NHS Wales
Information Security 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 purpose of the Policy is to set out the responsibilities of NHS Wales organisations 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 the workforce of all NHS Wales organisations including staff, students, trainees, secondees, volunteers, contracted third parties and any persons undertaking duties on behalf of NHS Wales.

For the purpose of this policy 'NHS Wales Organisations' will include all NHS Wales organisations including 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 "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 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 Data Protection Officer, Senior Information Risk Owner and the Caldicott Guardian or an Executive Director as appropriate.

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. 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.

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 this policy must be reported via local incident reporting processes.

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 to know 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

All organisations are 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.

5.1.3 Remote Working

NHS Wales recognises 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 relevant heads of service or their delegate. 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 from the IT Department, and where personal data is involved, authorisation must also be sought from the Information Governance Department.

5.2 Storage of Information

All information stored on behalf of, or within NHS Wales organisations is the property of that organisation. All software, information and programmes developed for NHS Wales organisations 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 NHS Wales 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 NHS Wales organisations 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 NHS Wales, unless they are used appropriately they pose a security risk to 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, including those used in medical devices. Appropriate controls must be in place to ensure any information copied to removable media is secure.

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 IT Department.

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 your information governance team.

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 format, is to be physically relocated, 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 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.

Staff should be reassured that NHS Wales organisations take 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 team.

In order for NHS 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 practices, 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 (Chair of the IGMAG policy sub group)	Original
01/12/2020	V1.1	Andrew Fletcher (Chair 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)