CYMORTH LLYWODRAETHU GWYBODAETH AR GYFER GOFAL SYLFAENOL

INFORMATION GOVERNANCE SUPPORT FOR PRIMARY CARE

NHS Wales
Information Governance Policy for Primary Care Service Providers

Author: IG Support for Primary Care, DHCW
Approved by: Darren Lloyd,
Associate Director of Information Governance & Patient Safety, DHCW
Version: Final V2.0
Date: April 2022
Review date: April 2024

Ty Glan-yr-Afan
21 Heal Ddwyreiniol Y Bont-Faen, Caerdydd CF11 9AD
21 Cowbridge Road East, Cardiff CF11 9AD
Ffon/Tel: 02920 500500
www.cymru.nhs.uk/gwybodeg
www.wales.nhs.uk/informatics

Document History

Revision History

Date	Version	Author	Revision Summary
24/11/2020	D0.1	Francesca Harries	Initial draft developed supplementary to the All Wales Information Governance Policy V1
30/11/2020	D0.2	Jeannette Short	Review of initial draft
30/11/2020	D0.3	Francesca Harries	Further updates
01/12/2020	D0.4	Francesca Harries	Updates following review by Darren Lloyd
02/12/2020	D0.5	Francesca Harries	Updates in line with All Wales Information Governance Policy V1.1
07/12/2020	V1.0	Francesca Harries	
13/09/2021	D1.1	Sarah Muirhead	'NWIS' updated to 'DHCW'
14/03/2022	D1.2	Jeannette Short	Review and Updates
25/03/2022	D1.3	Francesca Harries	Updates following review by Darren Lloyd
11/04/2022	V2.0	Francesca Harries	

Reviewers

This document requires the following reviews:

Date	Version	Name	Position
01/12/2020	D0.3	Darren Lloyd	Head of Information Governance, DHCW
04/12/2020	D0.5	Darren Lloyd	Head of Information Governance, DHCW
14/03/2022	D1.2	Jeannette Short	Primary Care Support and IG Assurance Manager, DHCW
25/03/2022	D1.2	Darren Lloyd	Associate Director of Information Governance & Patient Safety, DHCW

Authorisation

Signing of this document indicates acceptance of its contents.

Author's Name:	Francesca Harries
Role:	Information Governance Assurance Officer
Signature:	11/04/2022 X Francesca Harries Francesca Harries Information Governance Assurance Officer Signed by: Francesca Harries (Fr215649)

Approver's Name:	Darren Lloyd
Role:	Associate Director of Information Governance & Patient Safety

Signature:	11/04/2022 X  Darren Lloyd Associate Director of Information Governan... Signed by: Francesca Harries (Fr215649)

Contents

1. Introduction

This document is supplementary to the All Wales Information Governance Policy issued under the All Wales Information Governance Policy Framework and is maintained by Digital Health and Care Wales (DHCW) on behalf of all NHS Wales organisations.

2. Purpose

The aim of this Policy is to provide all staff of NHS Wales Primary Care Service Providers 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 all staff of Primary Care Service Providers.

The term 'staff' includes all health professionals, partners, employees, locums, students, trainees, secondees, volunteers, contracted third parties and any persons undertaking duties on behalf of the Primary Care Service Provider.

For the purpose of this policy 'Primary Care Service Providers', referred to in this policy as 'the Organisation' will include General Medical Practices, Pharmacies, Dentists and Optometrists commissioned to provide primary care services on behalf of NHS Wales.

This policy applies to all forms of information processed by the Primary Care Service Provider; 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 Senior Responsible Person within the Organisation is responsible for ensuring the highest level of organisational commitment to this policy and the availability of resources to support its implementation and any associated legal requirements. Specific responsibilities may be delegated to the representative Data Protection Officer and other individuals who have responsibility for information governance within the organisation. See Appendix A for Glossary of Terms.

The Organisation must have the following key roles in place:

- **Caldicott Guardian:** A senior person with delegated responsibility 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).

Where necessary, the Organisation will have a designated **Senior Information Risk Owner (SIRO)** with delegated responsibility for an organisation's information risk policy. The SIRO is accountable and responsible for information risk across the organisation.

In addition, the Senior Responsible Person must 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. Breaches of the policy must be reported via local incident reporting processes and dealt with in line with the Organisation's Disciplinary Policy where appropriate.

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.

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 on 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, the Organisation will 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/information. 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. The Organisation 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 the Organisation 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

The Organisation 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 the Organisation are working to the necessary standards and are complying with data protection legislation. In order to identify information risks a DPIA must be completed. The Senior Responsible Person/Information Governance Lead will provide the required guidance and template.

5.1.6. Incident Management and Breach Reporting

The Organisation 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

The Organisation 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[1].

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

[1] At the time of writing the Welsh Information Governance Toolkit is available for General Medical Practices to complete. It is intended that this will be expanded to include all Primary Care Service Providers.

5.1.8. Information Asset Management

Information assets will be catalogued and managed by the Organisation 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

The Organisation 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 NHS Wales Information Security Policy for Primary Care Service Providers for further details.

5.3. Records Management

The Organisation 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 the Organisation 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.

Organisations will work in compliance with NHS Wales Records Management Code of Practice for Health and Social Care 2022.

5.4. Access to Information

The Organisation is, 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 Senior Responsible Person/Information Governance Lead.

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.

The Organisation 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 Organisation's Senior Responsible Person/Information Governance Lead 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 Organisation's Senior Responsible Person/Information Governance Lead 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 Welsh 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 Digital Health and Care Wales and sets out how shared electronic health and care records are held. The Organisation will also have a local information asset register. Staff must follow their organisational procedures and guidance to ensure the information asset register is regularly updated.

5.8. Data Quality

The Organisation processes large amounts of data and information as part of its 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 and the Organisation are committed to ensuring that the data and information they hold and process 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 Organisation 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 all staff providing NHS services and must be completed at commencement of employment and at least every two years subsequently.

Staff who need support in understanding the legal, professional and ethical obligations that apply to them should contact their Senior Responsible Person/Information Governance Lead as appropriate.

7. Monitoring and Compliance

NHS Wales and the Organisation trusts their workforce; however, they reserve 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. NHS Wales and the Organisation respect the privacy of their staff and do not want to interfere in their personal lives however, monitoring of work processes is a legitimate business interest.

Staff should be reassured that NHS Wales and the Organisation take a considered approach to monitoring; however, they reserve 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 appropriate Counter Fraud Team.

In order for the Organisation 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 re-occurring.

8. Review

This policy will be reviewed one year after implementation and every two years thereafter 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.

Appendix A – Glossary of Terms

Term	Definition
Primary Care Service providers	General Medical Practices, Pharmacies, Dental Practices and Optometrists
Senior Responsible Person	**General Medical Practice –** Senior Partner, Caldicott Guardian, Data Protection Officer, Senior Information Risks Officer, Information Governance Lead, Practice Manager **Pharmacies –** Pharmacy Owner, Superintendent **Dental Practice** – Senior Partner, etc **Optometrists** – Senior Partner, etc
Staff	This is not an exhaustive list: all health professionals, partners, employees, locums, students, trainees, secondees, volunteers, contracted third parties and any persons undertaking duties on behalf of the Primary Care Service provider.

Annex 1: Equality Impact Assessment

Note: This EQIA has been taken from the original All Wales Information Governance Policy

Equality Impact Assessment (EQIA) Form		
Ref no: POL/IGMAG/Internet Use/v1		
Name of the policy, service, scheme or project:	Service Area	
NHS Wales Email Use Policy	Information Governance	
Preparation		
Aims and Brief Description	The policy is the product of the review of the All Wales Information Governance Policy. The policy will replace all local policies in this area.	
Which Director is responsible for this policy/service/scheme etc	All Wales policy developed in conjunction with Health Boards/Trusts	
Who is involved in undertaking the EQIA	Andrew Fletcher and EQIA Group	
Have you consulted with stakeholders in the development of this policy?	Yes. A sub group has developed this policy with a membership consisting of information governance leads and an OSSMB representative. IM&T leads and the Wales Partnership Forum have been consulted. The NHS Wales Information Governance Management and Advisory Group have approved the text of this Policy. The policy will be approved by the Wales Information Governance Board.	
Does the policy assist services or staff in meeting their most basic needs such as; Improved Health, fair recruitment etc	Yes. The policy will provide consistency throughout NHS Wales in having a single policy. This will ensure that staff who work across boundaries have a consistent standard to work to, hence strengthening the governance framework. A key driver during the process was the need to recognise that organisations needed to trust their staff.	
Who and how many (if known) may be affected by the policy?	All staff within General Medical Practices, Pharmacies, Dentists and Optometrists who provide primary care services on behalf of NHS Wales	
What guidance have you used in the development of this service, policy etc?	The policy is based on good practice and legal obligations as set out by the Information Commissioners Office and in the legislation. The policy has also been constructed from existing agreed principles and the corporate knowledge of its stakeholders.	

Equality Duties

The Policy/service/project or scheme aims to meet the specific duties set out in equality legislation.	Protected Characteristics										
	Race	Sex/Gender	Disability	Sexual orientation	Religion and Belief	Age	Gender reassignment	Pregnancy and Maternity	Marriage & civil Partnerships	Welsh Language	Carers
To eliminate discrimination and harassment	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Promote equality of opportunity	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Promote good relations and positive attitudes	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Encourage participation in public life	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
In relation to disability only, should the policy / service / project or scheme take account of difference, even if involves treating some individuals more favourably?							✓				

Key	
✓	Yes
x	No
-	Neutral

Human Rights Based Approach – Issues of Dignity & Respect

The Human Rights Act contains 15 rights, all of which NHS organisations have a duty. The 7 rights that are relevant to healthcare are listed below.

Consider is the policy/service/project or scheme relevant to:	Yes	No	N/A
Article 2: The Right to Life	X		
Article 3: the right not to be tortured or treated in a inhumane or degrading way	X		
Article 5: The right to liberty	X		
Article 6: the right to a fair trial	X		
Article 8: the right to respect for private and family life	X		
Article 9: Freedom of thought, conscience and religion	X		
Article 14: prohibition of discrimination	X		

Measuring the Impact

What operational impact does this **policy, service, scheme or project**, have with regard to the Protected Characteristics. Please cross reference with equality duties	
	Impact – operational & financial
Race	This is an all Wales high level framework approach which aims to achieve the values under the policy, it is the protection of everybody's information and gives clear guidelines. The policy details how the organisation protects someone's data and security without prohibiting access to services and providing adequate access to data to meet individual needs and the appropriate sharing of data.
Sex/gender	
Disability	
Sexual orientation	
Religion belief and non belief	
Age	
Gender reassignment	
Pregnancy and maternity	
Marriage and civil partnership	
Other areas	
Welsh language	
Carers	

Outcome report

Equality Impact Assessment: Recommendations

Please list below any recommendations for action that you plan to take as a result of this impact assessment

Recommendation		**Action Required**	**Lead Officer**	**Time-scale**	**Resource implications**	**Comments**
1	Communication of the changes	Make sure staff aware of the changes	AF	ASAP	Time	
2	Updated EQIA statement	Inclusion of reference to protected characteristics	AF	ASAP	Time	

Recommendation	**Likelihood**	**Impact**	**Risk Grading**
1	2	2	4
2	2	2	4

Risk Assessment based on above recommendations

Reputation and compromise position			Outcome
It is providing security and reassurance to stakeholders that the information we hold is used appropriately and any breach may lead to fines and reputational damage.			To ensure that information is used and protected appropriately and a framework in place to ensure that happens.
Training and dissemination of policy			
More training and dissemination on this policy			
Is the policy etc lawful?	**Yes** ☒	**No** ☐	**Review date**
Does the EQIA group support the policy be adopted?	**Yes** ☒	**No** ☐	**3 years**
Signed on behalf of NWIS Equal Impact Assessment Group	S Brooks	Lead Officer	
Date:	8 May 2018	Date: 8 May 2018	

	1	2	3	4	5
	Negligible	**Minor**	**Moderate**	**Major**	**Catastrophic**
Statutory duty	No or minimal impact or breach of guidance / statutory duty Potential for public concern Informal complaint Risk of claim remote	Breech of statutory legislation Formal complaint Local media coverage – short term reduction in public confidence Failure to meet internal standards Claims less than £10,000 Elements of public expectations not being met	Single breech in statutory duty Challenging external recommendations Local media interest Claims between £10,000 and £100,000 Formal complaint expected Impacts on small number of the population	Multiple breaches in statutory duty Legal action certain between £100,000 and £1million Multiple complaints expected National media interest	Multiple breaches in statutory duty Legal action certain amounting to over £1million National media interest Zero compliance with legislation Impacts on large percentage of the population Gross failure to meet national standards

Risk Grading Descriptors

LIKELIHOOD DESCRIPTION

5 Almost Certain	Likely to occur, on many occasions
4 Likely	Will probably occur, but is not a persistent issue
3 Possible	May occur occasionally
2 Unlikely	Not expected it to happen, but may do
1 Rare	Can't believe that this will ever happen