CATHAYS SURGERY

Information Governance Policy

Version: 1.0

Last Reviewed: August 2021

Author: NWIS DPO Support Service

Table of Contents

1.0 Introduction 4
2.0 Objective 5
3.0 Scope 5
4.0 Purpose 5
5.0 Roles and Responsibilities 6
5.1 Practice Manager and Senior Partner 6
5.2 Data Protection Officer 6
6.0 Policy 7
6.1 Data Protection and Compliance 7
6.2. Personal Data 7
6.3 Special Category Data 7
6.4 Fair and Lawful Processing 7
6.5 Individuals Rights 7
6.6. Accuracy of Personal Data 8
6.7 Data Minimisation 8
6.8 Data Protection Impact Assessments (DPIA's) 8
6.9 Incident Management and Breach Reporting 8
6.10 Information Governance Compliance 8
6.11 Information Asset Management 8
6.13 Third Parties and Contractual Arrangements 8
7.0 Information Security 9
7.1 Records Management 9
7.2 Access to Information 9
7.3 Confidentiality 9
7.3.1 Confidentiality: code of Practice for Health and Social Care in Wales 9
7.3.2 Caldicott 9
7.4 Sharing Personal Data 10
7.4.1 Wales Accord on the Sharing of Personal Data 10
7.4.2 One off Disclosures of Personal Data 10
7.5 Welsh Control Standard 10
7.5.1 The Control Standard 10
7.5.2 The Register for Information Sharing Systems 10

7.6 Data Quality 10
8.0 Training and Awareness 11
9.0 Monitoring and Compliance 11
10.0 Review 12
11.0 Equality Impact Assessment 12

1.0 Introduction

This Policy has been developed in line with the All Wales Information Governance Policy to be adopted by Cathays Surgery with assistance from the Data Protection Officer Support Service.

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 Data Protection Act 2018, General Data Protection Regulation 2016 (**GDPR**), the common law duty of confidence, NHS standards such as the Caldicott Principles, and associated guidance issued by the Welsh Government, the Information Commissioner's Office, and other professional bodies.

It is known that Information is a vital asset, both in terms of the clinical management of individual patients, ongoing management of corporate records and the efficient management of services and resources of the Practice. It is therefore paramount to ensure that information is efficiently managed, and that appropriate policies, procedures and management accountability, provide a robust governance framework for information management.

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.

2.0 Objective

The Practice recognises the need for an appropriate balance between openness and confidentiality in the management and use of personal information, and 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, both personal information about patients, staff and commercially sensitive information. The Practice also recognises the need to share patient information with other health organisations in a controlled manner consistent with the interests of the patient and, in some circumstances, the public interest, all within compliance with the Data Protection Act 2018 and the General Data Protection Regulation 2016.

3.0 Scope

This policy applies to all staff and includes any person who forms part of the workforce including but not limited to, permanent and temporary staff, students, trainees, volunteers, agency workers, contracted third parties and any other person(s) that regularly undertake duties on behalf of the Practice.

All duties are defined as any action that involve the review, handling, management and or processing of any personal information for and on behalf of the practice. This covers all processing by individuals for business functions, including information systems, networks and physical environment.

4.0 Purpose

The purpose of this policy is to inform all members of the workforce (permanent or otherwise) of their Information Governance responsibilities including the management arrangements that may be in place to demonstrate compliance with national standards, the General Data Protection Regulation 2016 and the Data Protection Act 2018.

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 priority 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

5.0 Roles and Responsibilities

5.1 Practice Manager and Senior Partner

The Practice Manager/Senior Partner is responsible for ensuring the highest level of commitment to the policy and the availability of resources to support its implementation. Specific responsibilities will be delegated to the Data Protection Officer who are the contracted service provided by the DPO Support Service, provided by the NHS Wales Informatics Service.

The Practice Manager/Senior Partner is responsible for the implementation of this policy throughout the Practice. In addition, they must ensure that all staff are aware of this policy, understand their responsibilities in complying with the policy requirements and are up to date with mandatory information governance training.

The workforce 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. Breaches of the policy must be reported in line with the Practice reporting and escalation processes and dealt with in line with the Practices' disciplinary process where appropriate.

5.2 Data Protection Officer

The Data Protection Officer (**DPO**) is provided through the Data Protection Support Service contracted through NHS Wales Informatics Services (**NWIS**). They're role is to act as the Practices trusted advisor, to 'inform and advise' and not 'to do' or 'decide' on behalf of the practice. The service also provides an open access forum for Practices to actively seek IG advice. The DPO Support Service will assist the Practice to operate within the law by advising and helping to monitor and demonstrate compliance. They play a key role in the practice's data protection governance structure and help to improve and facilitate 'accountability' to comply with General Data Protection Regulation.

6.0 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 General Data Protection Regulation 2016 (**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 own business sensitive data and provision for the security of this data will also be governed by this policy as appropriate.

6.2. 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.

6.3 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.

6.4 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**).

6.5 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.

6.6. 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.

6.7 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.

6.8 Data Protection Impact Assessments (DPIA's)

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.

6.9 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 as soon as they are found following the practices policy.

6.10 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 Practices risk management policy.

6.11 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.

6.13 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.

7.0 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.

7.1 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.

7.2 Access to Information

The Practice may be required by law to disclose information. This would include complying with Freedom of Information Act requests 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 practices Data Protection Officer by contacting the DPO Support Service at **NWISGMPDPO@wales.nhs.uk**.

7.3 Confidentiality

7.3.1 Confidentiality: code of Practice for Health and Social Care in Wales

Confidentiality: Code of Practice for Health and Social Care.pdf

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.

7.3.2 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.

7.4 Sharing Personal Data

7.4.1 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.

7.4.2 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.

7.5 Welsh Control Standard

7.5.1 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. The Practice has committed to abide by the Control Standard. The Control Standard will be underpinned by local level policies and procedures to ensure electronic records are accessed and used appropriately.

7.5.2 The Register for Information Sharing Systems

A register of core national systems is maintained by the NHS Wales Informatics Service and sets out how shared electronic health and care records are held. The Practice may include 'local' systems in their own local register. Cooperation must be maintained between organisations and the NHS Wales Informatics Service in order to ensure that the information is accurate and up to date.

7.6 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.

8.0 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 appropriate practice information governance lead or the DPO Support Service.

9.0 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 the employee's practices in work may come under scrutiny. [Practice Name] respect the privacy of its employees 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.

10.0 Review

This policy will be reviewed every two years 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;
- Change in Senior personnel e.g. Practice Manager or Senior Partner or
- Changing methodology.

11.0 Equality Impact Assessment

This policy has been subject to an equality assessment.

Following assessment, this policy was not felt to be discriminatory or detrimental in any way with regard to the protected characteristics, the Welsh Language or carers.