NHS Wales
Information Governance Policy

Author: Information Governance Management Advisory Group Policy Sub Group
Approved by: Information Governance Management Advisory Group
Approved by: Wales Information Governance Board
Version: 2
Date: 14th January 2021
Review date: 13th January 2023

This Page is intentionally blank

Contents

1. Introduction

This document is issued under the All Wales Information Governance Policy Framework and maintained by the NHS Wales Informatics Service (NWIS) on behalf of all NHS Wales organisations.

2. Purpose

The aim of this Policy is to provide all NHS Wales employees 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 legislation, the common law duty of confidence, NHS standards such as the Caldicott Principles, and associated guidance issued by Welsh Government, Information Commissioner's Office (ICO), Department of Health and other professional bodies.

The objectives of the Policy are to:

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

3. Scope

This policy applies to the workforce of all NHS Wales organisations including staff, students, trainees, secondees, volunteers, contracted third parties and any other persons undertaking duties on behalf of NHS Wales.

For the purpose of this policy 'NHS Wales Organisations' include all Health Boards and NHS Trusts.

It applies to all forms of information processed by NHS Wales organisations; and covers all business functions and the information, information systems, networks, physical environment and relevant people who support those business functions.

For the purpose of this policy, the use of the term "personal data" refers to information relating to both living and deceased individuals. Examples of key identifiable personal data include (but are not limited to) name, address, full postcode, date of birth, NHS number, National Insurance number, images, recordings, IP addresses, email addresses etc.

For the purpose of this policy "special category data" refers to the types of personal data that are defined by data protection legislation as relating to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life, sexual orientation, genetic and biometric data where processed to uniquely identify an individual. Some special category data is also protected by legislation separate to the data protection legislation. For example information relating to certain sexually transmitted diseases is subject to separate legislative provisions in certain circumstances.

4. Roles and responsibilities

The Chief Executive is responsible for ensuring the highest level of organisational commitment to the policy and the availability of resources to support its implementation and any associated legal requirements. Specific responsibilities will be delegated to the Chief Information Officer, the Data Protection Officer, Senior Information Risk Officer and the Caldicott Guardian or an Executive Director as appropriate.

NHS Wales Organisations must have the following key roles in place:

- **Chief Information Officer (CIO):** The most senior executive responsible for the management, implementation, and usability of information and computer technologies in an organisation;
- **Senior Information Risk Owner (SIRO):** An Executive Director or member of the Senior Management Board of an organisation with delegated responsibility from the CEO for an organisation's information risk policy. The SIRO is accountable and responsible for information risk across the organisation. The SIRO is accountable and responsible for information risk across the organisation;
- **Caldicott Guardian:** A senior person with delegated responsibility from the CEO for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing;
- **Data Protection Officer (DPO):** A data protection expert who is responsible for monitoring an organisation's compliance; informing and advising the organisation on its data protection obligations, and acting as a contact point for data subjects and the Information Commissioner's Office (ICO).

Managers are responsible for the implementation of this policy within their department/directorate. In addition, they must ensure that their 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 via local incident reporting processes and dealt with in line with the All Wales Disciplinary Policy where appropriate.

5. Policy

5.1 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. It stipulates 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 data is going to be used, stored and shared.

While the emphasis of this policy is on the protection of personal data, organisations will also own business sensitive data and provision for the security of that data will also be governed by this policy as appropriate.

5.1.1 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 the processing to be fair, NHS Wales organisations must be open and transparent about the way it processes personal data by informing individuals using a variety of methods. The most common way to provide this information is in a privacy notice. Guidance must be made available to staff to enable them to produce and make available privacy notices in line with the legislation.

5.1.2 Individual's Rights

Individuals have certain rights with regard to the processing of their personal data. NHS Wales organisations must ensure that appropriate arrangements are in place to manage these rights. Staff must follow their organisational procedures and guidance to ensure requests relating to individual rights are managed appropriately.

5.1.3 Accuracy of Personal Data

Arrangements must be in place to ensure that any personal data held by NHS Wales organisations is accurate and up to date. Staff must follow their organisational procedures and guidance to ensure that information, howsoever held is maintained appropriately.

5.1.4 Data Minimisation

NHS Wales organisations will use the minimum amount of identifiable information required when processing personal data. Where appropriate, personal data must be anonymised or pseudonymised. Staff must follow their organisational procedures and guidance to ensure the principle of data minimisation is appropriately upheld.

5.1.5 Data Protection Impact Assessment (DPIA)

All new projects or major new flows of information must consider information governance practices from the outset to ensure that personal data is protected at all times. This also provides assurance that NHS Wales organisations are working to the necessary standards and are complying with data protection legislation. In order to identify information risks a DPIA must be completed. Your information governance department will provide the required guidance and template.

5.1.6 Incident Management and Breach Reporting

NHS Wales organisations must have arrangements in place to identify, report, manage and resolve any data breaches within specified legal timescales. Lessons learnt will be shared to continually improve procedures and services, and consideration given to updating risk registers accordingly. Incidents must be reported immediately following local reporting arrangements.

5.1.7 Information Governance Compliance

NHS Wales organisations must have arrangements in place to monitor information governance compliance. Staff are required to assist in this activity when required. This may include providing evidence in relation to an investigation, or for completion of the information governance toolkit.

Any risks identified must be managed in line with local risk management arrangements.

5.1.8 Information Asset Management

Information assets will be catalogued and managed by NHS Wales organisations by using an Information Asset Register which must be regularly reviewed and kept up to date.

5.1.9 Third Parties and Contractual Arrangements

Where the organisation uses any third party who processes personal data on its behalf, any processing must be subject to a legally binding written contract which meets the requirements of data protection legislation. Where the third party is a supplier of services, appropriate and approved codes of conduct or certification schemes must be considered to help demonstrate that the organisation has chosen a suitable processor.

5.2 Information Security

NHS Wales organisations will maintain the appropriate confidentiality, integrity and availability of its information, and information services, and manage the risks from internal and external threats. Please refer to the National Information Security Policy for further details.

5.3 Records Management

NHS Wales organisations must have a systematic and planned approach to the management of records in the organisation from their creation to their disposal. This will ensure that organisations 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 efficiently when it is no longer required and outside the retention period.

5.4 Access to Information

NHS Wales organisations are in some circumstances required by law to disclose information. Examples include, but are not limited to, information requested under Data Protection legislation, Access to Health Records legislation, the Freedom of Information Act, the Environmental Information Regulations.

Processes must be in place for disclosure under these circumstances. Where required, advice should be sought from the organisation's information governance department.

5.5 Confidentiality

All staff have an obligation of confidentiality regardless of their role and are required to respect the personal data and privacy of others in line with the Common Law Duty of Confidence, and the Caldicott Principles.

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. It is only acceptable for staff to access their own record where self-service access has been granted.

Appropriate information will be shared securely with other NHS and partner organisations in the interests of patient, donor care and service management. (See section 5.6 on Information Sharing for further details).

5.6 Sharing Personal Data

The WASPI Framework provides good practice to assist organisations 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.

NHS Wales organisations will use the WASPI Framework for any situation that requires the regular sharing of information outside of NHS Wales wherever appropriate. Advice must be sought from the information governance department in such circumstances.

Formal Information Sharing Protocols (ISPs) or other agreements must be used when sharing information between external organisations, partner organisations, and external providers. ISPs provide a framework for the secure and confidential obtaining, holding, recording, storing and sharing of information. Advice must be sought from the information governance department in such circumstances.

Personal data may need to be shared externally on a one-off basis in the event of an emergency, where an ISP or equivalent sharing document does not exist. The sharing of such information must be formally documented with a clear, justifiable purpose, and processed securely.

5.7 Information Assets

5.7.1 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, and provides the mechanism through which organisations commit to them.

5.7.2 Asset Registers

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 within National Systems. NHS Wales organisations will also have local information asset registers. Staff must follow their organisational procedures and guidance to ensure information asset registers are regularly updated.

5.8 Data Quality

NHS Wales organisations process 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 organisation's efforts to deliver its objectives and for this reason, the NHS in Wales 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. NHS Wales organisations will implement procedures where necessary to support staff in producing high quality data and information.

6. Training and Awareness

Information governance is everyone's responsibility. Training is mandatory for NHS 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 their local information governance department.

7. Monitoring and compliance

NHS Wales 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 practices in work may come under scrutiny. NHS Wales organisations 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.

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

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

In order for the NHS Wales organisations 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.

8. 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; or
- Changing methodology.

9. 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.

Annex: Policy Development - Version Control

Revision History

Date	Version	Author	Revision Summary
26/06/2018	V1	Andrew Fletcher on behalf of the IGMAG Policy Sub Group	
1/12/2020	V d 1.1	Andrew Fletcher on behalf of the IGMAG Policy Sub Group	Draft incorporating comments
14/01/2021	2	Andrew Fletcher (Chair of the IGMAG policy sub group)	Final Policy

Reviewers

This document requires the following reviews:

Date	Version	Name	Position
1/12/2020	1.1	IGMAG Policy sub group	Sub group of the Information Governance Management and Advisory Group
4/01/2021	1.1	Information Governance Management and Advisory Group	All Wales Information Governance Leads
4/01/2021	1.1	Welsh Partnership Forum	All Wales workforce leads and trade unions
7/01/2021	1.1	Equality Impact Assessment	NWIS Equality Impact Assessment Group
14/01/2021	1.1	Information Governance Management and Advisory Group	All Wales Information Governance Leads
14/01/2021	1.1	Wales Information Governance Board	Advisory Board to the Minister for Health and Social Care (Welsh Government)

Approvers

This document requires the following approvals:

Date	Version	Name	Position
4/01/2020	2	Information Governance Management and Advisory Group	All Wales Information Governance Leads
14/01/2021	2	Wales Information Governance Board	Advisory Board to the Minister for Health and Social Care (Welsh Government)