CYMORTH LLYWODRAETHU GWYBODAETH AR GYFER GOFAL SYLFAENOL
INFORMATION GOVERNANCE SUPPORT FOR PRIMARY CARE

NHS Wales
Information Security 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
25/11/2020	D0.1	Francesca Harries	Initial draft developed supplementary to the All Wales Information Security Policy V1
30/11/2020	D0.2	Jeannette Short	Review of initial draft
01/12/2020	D0.3	Francesca Harries	Updates following review by Darren Lloyd
02/12/2020	D0.4	Francesca Harries	Updates in line with All Wales Information Security Policy V1.1
07/12/2020	V1.0	Francesca Harries	
13/09/2021	D1.1	Sarah Muirhead	'NWIS' updated to 'DHCW'
15/03/2022	D1.2	Jeannette Short	Review and Updates
11/04/2022	V2.0	Francesca Harries	

Reviewers

This document requires the following reviews:

Date	Version	Name	Position
01/12/2020	D0.2	Darren Lloyd	Head of Information Governance, DHCW
04/12/2020	D0.4	Darren Lloyd	Head of Information Governance, DHCW
15/03/2022	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 Security 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 purpose of the Policy is to set out the responsibilities of Primary Care Service Providers in relation to the security of the information they process. Processing broadly means collecting, using, disclosing, sharing, retaining or disposing of personal data or information.

These responsibilities include, but are not restricted to, ensuring that:

- All systems are properly assessed for security;
- The confidentiality, integrity, availability and suitability of information is maintained;
- All individuals as referenced within the scope of this policy are aware of their obligations.

This policy must be read in conjunction with relevant organisational procedures. Information must only be shared where there is a defined purpose to do so. Nothing in this policy will restrict any organisation from sharing or disclosing any information provided they have an appropriate legal basis for doing so. Any information sharing which involves Personal Data or business sensitive information must be transferred securely.

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.

It applies to all forms of information processed by Primary Care Service Providers; 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 "confidential information" refers to all personal data as defined by the data protection legislation, and information subject to the Duty of Confidence such as confidential business information and information relating to living or deceased individuals.

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.

In addition, they 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. User Access Controls

Access to information will be controlled on the basis of business requirements. System Managers will ensure that appropriate security controls and data validation processes, including audit trails, will be designed into application systems that store any information, especially personal data. The workforce has a responsibility to access only the information which they need in order to carry out their duties. Examples of inappropriate access include but are not restricted to:

- Accessing your own health record;
- Accessing any record of colleagues, family, friends, neighbours etc., even if you have their consent, except where this forms part of your legitimate duties;
- Accessing the record of any individual without a legitimate business requirement.

5.1.1. Physical Access Controls

The Organisation is responsible for determining the security measures required based on local risk assessment. All staff are responsible for following these security measures and to ensure they maintain confidentiality and security at all times regardless of the setting (e.g. when working from home or working in the community).

Maintaining confidentiality in clinical areas can be challenging and the need to preserve confidentiality must be carefully balanced with the appropriate care, treatment and safety of the patient.

Where physical security measures exist, it must be ensured that they are employed at all times (e.g. filing cabinets must be locked, security doors and windows must be closed securely, blinds to secure areas closed). Access cards, PIN codes, keycodes, etc. must be kept secure and regularly changed as required.

The workforce must ensure a clear desk and clear screen when away from their work area ensuring that confidential information, in any format, is secure and not visible to anyone who is not authorised to access it.

All central file servers and central network equipment will be located in secure areas with access restricted to designated staff as required by their job function.

5.1.2. Passwords

The workforce are responsible for the security of their own passwords which must be developed in line with NHS guidance ensuring they are regularly changed. Passwords must not be disclosed to anyone, and users must not allow anyone to access any work using their log-in details.

In the absence of evidence to the contrary, any inappropriate access to a system will be deemed as the action of the user. If a user believes that any of their passwords have been compromised, they must change them immediately.

NADEX passwords no longer expire therefore require a strong password to be set. However, if the workforce think anyone else might know their password it should be changed immediately.

5.1.3. Remote Working

NHS Wales and the Organisation recognise that there is a need for a flexible approach to where, when and how our workforce undertake their duties or roles. Handling confidential information outside of your normal working environment brings risks that must be managed.

Examples of remote working include, but are not restricted to:

- Working from home;
- Working whilst travelling on public/shared transport;
- Working from public venues (e.g. coffee shops, hotels etc.);
- Working at other organisations (e.g. NHS, local authority or academic establishments etc.);
- Working abroad.

As a control measure to mitigate risks involved in remote working, no member of the workforce will work remotely unless they have been authorised to do so. Remote working must not be authorised for anyone who is not up to date with mandatory training in information governance.

5.1.4. Staff Leavers and Movers

Managers will be responsible for ensuring that local leaving procedures are followed when any member of the workforce leaves or changes roles to ensure that user accounts are revoked / amended as required and any equipment and /or files are returned. Confidential information, including access to confidential information, must not be transferred to a new role unless authorised by the Organisation's Senior Responsible Person. The relevant checklist for leavers and movers must be completed in all cases.

5.1.5. Third Party Access to Systems

Any third-party access to systems must have prior authorisation, and where personal data is involved, authorisation must also be sought from the Organisation's Senior Responsible Person.

5.2. Storage of Information

All information stored on behalf of, or within the Organisation is the responsibility of that organisation. All software, information and programmes developed for the Organisation by the workforce during the course of their employment will remain the property of the Organisation.

Users are not permitted to use their personal devices or store confidential information on a personal device for the purpose of carrying out organisational business unless they have been explicitly authorised to do so in line with a documented organisational process (e.g. a Data Protection Impact Assessment).

All systems supported by the Organisation will be backed up as part of their backup regime. Unless specifically told otherwise this will not include information held on local hard drives, portable devices or removable media. Users must not store information on local drives (usually referred to as the C Drive). Exceptions to this may be for legitimate work purpose to a device that is encrypted.

5.3. Portable Devices and Removable Media

Whilst it is recognised that both portable devices and removable media are widely used throughout the Organisation, unless they are used appropriately, they pose a security risk to the NHS Wales and the Organisation.

Portable devices include, but are not limited to, laptops, tablets, Dictaphones®, mobile phones, cameras and some forms of medical devices.

All portable devices must utilise appropriate technical measures to ensure the security of all data.

Users must not attach any personal (i.e. privately owned) portable devices to any NHS organisational network without prior authorisation.

Removable media includes, but is not limited to, USB 'sticks' (memory sticks), memory cards, external hard drives, CDs / DVDs and tapes. Appropriate controls must be in place to ensure any information copied to removable media is encrypted.

5.4. Secure Disposal

For the purposes of this policy, confidential waste is any paper, electronic or other waste of any other format which contains personal data or business sensitive information.

5.4.1. Paper

All confidential paper waste must be stored securely and disposed of in a timely manner in the designated confidential waste bins or bags; or shredded on site as appropriate. This must be carried out in line with local retention and destruction arrangements.

5.4.2. Electronic

Any IT equipment or other electronic waste must be disposed of securely in accordance with local disposal arrangements. For further information, please contact your Organisation's Senior Responsible Person/Information Governance Lead.

5.4.3. Other Items

Any other items containing confidential information which cannot be classed as paper or electronic records e.g. film x-rays, orthodontic casts, carbon fax/printer rolls etc, must be destroyed under special conditions. For further information, please contact the Organisation's Senior Responsible Person/Information Governance Lead.

5.5. Transporting and relocation of information

5.5.1. Transporting Information

When information, regardless of the format, is to be physically transported from one location to another location, local procedures must be formulated and followed by staff to ensure the security of that information.

5.5.2. Relocating Information

When information, regardless of the format, is to be physically relocated to another location, local procedures must be formulated and followed by staff to ensure no information is left at the original location.

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 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 Security 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 Security 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	The revised policy is high level and focused on the security of information and the operational service management boards need to consider the detail around cyber security and procedures. It is about protecting information around the protected characteristics so it is used appropriately.
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	Updated statement in policy	Inclusion of reference to protected characteristics rather than homophobic, bi-phobic, racist etc so inclusive of all in the statement	AF	ASAP	Time	
2	Communication of the changes	Make sure staff aware of the changes	AF	ASAP	Time	
3	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
3	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