data concerning an individual's racial or ethnic origin, political opinion, religious or philosophical belief, trade union membership, health, sex life, sexual orientation, genetic and biometric data where processed to uniquely identify an individual.

6.1.3. Fair and Lawful Processing

Under data protection legislation, personal data, including special category data, must be processed fairly and lawfully. Processing broadly means; collecting, using, disclosing, sharing, retaining or disposing of personal data or information.

In order for processing to be fair, the Practice will be open and transparent about the way it processes personal data by informing individuals using a variety of methods. In order to provide assurance the Practice will identify and record the lawful basis for the information it processes in all privacy notices and in a Register of Processing Activities (**ROPA**).

6.1.4. Individuals Rights

Under data protection legislation, individuals have several rights with regards to the processing of their personal data. The Practice will ensure that appropriate arrangements are in place to manage these rights.

6.1.5. Accuracy of Personal Data

The Practice will ensure that arrangements are in place to ensure that any personal data held by the Practice is accurate and up to date.

6.1.6. Data Minimisation

The Practice will use the minimum amount of identifiable information required when processing personal data and where appropriate, will ensure that personal data is anonymised or pseudonymised.

6.1.7. Data Protection Impact Assessments (DPIAs)

When developing any new projects or agreeing flows of information, the Practice will consider information governance practices from the outset to ensure that personal data is protected at all times. This also provides assurance that the Practice is working to the necessary standards and are complying with data protection legislation. In order to identify information risks, the practice will complete a Data Protection Impact Assessment.

6.1.8. Incident Management and Breach Reporting

The Practice will have arrangements in place to; identify, report, manage and resolve any data breaches within specified legal timescales. Any incidents that occur will be learnt from to continually improve procedures and services that the Practice provides. Incidents must be reported immediately following the Practice's policy.

6.1.9. Information Governance Compliance

The Practice will have the necessary arrangements in place to monitor information governance compliance. Any risks identified must be managed in line with the Practice's risk management policy.

6.1.10. Information Asset Management

Information assets will be catalogued and managed by the Practice through the use of an Information Asset Register which will be regularly reviewed and kept up to date.

6.1.11. Third Parties and Contractual Arrangements

Where the Practice engages any third party who processes personal data on its behalf, any processing will be subject to a legally binding contract or Data Processing Agreement. This will meet the requirements of data protection legislation. Where the third party is the supplier of services, appropriate and approved codes of conduct or certification schemes will be considered to help demonstrate that the practice has chosen a suitable processer.

6.2. Information Security

The Practice will maintain the appropriate confidentiality, integrity and availability of its information, and information services, and manage the risks from internal and external threats in line with the Practice's Information Security Policy.

6.3. Records Management

The Practice will have a systematic and planned approach to the management of records from their creation to their disposal. This will ensure that the practice can control the quality and quantity of the information that it generates, can maintain that information in an effective manner, and can dispose of information appropriately when its retention periods have expired.

6.4. Access to Information

The Practice may be required by law to disclose information. This includes complying with requests made under the Freedom of Information Act and Subject Access Requests. The Practice will ensure processes are in place for the disclosure of information under these circumstances. Where required, advice will be sought from the Practice's Data Protection Officer by contacting the DPO Support Service at DCHWGMPDPO@wales.nhs.uk.

6.5. Confidentiality

6.5.1. Confidentiality: Code of Practice for Health and Social Care in Wales

Code of Practice for Health and Social Care in Wales

The Practice has adopted the Confidentiality: Code of Practice for Health and Social Care in Wales. All staff have an obligation of confidentiality regardless of their role and are required to respect the personal data and privacy of others.

Staff must not access information about any individuals who they are not providing care, treatment or administration services to in a professional capacity. Rights to access information are provided for staff to undertake their professional role and are for work related purposes only.

Appropriate information will be shared securely with other NHS and partner organisations in the interests of direct patient care and service management.

6.5.2. Caldicott

The Practice will uphold the Caldicott Principles in relation to patient information and appoint a Caldicott Guardian whose role is to safeguard the processing of patient information.

6.6. Sharing Personal Data

6.6.1. Wales Accord on the Sharing of Personal Data

The WASPI Framework provides good practice to assist the practice to share personal data effectively and lawfully. WASPI is utilised by organisations directly concerned with the health, education, safety, crime prevention and social wellbeing of people in Wales.

The Practice will use the WASPI Framework for any situation that requires the regular sharing of information for example where cluster working is necessary to deliver direct care.

6.6.2. One off Disclosures of Personal Data

Personal data may need to be shared externally on a one-off basis, where an Information Sharing Protocol or equivalent sharing document does not exist. The Practice will ensure that sharing follows all the principles of good information governance and that local arrangements are made and followed to ensure suitable processes are in place.

6.7. Information Assets

6.7.1. The Control Standard

The Wales Control Standard for Electronic Health and Care Records describes the principles and common standards that apply to shared electronic health and care records in Wales. It provides the mechanism through which organisations commit to them.

6.7.2. Asset Registers

A register of core national systems is maintained by Digital Health and Care Wales and sets out how shared electronic health and care records are held. The Practice will have a local asset register. The Practice will ensure suitable processes are in place to ensure the asset register is accurate and up to date.

6.8. Data Quality

The Practice processes large amounts of data and information as part of their everyday business. For data and information to be of value they must be of a suitable standard.

Poor quality data and information can undermine the efforts to deliver its objectives and for this reason the Practice is committed to ensuring that the data and information it holds and processes is of the highest quality reasonably practicable under the circumstances. All staff have a duty to ensure that any information or data that they create or process is accurate, up to date and fit for purpose. The Practice will implement procedures where necessary to support staff in producing high quality data and information.

7. Training and Awareness

Information governance is everyone's responsibility. Training is mandatory for all Practice staff and must be completed at commencement of employment and at least every two years subsequently. Non-NHS employees must have appropriate information governance training in line with the requirements of their role.

Staff who need support in understanding the legal, professional and ethical obligations that apply to them should contact the practice information governance lead or the DPO Support Service.

8. Monitoring and Compliance

The Practice trusts its workforce; however, it reserves the right to monitor work processes to ensure the effectiveness of the service. This will mean that any personal activities that staff practice in work may come under scrutiny. THE VALE OF NEATH PRACTICE respects the privacy of its staff and does not want to interfere in their personal lives but monitoring of work processes is a legitimate business interest.

Staff of the Practice should be reassured that the Practice takes a considered approach to monitoring, however it reserves the right to adopt different monitoring patterns as required. Monitoring is normally conducted where it is suspected that there is a breach of either policy or legislation. Furthermore, on deciding whether such analysis is appropriate in any given circumstances, full consideration is given to the rights of the employee.

Managers are expected to speak to staff of their concerns should any minor issues arise. If breaches are detected an investigation may take place. Where this or another policy is found to have been breached, disciplinary procedures will be followed.

Concerns about possible fraud and or corruption should be reported to the counter fraud department.

In order for the Practice to achieve good information governance practice staff must be encouraged to recognise the importance of good governance and report any breaches to enable lessons learned. They must be provided with the necessary tools, support, knowledge and training to help them deliver their services in compliance with legislation.

Ultimately a skilled workforce will have the confidence to challenge bad information governance practice, and understand how to use information legally in the right place and at the right time. This should minimise the risk of incidents occurring or recurring.

9. Review

This policy will be reviewed every 12 Months or more frequently where the contents are affected by major internal or external changes such as:

- Changes in legislation;
- Practice change or change in system/technology; or
- Changing methodology.