GIG CYMRU NHS WALES | Bwrdd Iechyd Prifysgol Hywel Dda University Health Board

Name of Sub-Committee:	**Information Governance Sub-Committee (IGSC)**
Chair of Sub-Committee:	**Huw Thomas, Director of Finance**
Reporting Period:	**13th April 2021**

Key Decisions and Matters Considered by the Sub-Committee:

Clinical Coding Update

The IGSC noted the Hywel Dda University Health Board (HDdUHB) clinical coding performance for January 2021 was 64.3% which is significantly below the Welsh average of 87.5% and requested that an urgent recovery plan be developed. This performance indicates that HDdUHB is ranked 8th in NHS Wales. The IGSC acknowledged that this is not acceptable, and requested that further avenues are explored to improve the recovery plan. The anticipated year end performance will be 88%. It was noted that prioritisation of workload has changed during COVID-19. Staff have been balancing prioritisation, including end of month completeness target, coding of deaths to support the mortality review and other specific uses of such data and finally the COVID-19 patients, including those suspected of having COVID-19; this is done to support the data modelling requirements as part of the COVID-19 response. To date, approximately 70% of positive COVID-19 patient admissions have been coded with approximately 380 admissions outstanding.

The IGSC agreed that the coding service should concentrate upon the backlog cases for 2019/2020 onwards, which indicates that there are 24,079 cases requiring coding by end of June 2021. The IGSC agreed to monitor the situation.

Enterprise Master Patient Index (EMPI) Implementation Plan

The IGSC was presented with an update on the EMPI Implementation Plan. Members noted introduction of the EMPI had gone live and is operational within HDdUHB. The IGSC expressed gratitude to the Information Services Team for their work in implementing the EMPI into HDdUHB. The IGSC requested that a data quality assessment be undertaken after 3 months of introduction, to provide assurance that the benefits identified in previous papers to IGSC are being realised.

Digital Services/IG Document Review

The IGSC noted that the policies detailed below have been updated and are out for global consultation, and will be presented to the June 2021 meeting for approval. The documents out for consultation are:

- The Data Protection Impact Assessment Procedure.
- The Information Classification Policy.
- The Secure Transfer of Personal Information Policy.
- The Corporate Subject Access Request Procedure.
- The Information Rights Procedure.

Information Governance Toolkit – Compliance Update with Improvement Plan

The IGSC noted that an extraordinary meeting had been held to discuss the outputs of the toolkit prior to its submission on 31st March 2021. The IGSC noted that there are four specific areas where the Information Governance Team assessed HDdUHB as not attaining the target level 1.

Cyber Security Awareness Training Update
The IGSC noted the contents of the paper, and that Digital Health and Care Wales (DHCW) have confirmed that licences for the current training product will not be renewed. They are considering the procurement of a new training package and will be going out to tender imminently. Several options were presented to members, and it was agreed that due to the importance of Cyber Security, HDdUHB should consider whether there is a product that would be adequate for its needs. The IGSC requested further updates to be provided to the Sub-Committee.

Information Asset Registers
The IGSC was asked to approve three Information Asset Registers (IARs), following assurance by the Information Asset Owners Group (IAOG) meeting and the services' lead Directors:

- Dental Services (Jill Paterson).
- Primary Care GMS (Jill Paterson).
- Service Improvement (Jill Paterson).

Review of the Privacy Notice
The IGSC were presented with an updated Privacy Notice for HDdUHB, which will be made available to patients via the internet site. Members also noted that the Information Goverance Team are also ensuring that the document complies with digital accessibility requirements.

Leavers and Disabled Accounts and Email Deletion
The IGSC were presented with a detailed report on the issues associated with the migration of mailboxes as a result of Microsoft Office 365 (O365). The lack of a defined national Starters, Leavers and Movers Policy currently indicates that the HDdUHB is retaining information in O365 of employees who have left the organisation. Not only is this potentially against the principles of General Data Protection Regulation (GDPR), it is incurring costs to HDdUHB in respect of Microsoft license charges. The IGSC agreed the following:

- The decommissioning of our on-premise e-mail environment once the final room mailboxes have been migrated with a saving of £30,000 per annum.
- The removal of O365 licences of disabled accounts and the deletion of the associated user account, which will release 1,144 user accounts with a possible cost avoidance of £19,078.

All Wales Policies
The Information Governance Sub-Committee (IGSC) approved the following All Wales Policies:

- All Wales Information Governance Policy.
- All Wales Information Security Policy.
- All Wales Internet Use Policy.

Health Records Standard Operating Procedure
The IGSC received a report on the update in terms of the progress made against a specific recommendation contained within the Welsh Audit Office report for the clinical coding service, with a specific reference to the creation of "polly pockets" within the health record. The recommendation identified was that HDdUHB are required to "remove the use of temporary records, including polly-pockets and ensure files are merged into the master patient record". Clearly, totally eradicating the use of temporary records is not a sustainable option, however ceasing the use of polly pockets and ensuring records are merged accordingly can be implemented.

Over the past 6 - 12 months, the Health Records Service has been reviewing and updating its standard operating procedures (SOPs) for distribution and circulation to relevant staff groups. During the ongoing review, it was essential to identify any tasks or duties that did not have an allocated SOP, which could result in inappropriate use and management of the patient record. It was recognised that there was no SOP available for staff to follow and provide appropriate guidance when there is a delay in the availability of the patient's medical record.

The IGSC expressed gratitude to the reporting officer and approved the newly revised procedure/process on the creation of a temporary record.

IG Activity Report
The IGSC received the IG Activity Report, noting the following:

- **Enquiries on Data Protection Framework –** the number of enquiries (**106**) received during **Quarter (Q)4** indicated a substantial increase in figure to the previous quarter (**67** enquiries), and a large increase compared to **Q4** of previous year 2019/20 (**83**).

- **Information Sharing –** the number of information sharing requests (**26**) received during **Q4** increased from the previous quarter (**19** requests), demonstrating a significant increase compared to **Q4** of the previous year 2019/20 (**11**).

- **Personal Data Breaches –** the number of personal data breaches reported to IG during **Q4** equated to **28,** which is a decrease to **Q3** (**40**).
  It is important to note that of these **28** breaches, **15** were Near Misses.
  The majority of the incidents fall within the following categories:
    - Lost or stolen paperwork (**2**);
    - Disclosed in error (**10**); and
    - Unauthorised Access/Disclosure (**3**)
    - Technical security failing (including hacking) (**1**).

  Additionally, there were **7** incidents that were not owned by HDdUHB, 4 of which were owned by other Health Boards and 1 by a managed GP practice.

- **Data Subject Requests** - The number of Health Subject Access Requests (SAR) received totaled **791** during **Q4**, which was an increase in comparison to the previous quarter (**638**) and of **Q4** of the previous year (**744**). There were **5** Corporate Subject Access Requests (SAR) received in **Q4**, similar compared with **Q3** (**8**).

- **Information Asset Registers** – **1** Information Asset Register enquiry was processed during **Q4** where internal meetings to map the workflows within services were undertaken.

- **Requests for Information (Third Party) –** there has been a further increase in requests from third parties during **Q4** (**105**) since the earlier quarter (**62** requests) in addition there continues to be a large increase compared to **Q4** of the previous year 2020/21 (**83**).

  The number of Schedule 2(1)(2) Police requests in **Q4** 2020/21 (**96**) has risen since the last quarter (**60**) and continues to be a significant increase, compared to 2019 **Q4** 2019/20 (**70**).

- **Freedom of Information** – the number of Freedom of Information requests received during **Q4** (**135**) was similar to the previous quarter Q3 (**136**). The figure has increased compared with the same period during **Q4** of previous year 2019/20 (**120**).

- **Training Compliance** – The IG training compliance has increased slightly with **Q4** recording **78.79%**, which is a marginal increase to the previous quarter (**78.61%**). A 2.57% increase compared to the end of **Q4** of the previous year 2019/2020 (**76.22%**). The booking onto the Electronic Staff Record (ESR) Weekly IG virtual training (Microsoft Teams) was rolled out during late February 2021 in order to encourage staff to complete their IG ESR compliance.

  It is noted that students maintained **100%** compliance during Q4.
  Medical and Dental services decreased slightly to **39.29%.**

  Estates and Ancillary compliance has increased slightly during **Q4** 2020/21 (**65.00%**) compared to the previous quarter (**61.77%**). This remains a substantial decrease compared to March to October 2019 where the service plateaued around 90 – 92.49%%. Nonetheless there has been an increase compared with **Q4** of previous year 2019/20 (**54.10%**).

  The IG Compliance classroom training via Microsoft Teams is now available to book via ESR. In addition, the new virtual training video is under development providing staff with an option as to how they wish to complete their IG compliance.

- National Intelligent Integrated Auditing Solution **(NIIAS) Monitoring – Alerts Received** During **Q4, 29** Own Access Notifications were received, in comparison to the previous quarter (**43**); the decrease has been welcomed. Having considered the individual alerts it was identified that **3** of the triggers have been confirmed as legitimate accesses, and these accesses have been verified as legitimate by the Line Manager of the Service. Of the remaining **26** triggers, **9** Staff have attended the Virtual Training, **3** staff had more than one NIIAS trigger, **7** have booked onto future training sessions and **7** staff members notifications remain outstanding.

  During **Q4, 16** Potential Family Access Notifications were recorded. **1** of these was found not to be a relation and **2** were legitimate accesses related to their work. **4** have been identified as requiring training, **3** of which have attended training; whilst **8** enquiries remain outstanding. This is a welcomed decrease in notifications requiring investigation in comparison with the previous quarter (**43**), as well as compared to **Q3** of the previous year 2019/20 (**30**).

  There were **6,981** Staff Accessing Staff Files Notifications during **Q4**. compared with last quarter (**6,940**). It is noted that these figures are lower compared with the same quarter as last year **Q4** 2019/20 (**7,140**).

  There were **2** Choose Pharmacy alerts during **Q4,** compared with 1 last quarter, and Q4 2019/20 (**0**).

Information Governance are awaiting an update as to when the functionality of the report builder will become available in order to further monitor staff accesses.

Caldicott Guardian Register
The IGSC received the latest Caldicott Guardian Register and noted the processes that the Information Governance Team carries out in support of the Caldicott Guardian's function. It was agreed that officers will undertake a review of the current register to ascertain whether it is still current, and documents previously approved are removed.

Digital Communications
A report was presented to the IGSC to provide an update on the work associated with the audit recommendation relating to communication as highlighted in the IM&T Control & Risk Assessment (HDdUHB-2021-20_002). The IGSC noted the progress to date and agreed that further updates be provided at subsequent meetings.

Security of Network and Information Systems (NIS Directive) – Welsh Government Guidance
The IGSC were presented with a comprehensive update on the NIS Directive and the impact upon the HDdUHB. The purpose of the NIS Directive is to ensure providers of essential digital services and infrastructure have adequate data and cyber security measures in place. This directive is enshrined in legislation and was adopted by the European Parliament in July 2016 and formally adopted by the UK Government in May 2018. The UK Government legislation was amended in 2019 to reflect the UK leaving the EU.

The NIS Directive aims to ensure security across sectors which are vital for society and covers several industries including Energy, Transport, Water Companies, Financial Markets and Healthcare.

Organisations of these sectors are identified as "Operators of Essential Services" (OES) and they must ensure they take appropriate security measures to protect their infrastructure and notify any security incidents that occur to the relevant competent authority. The relevant competent authority for NHS Wales is the Welsh Government.

Due to the importance of the NIS Directive, the IGSC approved several next steps, namely:

- Create a NIS Directive project group reporting to the IGSC chaired by the Senior Information Risk Owner (SIRO) or Deputy SIRO to reflect the importance of compliance with this legislation.
- Ensure the work required to undertake the assessment against the Cyber Assessment Framework (CAF) is the priority for our Cyber Security Specialist starting on 19th April 2021.
- Engage with our third-party provider who has been contracted to provide a Cyber response plan and incident response service.
- Ensure incident management process is in place in order for HDdUHB to comply with the reporting requirements of the NIS Directive.
- Identification of critical systems which are covered by the NIS Directive.
- Undertake CAF assessment against each of the critical systems.

In view of the work required, the Digital Team have been in contact with a number of external consultancies to provide a gap analysis, and implementation plan to ensure that HDdUHB is applying the NIS Directive within the 12-month timescale outlined by Welsh Government. The IGSC also agreed that the NIS Directive will become a standing agenda item.

Matters Requiring People Planning and Performance Assurance Committee Level Consideration or Approval:

- Updates to the local Privacy Notice.
- The following all Wales policies were approved, and are presented to the Committee for ratification:
    - All Wales Information Governance Policy.
    - All Wales Information Security Policy.
    - All Wales Internet Policy.

Risks / Matters of Concern:

- No matters of concerns or risk were raised.

Planned Sub-Committee Business for the Next Reporting Period:

Future Reporting:

- Information Asset Owners and Information Asset Mapping update.
- Data Quality and Clinical Coding.
- Information Governance Risk Register.
- Information Governance Toolkit.
- IG Training Strategy.
- Clinical Coding Recovery Plan.
- Update on Cyber Security.
- Caldicott Register to be returned to the IGSC meetings.
- Digital / IG policies and procedures.
- Audit of Network Communications Rooms.
- Digital Communications

Date of Next Meeting:

Tuesday, 8th June 2021 at 10:00 a.m.

NHS Wales
Internet Use Policy

Author: Information Governance Management Advisory Group Policy Sub Group
Approved by: Information Governance Management Advisory Group
Approved by: Wales Information Governance Board
Version: 3
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

This policy provides assurance that NHS Wales internet facilities are being used appropriately to assist in delivering services.

The policy also sets out the responsibilities of all users when using the internet. These responsibilities include, but are not restricted to, ensuring that:

- The confidentiality, integrity, availability and suitability of information and NHS computer systems are maintained by ensuring use of internet services is governed appropriately;
- 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.

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.

The policy describes the principles which must be adhered to by all in the use of the internet, the NHS Wales Network (which is defined as a corporate Intranet) and other affiliated sites.

The terms "internet access" or "internet use" encompass any use of any resources of the internet including social media / social networking, browsing, streaming, downloading, uploading, posting, "blogging", "tweeting", chat and email. The NHS Wales Social Media Policy provides information on the appropriate use of social media.

This policy applies to all staff that make use of the NHS network infrastructure and / or NHS equipment to access internet services regardless of the location from which they accessed and the type of equipment that is used including corporate equipment, third party and personal devices.

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 Officer 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 Position Statement

Internet access is provided to staff to assist them in the performance of their duties and the provision of these facilities represents a major commitment on the part of NHS Wales in terms of investment and resources.

The NHS Wales workforce should become competent in using internet services to the level required for their role in order to be more efficient and effective in their day-to-day activities.

NHS Wales will support its workforce in understanding how to safely use internet services and it is important that users understand the legal, professional and ethical obligations that apply to its use. If used correctly, the internet can increase efficiency and safety within patient care.

5.2 Conditions & Restrictions

To avoid inadvertent breaches of this policy, inappropriate content will be blocked by default where possible. Inappropriate material must not be accessed. Exceptions may be authorised for certain staff where access to particular web pages are a requirement of the role. Subject matter considered inappropriate is detailed in appendix A.

Some sites may be blocked by default due to their general impact on network resources and access to these for work purposes can be requested by contacting the Local IT Service Desk.

Regardless of where accessed users must not participate in any online activity or create or transmit or store material that is likely to bring the organisation into disrepute or incur liability on the part of NHS Wales.

Business Sensitive Information or Personal Data (which includes photographs and video recordings) of any patient, member of the public, or member of staff taken on NHS Wales premises must not be uploaded to any form of non NHS approved online storage, media sharing sites, social media, blogs, chat rooms or similar, without both the authorisation of a head of service and the consent of the individual who is the Data Subject of that recording. The NHS Wales Social Media Policy provides information on the appropriate use of social media.

It is each user’s responsibility to ensure that their internet facilities are used appropriately. Managers are reminded that, as an NHS Wales resource, the internet is in many ways similar to the telephone systems and should be managed accordingly.

5.3 Personal Use

NHS Wales organisations allow staff reasonable personal use of internet services providing this is within the bounds of the law and decency and compliance with policy.

Personal use should be incidental and reasonable. As a threshold, NHS Wales defines this as a maximum of thirty minutes in one calendar day and before or after normal working hours, or during agreed break times. These limitations are also necessary due to network demands and therefore local restrictions may apply dependent on the duration of access and the capacity of resources available. In addition to this, users must not stream or download large volumes of data (e.g. streaming audio or video, multimedia content, software packages) as these may have a negative impact on network resources.

Where local organisations have provided patients and staff with access to public Wi-Fi services, employees are encouraged to use these facilities by default on personally-owned devices instead of using NHS equipment. Local agreements will be in place for the use of and availability of these facilities.

Staff who use NHS equipment outside NHS Wales premises (for example – in a home environment) are permitted to connect to the internet. Use of the internet under these circumstances must be through the secure connection provided by the NHS Wales organisation (for example via VPN, Multi Factor Authentication). Use of the equipment for such purposes is still subject to the same conditions as laid out in this policy.

All personal use of the internet is carried out at the user's own risk. The NHS Wales does not accept responsibility or liability for any loss caused by or liability arising from personal use of the internet.

Internet access facilities must not be used to run or support any kind of paid or unpaid personal business venture outside work, whether or not it is conducted in a user's own time or otherwise.

At no time should access to the internet be used by any individual for personal financial gain (E.g. using eBay or any other auction sites).

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.

The NHS Wales workforce should become competent in using internet services to the level required of their role in order to be efficient and effective in their day-to-day activities.

7. Monitoring and compliance

NHS Wales trusts its workforce.

NHS Wales 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.

NHS Wales uses software to automatically and continually record the amount of time spent by staff accessing the internet and the type of websites visited by staff. Attempts to access any prohibited websites which are blocked is also recorded.

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 or when a manager has concerns around employees performance, (e.g. excessive internet usage). 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 IG 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 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.

Appendix A - Inappropriate use

For the avoidance of doubt, inappropriate use includes, but is not limited to:

- Excessive personal use.
- Allowing access to NHS Wales internet services by anyone not authorised to access the services, such as by a friend or family member.
- Communicating or disclosing confidential or sensitive information via the internet without authorisation or without the appropriate security measures being in place.
- Downloading or communicating any information or images which are unlawful, or could be regarded as defamatory, offensive, abusive, obscene, hateful, pornographic, violent, terrorist, indecent, being discriminatory in relation to the protected characteristics,; or using the email system to inflict bullying or harassment on any person.
- Downloading, uploading, transmitting, viewing, publishing, storing or distributing defamatory material or intentionally publishing false information about NHS Wales or its staff, clients or patients.
- Knowingly accessing, or attempting to access internet sites that contain obscene, hateful, pornographic, violent, terrorist, racist or otherwise illegal material. This will include such pages on social media sites.
- Knowingly and without authority view, upload, or download material that may bring NHS Wales into disrepute; or material that could cause offence to others.
- Sending or saving information or images which could be considered defamatory, obscene, hateful, pornographic, violent, terrorist, racist or otherwise illegal material.
- Downloading or installing or distributing unlicensed or illegal software.
- Downloading software without authorisation or changing the configuration of existing software using the internet without the appropriate permissions.
- Breaching copyright or Intellectual Property Rights (IPR).
- ‘Hacking’ into others accounts or unauthorised areas.
- Deliberately attempting to circumvent security systems protecting the integrity of the NHS Wales network.
- Any purpose that denies service to other users (for example, deliberate or reckless overloading of access links or switching equipment).
- Intentionally introducing malicious software such as Viruses, Worms, and Trojans into the NHS Wales network.
- To access sites with the intention of making a personal gain (for example - running a business).
- Access to internet based e-mail providers such as Gmail, Hotmail, Yahoo etc is prohibited for reasons of security with the exception of:

    - Access to email services provided by a recognised professional body or a trade union recognised by the employer;
    - Any UK university hosted e-mail account (accounts ending in .ac.uk);
    - Any email account hosted by a body which the employee contributes to in conjunction with their NHS role, such as a local authority or tertiary organisation.

- Altering any of the system settings on a NHS Wales owned PC or trying to change the access server in an attempt to avoid the restriction imposed by the filtering software. This will be deemed as a breach of this policy and will be dealt with under the All Wales Disciplinary Policy.

Annex 1: Policy Development - Version Control

Revision History

Date	Version	Author	Revision Summary
26/06/2018	2	Andrew Fletcher (Chair of the IGMAG policy sub group)	Original policy as approved.
1/12/2020	2.1	Andrew Fletcher (Chair of the IGMAG policy sub group)	Policy with incorporated comments
14/01/2021	3	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	2.1	IGMAG Policy sub group	Sub group of the Information Governance Management and Advisory Group
4/01/2021	2.1	Information Governance Management and Advisory Group	All Wales Information Governance Leads
4/01/2021	2.1	Welsh Partnership Forum	All Wales workforce leads and trade unions
7/01/2021	2.1	Equality Impact Assessment	NWIS Equality Impact Assessment Group
14/01/2021	2.1	Information Governance Management and Advisory Group	All Wales Information Governance Leads
14/01/2021	2.1	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	3	Information Governance Management and Advisory Group	All Wales Information Governance Leads
14/01/2021	3	Wales Information Governance Board	Advisory Board to the Minister for Health and Social Care (Welsh Government)

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)

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)