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

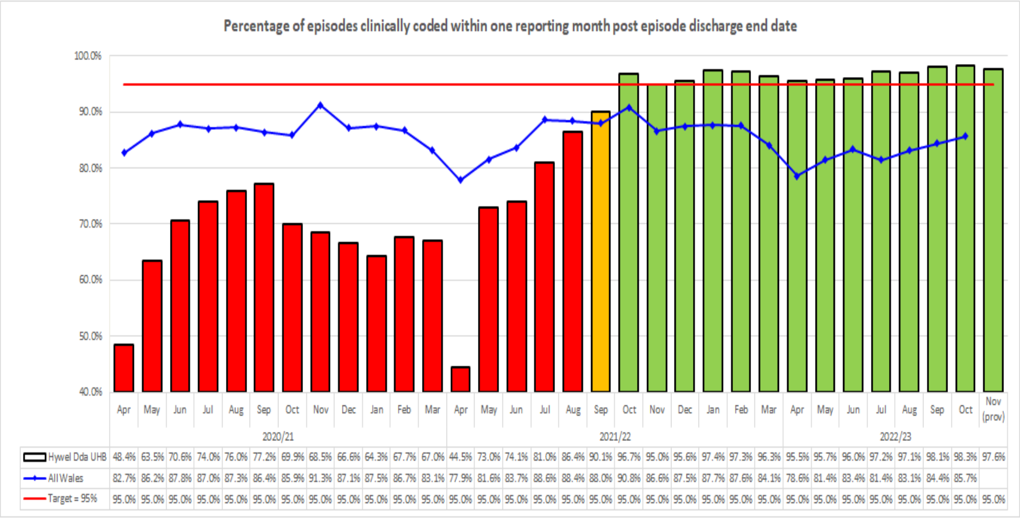
Enw y Grŵp/Is-Bwyllgor: Name of Group:	**Information Governance Sub-Committee (IGSC)**
Cadeirydd y Grŵp/Is-Bwyllgor: Chair of Group:	**Huw Thomas, Director of Finance**
Cyfnod Adrodd: Reporting Period:	**31 January 2023**

Y Penderfyniadau a'r Materion a Ystyriodd y Grŵp/Is-Bwyllgor:
Key Decisions and Matters Considered by the Group:

Policies and Procedures:
The Sub-Committee received the following policy for approval.

- 275 Secure Transfer of Personal Information Policy – approved to be passed to the Committee for approval
- 193 Retention and Destruction of Records Policy – approved to be passed to the Committee for approval
- 174 Reuse of Public sector Information Procedure – approved to be passed to the Committee for approval
- 282 Network Security Policy – approved to be passed to the Committee for approval
- 319 - Disposal of Digital Equipment Policy – approved to be passed to the Committee for approval
- 422 - Consumer Device Policy – approved to be passed to the Committee for approval

Clinical Coding Update
The Sub-Committee received a paper which provided an update on the clinical coding position for the Health Board. Health Board performance has achieved the 95% target for the last 13 months, with latest performance for November 2022 provisionally at 97.6%.


Percentage of episodes clinically coded within one reporting month post episode discharge end date

2020/21	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar
Hywel Dda UHB	48.4%	63.5%	70.6%	74.0%	76.0%	77.2%	69.9%	68.5%	66.6%	64.3%	67.7%	67.0%
All Wales	82.7%	86.2%	87.8%	87.0%	87.3%	86.4%	85.9%	91.3%	87.1%	87.5%	86.7%	83.1%
Target = 95%	95.0%	95.0%	95.0%	95.0%	95.0%	95.0%	95.0%	95.0%	95.0%	95.0%	95.0%	95.0%

2021/22	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar
Hywel Dda UHB	44.5%	73.0%	74.1%	81.0%	86.4%	90.1%	96.7%	95.0%	95.6%	97.4%	97.3%	96.3%
All Wales	77.9%	81.6%	83.7%	88.6%	88.4%	88.0%	90.8%	86.6%	87.5%	87.7%	87.6%	84.1%
Target = 95%	95.0%	95.0%	95.0%	95.0%	95.0%	95.0%	95.0%	95.0%	95.0%	95.0%	95.0%	95.0%

2022/23	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov (prov)
Hywel Dda UHB	95.5%	95.7%	96.0%	97.2%	97.1%	98.1%	98.3%	97.6%
All Wales	78.6%	81.4%	83.4%	81.4%	83.1%	84.4%	85.7%	
Target = 95%	95.0%	95.0%	95.0%	95.0%	95.0%	95.0%	95.0%	95.0%

The current backlog position for 2022/23 activity shows that the Health Board has 98.5% of episodes from April to November coded so well on track to achieve the 98% for the end of the financial year by continuing on this trajectory.

Information Quality Assurance (IQA) Data Quality
The Sub-Committee received an update on data quality within the Health Board specifically around three deep dives.

- Discharge Lounge Activity reporting
- Maternity Reporting
- Acute Medical Assessment Unit (AMAU) Ward Attender Recording

The Sub-Committee welcomed the work and noted the recommendations included within the reports and requested that these form an action plan for the Sub-Committee to monitor.

HDdUHB – Information Governance Audits
The Sub-Committee received an update from the Information Governance Team on a number of IG audits undertaken to check for any Information Governance and Information Security risks, and seek assurance that Services are taking appropriate actions to ensure that data and assets are protected. The following areas have been visited initially:

- Accident & Emergency / Minor Injuries Units
- Outpatients Clinics
- 2 Hospital Wards (IG will aim to visit wards where there have been personal data breaches reported).

The Information Governance Team will be checking general IG compliance which includes:

- The display of Information Governance posters in staff areas
- The security of personal data within the ward/service area
- The use of lockable filing trollies for medical records
- That paperwork is not being left unattended e.g., ward round sheets being left on desk
- That patient names are not on notice boards in clear view of visitors or other patients
- That all staff on the ward have completed their Information Governance Training on ESR

The Sub-Committee welcomed the work and requested that regular updates are brought back to the sub-committee for monitor and escalation if required.

Microsoft Office 365 – Legal Hold (Litigation Hold)
The Sub-Committee received a paper on the proposed changes to the Litigation Hold contained within Microsoft Office 365 (O365). During the implementation of O365 it was noted that litigation hold was never used as intended. It should only be used where a reasonable expectation of litigation exists to preserve the integrity of the information. However, due to Microsoft not having a back-up solution, organisations were using litigation hold as a back-up solution which has caused the issues being experienced. The recommendation proposed that litigation is turned off as default for eligible licenced users (which was implemented for all new users as of May 2021) and disable litigation hold for all mailboxes that were enabled prior to May 2021, except for identified mailboxes that require litigation hold. The Sub-Committee were informed that HDdUHB had not applied the blanket approach to Litigation hold to all employees in the same way as in the other health boards across NHS Wales. The Health Board was utilising the Archiving functionality before the introduction of O365 and therefore it was not necessary to apply the Legal Hold across all employees, and those that have Litigation Hold applied to their accounts will not be removed as rules had been applied appropriately.

HDdUHB's Corporate and Medical Records Storage Assurance Report – Update

The Sub-Committee received an update on the current audit of storage facilities across the Health Board. The IG team contacted the Withybush Senior Team to discuss a number of storage containers at the rear of the hospital.

Information Commissioner Office (ICO) Notifications

Since April 2022, there have been 5 occurrences when a notification to the ICO has been required. The following table highlights the current notifications:

	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Total
Open	1	0	2	0	1	0	0	0	1	-	-	-	5
Closed	-	-	-	-	-	-	-	-	-	-	-	-	0
Total	1	0	2	0	1	0	0	0	0	0	0	0	4

Cyber Security and Network and Information Systems (NIS) Directive Update

A separate report has been prepared for presentation to the In-Committee meeting of the Sustainable Resources Committee to provide an update on progress of Cyber Security.

Materion y Mae Angen Ystyriaeth neu Gymeradwyaeth Lefel y Pwyllgor Adnoddau Cynaliadwy:
Matters Requiring Sustainable Resources Committee Level Consideration or Approval:

Approval of the following policies:

- 275 Secure Transfer of Personal Information Policy, attached at Appendix 1
- 193 Retention and Destruction of Records Policy, attached at Appendix 2
- 174 Reuse of Public sector Information Procedure, attached at Appendix 3
- 282 Network Security Policy, attached at Appendix 4
- 319 - Disposal of Digital Equipment Policy, attached at Appendix 5
- 422 - Consumer Device Policy, attached at Appendix 6

Risgiau Allweddol a Materion Pryder:
Key Risks and Issues / Matters of Concern:

- The wider strategic issue of the storage of records and boxes within external storage companies.

Busnes Cynlluniedig y Grŵp/Is-Bwyllgor ar Gyfer y Cyfnod Adrodd Nesaf:
Planned Group/Sub-Committee Business for the Next Reporting Period:

Adrodd yn y Dyfodol:
Future Reporting:

- Information Asset Owners and Information Asset Mapping Update
- Data Quality and Clinical Coding
- Information Governance Risk Register
- Information Governance Toolkit improvement plan
- Update on Cyber Security / NISR
- Caldicott Register to be returned to the IGSC meetings
- Digital / IG Policies and Procedures

Dyddiad y Cyfarfod Nesaf:
Date of Next Meeting:

6 April 2023

Bwrdd Iechyd Prifysgol
Hywel Dda
University Health Board

Secure Transfer of Personal Information Policy

Policy information

Policy number: 275

Classification:

Corporate

Supersedes:

N/A

Local Safety Standard for Invasive Procedures (LOCSSIP) reference:

List the LOCSSIP reference if applicable, if not state not applicable

National Safety Standards for Invasive Procedures (NatSSIPs) standards:

List the NatSSIP reference if applicable, if not state not applicable

Version number:

V.04

Date of Equality Impact Assessment:

Detail date of EqIA

Approval information

Approved by:

Complete

Date of approval:

Enter approval date

Date made active:

Enter date made active (completion by policy team)

Review date:

Enter review date (normally three years from approval date)

Summary of document:

This policy lays out the security requirements for the transfer of personal information into, across and out of the Health Board in any format.

Scope:

This policy applies to all staff and service areas across the Health Board.
It applies to all hard copy and electronic personal information processed by the Health Board.

To be read in conjunction with:

837 – All Wales Information Security Policy
172 - Confidentiality Policy
224 - Information Classification Policy
836 – All Wales Information Governance Policy
291 - Personal Employee Records Management Policy
201 – All Wales Disciplinary Procedure and Policy
491- All Wales Email Use Policy
301 - User Account Management Policy

Patient information:

Include links to Patient Information Library

Owning group:

IGSC

Date signed off by owning group

Executive Director job title:

Huw Thomas, Director of Finance

Reviews and updates:

Reviews and updates		
Version no:	Summary of Amendments:	Date Approved:
1	New Policy	May 2012
2	Updated Policy following review	22.08.2017
3	Updated – Data Protection Act 2018/UK General Data Protection Regulation or any subsequent legislation to the same effect	26.06.2018
4	Review by IG	09.09.2021

5	Moved to new template	18.11.2022
6	Policy Review	11.11.2022
8	Policy Review following IGSC November 2022 – Updated Cloud storage / Verbal Communications / Text Messaging	20.01.2023
9	Additions and amendments as highlighted at IGSC January 2023	13.02.2023

Keywords

Information Governance, Information Security, Personal Information

Glossary of terms

Provide a glossary of terms and abbreviations

Term	Definition
Caldicott Guardian	A Caldicott Guardian is a senior person responsible for protecting the confidentiality of people's health and care information and making sure it is used properly. They uphold the Caldicott Principles that lay out how patient information should be handled by NHS organisations to ensure confidentiality is upheld.
Bulk Transfer	The transfer of electronic or paper information that is ‘batched up’ to be sent out of a location and/or organisation and involves sending personal information about multiple individuals.
Data Protection Legislation	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.
Encryption	Is the process of converting information into a form unintelligible to anyone except holders of a specific key or password.
Information Asset Owner	Every information asset must be assigned an owner within the Health Board who will be responsible for it throughout its lifecycle. This Owner may work in any department but must have sufficient ability, authority and experience to understand the contents and approve the processing of the record
Personal Data	Personal Data is information which relates to a living individual who can be identified from the information itself or by linking it with other information – for example a person’s name and address, an online profile, a member of staff’s HR record or records relating to individual’s such as patients or service users.
Personal Data Breach	A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.
Removable Media	Is a term used to describe any kind of portable data storage device that can be connected to and removed from a computer e.g. floppy

	discs, CDs/DVDs, USB flash memory sticks or pens, PDAs, tablets, and smart phones/devices
Requester	Any individual that requests records from a Health Board department / service. They may be another Health Board department / service, a Service provider, an Integrated Services Team, or an external Agency.
Sender	The individual acting for the Health Board that initiates a Data Transfer/sends information. They must have the authority and sufficient knowledge of the nature of the information to determine whether it should be sent and that it is sent securely. Where the final actual task is delegated to administrative, untrained or inexperienced staff, the original Sender remains responsible for ensuring the Transfer complies with this policy
Senior Information Risk Owner (SIRO)	An Executive Director or member of the Senior Management Board with overall responsibility for information risk across the Health Board.
Special Category Data	Special category data means personal data consisting of information as to: - Genetic and biometric data - Political opinions - Religious or other beliefs - Trade union membership - Physical or mental health/condition - Sexual life And although not specifically described as special category data, this information requires the same treatment: - The commission or alleged commission of any offence - Any proceedings for any offence committed/alleged to have been committed, the disposal of such proceedings or the sentence of such proceedings
TLS	Transport Layer Security (TLS) is an encryption protocol that protects data when it moves between computers. The current standard is TLS 1.3.
Unauthorised Access	Access to information that is not part of your work duties. Access to a patients record where the patient is not under your care.

Contents

Introduction

The sharing of information between departments within the Health Board, to third-party service providers, to other public bodies, commercial organisations and individuals is an important part of delivering safe and effective patient care and for the effective running of the Health Board.

Although information sharing is an important part of what the Health Board does, all staff need to make sure that it is done safely, legally and in a way that ensures confidentiality at all times.

In every transfer of information there is a risk that the information may be lost, misappropriated or accidentally released. The Health Board has a legal and moral duty of care when handling information, particularly that containing personal and/or confidential information belonging to our patients and staff.

Policy statement

The organisation recognises its responsibility to process its personal information correctly and in-line with all legal, regulatory and internal policy requirements.

Scope

This policy provides information to all staff about the minimum security requirements they must use when transferring information into, across and out of the organisation, via any media and in any format. This policy applies to all employees of the Health Board, volunteers, any contracted staff and third-party organisations that processes the organisation's information.

Aim

This policy outlines the responsibilities and the minimum security requirements for the transfer of personal information and should be read and understood by all staff and third parties that use and transfer Health Board information.

The correct application of this policy will ensure that the Health Board is compliant with its legislative responsibilities including the Data Protection Act 2018/UK General Data Protection Regulation or any subsequent legislation to the same effect, reduce the risk of an information security breach taking place and provide assurance to our staff and patients that information assets are being properly managed.

Objectives

The aim of this document will be achieved by the following objectives:

- Ensure that staff understand their responsibilities and the most appropriate methods for transferring and sharing information.
- Protect and prevent personal or confidential information from being lost, stolen or intercepted by unauthorised persons.
- Reduce the risk of an information security breach from taking place.
- Maintain patient and staff trust in the Health Board that their personal information is being managed safely and appropriately by staff across the organisation.
- Ensure that access to information is maintained by preventing information from being lost or stolen or sent to the wrong individual or location.
- Ensure the Health Board is meeting its legal and moral duties in relation to maintaining confidentiality in line with the Data Protection Act 2018/UK General Data Protection Regulation

or any subsequent legislation to the same effect, the Common Law Duty of Confidentiality, the Human Rights Act 2015 and other legislative requirements.

Main body

1. Risks in transferring Personal Information

There are a number of risks associated with transferring personal information.

The severity and type of these risks will vary depending on the method of transfer. Examples of such risks include:

- Information being lost, damaged or intercepted in transit e.g. stolen laptops, lost memory sticks, opened envelopes.
- Delivery service delivering mail incorrectly.
- Information being sent to the wrong address via e-mail, post or fax.
- Information received by the organisation but not delivered to the correct person.
- Personal information not being disposed of appropriately.
- Personal information being deliberately transferred with criminal/fraudulent intent e.g. ID theft.
- Personal information being uploaded to public cloud services such as Dropbox, Google Drive and iCloud which maybe unencrypted and stored in countries without the same regulatory framework as the UK.

Where such risks are realised and personal information is compromised there is an impact on the following:

Individuals - whose information has been put at risk:
Loss of personal information can cause harm and severe distress to individuals, particularly where it is sensitive and private information (special category data) e.g. about their health and care. Loss of information could also have a direct impact on patient care if it is not readily available to the care team. Individuals could also be the victims of identify fraud or other types of crime if their personal information is lost or stolen.
Staff - whose actions placed the information at risk:
Staff who have breached this policy could potentially face disciplinary action. There may also be legal implications and potential criminal action taken if they have knowingly breached key legislation.
The Organisation - whose actions placed the information at risk:
The Health Board may experience a loss of trust, confidence or reputation from the patients/clients, service users, staff, volunteers, partners, contracted staff and visitors, who we rely upon to share information with us to provide a quality and safe service. The organisation could also face a potential fine from the regulator (the Information Commissioners Office) if we do not properly look after and safeguard personal information.

If any staff member has concerns about how information is being sent, shared or transferred within the Health Board they should report this to the Information Governance Team as soon as possible so that appropriate action can be taken.

2. Use of Caldicott and Data Protection Principles when transferring personal information

Before transferring any personal information the Principles should be applied. These are:

Caldicott Principles		**Data Protection Act 2018 Principles**	
Number	**Principle**	**Article**	**Principle**
1	Justify the purpose(s) for using confidential information.	5(1)(b)	Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation').

2	Use confidential information only when it is necessary.	5(1)(b)
		5(1)(c)
			As above, and
			Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').

3	Use the minimum necessary confidential information.		
4	Access to confidential information should be on a strict need-to-know basis.	5(1)(f)	Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').
5	Everyone with access to confidential information should be aware of their responsibilities.		
6	Comply with the law.	5(1)(a)	Processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency').
7	The duty to share information for individual care is as important as the duty to protect patient confidentiality.	5(1)(b)	As above
8	Inform patients and service users about how their confidential information is used.	5(1)(a)	As above
		Additional Principles - Data Protection Act 2018	
		5(1)(d)	Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy').
		5(1)(e)	Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation').
		5(2)	The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

This policy will assist staff in meeting these principles when sending and transferring personal information.

3. General requirements for transferring personal information

Before sending or transferring any personal information, the sender must consider the various methods available and whether these are appropriate for the type of information being sent.

This policy sets out the main methods / media that can be used for transferring or sending personal information and the minimum requirements that must be followed.

If any staff members are unsure about what method to use for sending or transferring information they can contact their line manager, Head of Department or the Information Governance Team for further advice.

For all transfers of all personal information it is essential that the identity and authorisation of the recipient has been appropriately authenticated by the sender.

This includes taking the following action:

- Double checking any information sent by post to make sure you have the correct name and address. Check these are up to date against any central patient administration systems if appropriate.
- Before putting any information into an envelope to send to another individual, double check to make sure it contains no other information that should not be sent to that person – mixing up of paperwork for different individuals is a common mistake made by staff and can lead to a serious personal data breach.
- Before you send any personal information by e-mail double check you have the correct recipient/e-mail address selected. Double check that the attachments are correct before you press send.
- If sending email communication outside of the Health Board to multiple recipients use the BCC functionality so you do not share individuals' email addresses

3.1. Bulk Transfer

It is essential that all departments of the Health Board have in place systems to ensure that bulk transfers of personal information are appropriately controlled and carried out securely. Bulk transfers are any situation where a department is sending or transferring information about more than ten individuals at the same time.

Any bulk transfer of information should be authorised by your Line Manager / Head of Department for the information being sent. They will decide whether to authorise the transfer of this information after careful consideration of the content, format and method of transfer. They can seek further advice from the Information Governance Team if required about the best method for sending or transferring the information.

The safest way to send a bulk transfer is by setting up a regular file transfer using the Secure File Sharing Portal. All staff can access the portal by following the link and entering their staff Cymru Id and Password. If you have any issues accessing the portal, please log a request to the ICT Service Desk.

Staff can also contact the Information Governance Team for more information about the Secure File Sharing Portal.

3.2. Electronic Mail

Electronic mail should be used in accordance with the Health Board's 491 - All Wales Email Use Policy.

Personal e-mail accounts (e.g. Outlook.com accounts, Gmail, iCloud) must not be used at work for transferring personal information. Additionally, no information about patients or staff should be sent to your private email addresses.

The NHS Wales network is considered to be secure for the transfer of any information including PII and business sensitive information. This includes all email addresses in the NHS email directory which include those email addresses typically end in "wales.nhs.uk".

All electronic documents containing personal information and sent outside of the NHS Wales network should be sent using the Secure File Sharing Portal. See point 9 above about how to get access to the Secure File Sharing Portal.

Information sent within the NHS Wales network (anybody with a @wales.nhs.uk e-mail address) can be sent by standard e-mail, unless the information being sent is classified as 'restricted' or 'OFFICIAL – SENSITIVE' information. See the Health Board's 224 - Information Classification Policy for details about the type of information that should be classified as 'restricted' or 'OFFICIAL – SENSITIVE'.

If 'restricted' or 'OFFICIAL – SENSITIVE' information is being transferred or sent by e-mail within the NHS Wales Network then always password protect any attachments as an additional precaution in case the e-mail is sent in error to the wrong recipient. The password should be compliant with the requirements in the User Account Management Policy. Any method for giving the password to the intended recipient should be done via a different method i.e. by telephone, in person etc.

If 'restricted' or 'OFFICIAL – SENSITIVE' information is being transferred or sent by e-mail outside of the NHS Wales Network then always use the Secure File Sharing Portal and upload the information through the 'Packages' option. This is the option used for regular file sharing within the portal.

This means, if you do send the information to the wrong e-mail address in error, you can remove the documents from the folder on the Secure File Sharing Portal (so long as they haven't already been accessed).

In emergencies, if you are unable to access the Secure File Share Portal and the information you need to send is time critical, place all PII in attachments which are encrypted with a password and contact the recipient by phone with the password.

The following checks/precautions should be carried out by the sender at all times when transferring personal information by e-mail:

- Always double check that the name and e-mail address of the recipient are correct. It is good practice to turn off 'auto complete' from your e-mails as this prevents the wrong name and e-mail address being automatically chosen in error.
- The Email message must contain clear instructions on the recipient's responsibilities and instructions on what to do if they are not the correct recipient.
- Check with the recipient that his / her e-mail system will not filter out or quarantine the transferred file.

- The sender must check at an appropriate time that the transfer has been successful, and report any issues to his / her line manager.
- Ensure that the information within the e-mail is stored in the agreed format for the record type i.e. in line with professional record keeping guidelines. See the Health Board's 224 - Information Classification Policy for further details.

TLS – Transfer Layer Security

The NHS Wales network is considered to be secure for the transfer of any information including personal data and business sensitive information within NHS Wales and organisations with Transport Layer Security (TLS) enabled. This includes all email addresses within the NHS email directory that end in "wales.nhs.uk", which are hosted on the NHS Wales email service and the email services of TLS enabled organisations as listed on HOWIS. The list can be accessed here: http://howis.wales.nhs.uk/sites3/page.cfm?orgid=852&pid=74727.

Transfer of personal data or business sensitive information between any email address not ending in "wales.nhs.uk", or TLS enabled is not currently considered secure. Where this type of information needs to be sent, appropriate security measures must be implemented, for example, the information should be sent via the Secure File Sharing Portal or via email with an appropriate level of encryption.

Users must be vigilant in ensuring that all emails are sent to the correct recipient and must check that the correct email address is used, for example by checking the NHS Wales email address book. Even where the recipient email address is considered secure, as a mitigating factor to avoid any inadvertent misdirection, encryption of any email attachment containing sensitive data should be considered. Misdirected emails should be reported via Datix.

3.3. Electronic Data Transfer (FTP (File Transfer Protocol), Secure FTP)

Standard FTP without encryption is inherently insecure and must not be used for transmitting personal information. Always use the Secure File Sharing Portal when transferring personal information outside of the NHS Wales network.

3.4. Electronic memory and removable devices, (CD, DVD, Floppy, USB drive, Memory Card)

It is always safer to send electronic information using the Secure File Sharing Portal wherever possible. If it is not possible to send or transfer the information via the portal and a removable device needs to be used the following guidance must be followed:

- Personal Information must be enclosed in a file and encrypted using a product approved by the Health Board.
- If the information needs to be posted, it must be sent using an approved courier or a secure mail method which can be tracked and is signed for e.g. Royal Mail Special Delivery.
- Any attachment is required to be password protected.
- Any password must be to organisation standard. 7 characters, mix of alpha and numeric.
- Any password to open the attached file must be transferred to the recipient using a different method than email, e.g. a telephone call to an agreed telephone number, closed letter.

- An accompanying message must contain clear instructions on the recipient’s responsibilities, and instructions on what to do if they are not the correct recipient.
- Any accompanying messages and the filename must not reveal the contents of the encrypted file.
- The sender must check at an appropriate time that the transfer has been successful and report any issues to his/her line manager.

3.5. External and Internal Post/Courier

It is always safer to use the Secure File Sharing Portal to send information to individuals outside the NHS Wales network and this should always be considered as the first option.

If it is not possible to use the Secure File Sharing Portal e.g. you are unable to scan in paper documents to prepare for sending; documents that contain personal information should always be sent using the following methods:

Information classified as being ‘confidential’

- **Internal mail to recipients within the Health Board**: If internal mail envelopes are used to send personal information internally, the information must be placed by the sender in a secondary sealed envelope and clearly marked ‘Confidential’ on the outside of this secondary envelope. Always provide a name and return address on the secondary envelope.
- Send an e-mail or phone the recipient to let them know you have sent them information via the internal mail and ask them to confirm receipt.

- **External mail to recipients outside the Health Board:** Always send information by e-mail using the Secure File Sharing Portal where possible. If this is not possible then always use an approved courier or a secure mail method which can be tracked and is signed for e.g. Royal Mail Special Delivery.

NB: Only correspondence letters should be sent using standard Royal Mail postage. The name and address of the individual should always be double checked against available systems to ensure it is correct.

Information classified as being ‘restricted’ or ‘OFFICIAL SENSITIVE’

- **Internal mail to recipients within the Health Board:** Staff should always consider scanning in and sending restricted information by e-mail to internal staff within the Health Board. Additional password protection should be applied to any attachments. The use of internal mail for sending restricted information should only be carried out in exceptional circumstances and must be approved by your Head of Department or Information Asset Owner.
- **External mail to recipients outside the Health Board:** Always send information by e-mail using the Secure File Sharing Portal through the ‘Packages’ option where possible. If this is not possible then always use an approved courier or a secure mail method which can be tracked and is signed for e.g. Royal Mail Special Delivery.

There are a number of standard requirements which must be adhered to when transferring information by post or courier services. There are also additional requirements around removable media and bulk transfers.

3.6 Standard Requirements: Sending or transferring by post

- Confirm the name, department and address of recipient and enter details correctly on the envelope/parcel.
- Mark the envelope/parcel, private and confidential and add a return address and contact details, unless this will directly compromise confidentiality.
- Package securely to protect the contents from being tampered with or from any physical damage likely to arise during transit e.g. a tamperproof wallet.
- Always use an approved courier or secure mail method for sending personal information which can be tracked and is signed for e.g. Royal Mail Special Delivery (unless you are sending standard correspondence letters).
- Packages must be received and signed for by the addressee.
- The sender must check at an appropriate time that the transfer has been successful, and report any issues to his / her line manager.
- When sending Medical Records / Health Care Records copies should be sent whenever possible and the sender must send them in sealed double envelopes with the address on both.

3.7 Standard Requirements: Sending or transferring by removable media using mail/postal services e.g. disks, encrypted memory sticks etc.

When transferring personal information (including bulk transfers) electronically you should always use the Secure File Sharing Portal to complete this task wherever possible.

If you do need to send electronic personal information via other removable media devices then the following should be followed:

- Devices containing information must be sent by an approved courier or a secure mail method which can be tracked and signed for e.g. Royal Mail Special Delivery:
- The individual responsible for passing the information to the Courier, must check the ID of the Courier and obtain a receipt from the Courier when the bulk personal information is collected.
- The sender must confirm the transfer has been received by contacting the recipient.
- The courier must only hand this information over to the recipient or to a nominated individual and obtain a signature when delivered
- Information must be encrypted prior to transfer, in line with Health Board standards.

3.8. In Person

On occasions, personal information may need to be transferred in person. This may be due to the needs of the team or because this may be the most secure method of transferring the information. Examples of this include handing a patient’s health care record over to a colleague off site, handing over an encrypted CD of personal data to another organisation etc.

Due to the number of different approaches to transferring personal information in person e.g. on foot, by car, public transport, in electronic or paper formats, it is not possible to give a definitive list of actions to be taken. Careful consideration must be given by the sender and their Head of Department before taking personal information off-site. Any potential risks should be considered and any actions taken to mitigate these risks should be agreed upon and documented.

Information classified as ‘restricted’ should not be taken off-site unless this has been specifically agreed by the Head of Department and/or Information Asset Owner for the information in question. If ‘restricted’ information needs to be taken off-site and it is not possible to send it via the Secure File Sharing Portal, this should be done using an encrypted device wherever possible.

Taking paper copies of ‘restricted’ information off-site should be avoided where ever possible. If it is absolutely necessary to take paper copies off-site, actions need to be agreed to mitigate any risks wherever possible with the Head of Department and/or Information Asset Owner as described above.

3.9. Verbal communications, including telephones

Requests for person-identifiable information from patients or other parties must be verified to confirm the person making the request has a right to know before release of any information.
Person-identifiable information should not be discussed on telephones that have ‘hands free’ capability unless they are situated in a single user office or car, and only those persons who need the information are present. Headsets should be used in virtual online meetings wherever possible.

3.10. Fax Transmission

Fax is inherently insecure and is not recommended for the transfer of personal information. It is always safer to share information using the internal e-mail system within the NHS Wales network or, the Secure File Sharing Portal to send information outside of the NHS Wales network.

However it is acknowledged that in certain circumstances information will need to be sent by fax. If this is the case the following guidance must be followed in all cases:

- The sender must check that the Fax number is correct and that the receiver is awaiting transmission.
- For personal information the number must be double-checked by a colleague before transmission and telephone contact must be maintained throughout transmission.
- Both sender and receiver must have an agreed process to avoid their copy being left on the Fax machine and a clear requirement to securely destroy the message when no longer required.
- The message must contain clear instructions on the recipient’s responsibilities and instructions on what to do if they are not the correct recipient.
- The sender must check at an appropriate time that the transfer has been successful and report any issues to his / her line manager.

Faxes should not be used for sending information classified as ‘restricted.’ The information should be scanned and sent via the Health Board’s Secure File Sharing Portal. Any agreement to use fax for sending ‘restricted’ information must be agreed by the Information Asset Owner for the information and the SIRO or Caldicott Guardian where patient information is being sent.

3.10 Text messaging (SMS)

There are various potential applications for text messages in the provision of services, e.g. service user appointments. The benefits of using text messages to convey information must be weighed against the risks. Key considerations when using text messages are:

- Is the mobile phone number correct?
- Is the mobile phone receiving the text message being used by the intended recipient of the message?

• Has the message been received, and what provision is there to audit message receipt?

Personal Mobile devices should not be used to communicate with patients.

Text messages should not be used to convey sensitive information and the use of text messages for the transfer of data should be kept to a minimum, e.g. an appointment reminder does not need to include the name of the specific clinic.

No personal information should be sent using SMS without express agreement from the Information Governance Team who will require a privacy impact assessment to be undertaken prior to any sharing of personal information taking place.

3.11. Information Sharing Agreements

All regular sharing of personal information should be subject to the appropriate agreement (unless the Information Governance Team confirm that an agreement is not required). Further advice and guidance on this can be sought from the Information Governance Team.

3.12. Cloud Storage

Where there is a requirement to share information with others using a cloud storage service, then it is important that individuals who enable the sharing of data do so with the following safeguards:

- Check if the Cloud Storage solution is safe by contacting Information Governance & the Cyber Security Team.
- Once approved as safe grant access only to the specific folders and files that are required to support the collaboration or information sharing. Ensure that no other folders or files are made available.
- Take care to ensure access is granted to the correct individuals.
- Inform all individuals involved in the collaboration or information sharing that they have a duty of care for the information provided and must honour all security requirements as well as privacy and confidentiality commitments.

All access to Cloud based storage should be approved by the Information Governance & Cyber Security Team.

4. Responsibilities

Executive Directors

Executive Directors are responsible for the management of information risk within their service areas and are responsible for ensuring their staff and managers are aware of this policy.

The Senior Information Risk Owner and Caldicott Guardian

The Senior Information Risk Owner and Caldicott Guardian are responsible for managing information risk and the safe and ethical use of information across the Health Board and are responsible for ensuring their staff and managers are aware of this policy.

Information Asset Owners

Information Asset Owners are responsible for understanding what information is held within their service areas and for ensuring that this policy is being applied to their information assets by staff and managers.

They are responsible for deciding upon the classification levels of information within their service or information asset area with support from the Information Governance Team where required.

They are responsible for making decisions as to how personal information contained within their information assets and/or sent from their service area should be transferred safely and securely by communicating with staff and managers. Further advice can be sought from the Information Governance Team as required.

They are able to delegate this responsibility to another named individual but they must retain overall responsibility for the information asset and the correct application of this policy to that asset.

Information Governance Team

The Information Governance Team are responsible for disseminating this policy across the Health Board and ensuring it is readily available to all staff. The team are responsible for providing appropriate support and advice to the Information Asset Owners, Service Lead, staff and managers to ensure the policy is understood and adhered to.

Line Managers

Line Managers must ensure that their staff have read and understood this policy and monitor staff compliance in meeting the policy requirements. Line Managers are responsible for reporting the non-compliance of this policy to the Information Governance Team.

All staff

All staff must read, understand and comply with this policy. If a staff member is not clear about any aspect of this policy and its application they are responsible for raising this with their line manager for further clarification.

5. References

- The Data Protection Act 2018/UK General Data Protection Regulation or any subsequent legislation to the same effect
- The Freedom of Information Act 2000
- Common Law Duty of Confidentiality

- Information Commissioner’s Office

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

Retention and Destruction of Records Policy (Including Health Records)

Policy information

Policy number: *193*

Classification: Corporate

Supersedes: Previous versions

Version number: 4

Date of Equality Impact Assessment:
08/12/2022

Approval information

Approved by:
Sustainable Resources Committee
Enter approval date

Date made active:
Enter date made active (completion by policy team)

Review date:
Enter review date (normally three years from approval date)

Summary of document:
This policy states our commitment to meet the required standards and legal obligations for the storage, retention and destruction of records, highlighting staff roles and responsibilities

Scope:
This policy has been written as guidance for Hywel Dda University Health Board in dealing with the legal retention and destruction timescales for all clinical and non clinical records and ensuring information is processed and disposed of in accordance with the Data Protection Act /General Data Protection Regulations 2018 or any subsequent legislation to the same effect. Staff working for the Health Board must make every effort to comply with this policy and applies to all permanent, temporary or contracted staff employed by Hywel Dda University Health Board (including Executive and Non – Executive Directors).

To be read in conjunction with:
[191] – Health Records Management Strategy
[192] – Health Management Policy
Records Management Code of Practice for Health and Social Care 2022
[172] – Confidentiality Policy
[836] – All Wales Information Governance Policy
[347] – Corporate Records Management Policy
[224] – Information Classification Policy
[837] – All Wales Information Security Policy

Patient information:
Include links to Patient Information Library

Owning group:
IGSC
Date signed off by owning group

Executive Director job title:
Director of Operations

Reviews and updates:

1. *New ;policy September 2012*
2. *Full review 23.2.2016*
3. *DPA update 26.6.2018*
4. *Full review*

Keywords
Retention and destruction, health records

Glossary of terms
Records management - is that "field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and [disposal] of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records". ISO 15489-1: 2016 Information and documentation – Records Management Records management is about controlling the organisation's records to ensure authenticity, reliability, integrity and usability

Retention Schedule - is a document setting out what records the Health Board holds and how long they will be retained before disposal. It can also be used to set out what needs to happen to records at various different stages of their lifecycle to ensure that they are stored efficiently.

A record - A health record is "*one which relates to the physical or mental health of an individual which has been made by or on behalf of a health professional in connection with the care of that individua*l". Anything that contains information that has been created or gathered as a result of any aspect of the work of NHS employees

Data Protection Legislation – the term Data Protection Legislation means all applicable laws, regulations and regulatory rules which govern the processing of personal data including (i) the Data

Protection Act 2018, Regulation (EU) 2016/679 the UK General Data Protection Regulation (UK GDPR), the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended) and any subsequent legislation enacted and duly in force from time to time relating to the processing of Personal Data; and (ii) all guidance and / or codes of practice issued from time to time by the Information Commissioner or relevant government department, and any relevant rulings from time to time of the Information Commissioner or of the Courts of England and Wales relating to the processing of Personal Data.

Contents

Introduction

The Public Records Act 1958 requires that there is a systematic and planned approach to the management of records within an organisation. NHS organisations have a statutory duty to make arrangements for the creation, safekeeping and eventual disposal of all such records, which ensures that the Health Board has access to reliable information. Records are a valuable resource because of the information they contain and the Health Board needs to maintain information in a manner that effectively serves its own business needs, those of the patient and to dispose of the information efficiently when no longer required.

High quality information underpins the delivery of high quality evidence based healthcare and many other key service deliverables. Information has most value when it is accurate, up to date and accessible when needed. An effective records management service ensures that all records and information is appropriately managed in line with legal requirements and is available whenever and wherever there is a justified need for that information, in whatever form of media it is required.

The key statutory requirement for compliance with records management principles is the Data Protection Act 2018 / UK General Data Protection Regulation 2016 or any subsequent legislation to the same effect. It provides a broad framework of general standards that have to be met and considered in conjunction with other legal obligations. The Acts regulate to the processing of personal data, held both manually and on computer. It applies to personal information generally, not just to health records.

Policy Statement

This policy complies with the Welsh Government National Guidance: Records Management Code of Practice for Health and Social Care – A guide to the management of health and care records.

The Code is a guide to use in relation to the practice of managing records. It is relevant to organisations working within, or under contract to, the NHS in Wales and provides a framework for consistent and effective records management based on established standards and current legislation. It includes guidelines on topics such as legal, professional, organisational and individual responsibilities when managing records. It also advises on how to design and implement a records management systems including advice on organising, storing, retaining and deleting records. It applies to all records regardless of the media they are held on.

This Code replaces the previous guidance: WHC 2000 (71): For the record – Managing Records in NHS Trusts and Health Authorities.

Individual members of staff are responsible for any records they create or use and all organisations and managers need to enable staff to conform to this policy and the standards of the code.

Scope of policy

This policy is provided to Hywel Dda University Health Board to deal with the legal retention and destruction timescales for all clinical and non-clinical records and ensuring information is processed and disposed of in accordance with the Data Protection Legislation or any subsequent legislation to the same effect.

Staff working for the Health Board must make every effort to comply with this policy and it applies to all permanent, temporary or contracted staff employed by Hywel Dda University Health Board (including Executive and Non – Executive Directors).

Aim

The policy will provide a framework within the Health Board to ensure compliance with Welsh Government National Guidance: Records Management Code of Practice for Health and Social Care – A guide to the management of health and care records.

The Health Board has an individual responsibility to retain all records securely, in line with legal timeframes. The aim of the policy is to ensure that retention periods for health records are maintained in accordance with Statute law. The policy will underpin all operational procedures and provide assurance and assistance to staff in terms of activities connected with the retention and destruction of records.

Objectives

The objectives of the policy are to provide all Health Board staff with clear guidance and standards to attain on a daily basis and provide robust assurance in regards the retention and destruction of sensitive and confidential patient information. The policy will ensure:

- All records are only retained for the minimum and legal timescales.
- Clearly appraised, validated and culled in line with guidance and best practice.
- Provide assurance that only relevant and appropriate records are destroyed.
- All records are destroyed in a confidential manner.
- Provide simplistic reference points for staff to identify retention periods for both clinical and non clinical records.
- Used as a service guide for all areas to comply with retention periods.
- Utilised as a guide for effective working and storage management.

What is a Record

There are a couple of definitions of a record, which are useful to highlight.

The ISO standard ISO 15489 – 1:2016 defines a record as:

- Information created, received and maintained as evidence and as an asset by an organisation or person, in pursuance of legal obligations or in the transaction of business.

Section 205 of the Data Protection Act 2018 defines a health record as a record which:

- Consists of data concerning health.
- Has been made by or on behalf of a health professional in connection with the diagnosis, care or treatment of the individual to whom it relates.

Records Management applies to any material that holds information gathered as part of the work undertaken in the NHS. A health record can be anything that contains information and has been gathered and created as a result of any aspect of the work of NHS employees – including management consultant agency or bank/agency staff. It will included decisions which relate to the physical and mental health of an individual which has been made by or on behalf of a health professional.

There will be a wide range of record formats and that will include both physical and digital records**.** Only relevant records that are utilised by Hywel Dda staff to undertake their daily duties, should be managed through this policy and in line with the guidance provided in Appendix ii and iii of the Records Management Code of Practice for Health and Social Care – A guide to the management of health and care records. A link to the Code of Practice is provided in the retention timescales section below.

Retention

Access to the health record is essential to the delivery of effective patient care. Patient health records must therefore be retained securely for the whole period that the patient is receiving active treatment and must be easily retrievable from either internal or offsite storage, whenever they are required by a clinician.

It is important to note that prior to relocating any records to a non Health Board storage provider/facility these proposals should be outlined and discussed with both the Health Records Manager and the Information Governance Service. Only approved Third Party Providers should be used.

This policy details the legal minimum recommended periods for the retention and destruction of records. Health Board staff will be responsible for complying with the minimum retention periods and providing assurances that retention timescales are being applied and adhered to, following the conclusion of treatment. The recommended minimum retention periods apply to both paper and digital records.

Destruction

All organisations have a responsibility to dispose of records at the end of their lifecycle, which is usually at the end of the retention period. Normally an appraisal will be completed, to decide what to do with the records, once their business need has ceased and the minimum retention period has been reached. Paper records selected for destruction and can be destroyed either in-house or under contract with an approved provider. If an external provider is used, the health organisation is responsible for ensuring the chosen provider meets the necessary requirements.

A record should be maintained and preserved confirming the destruction of records, showing their reference, description and date of destruction, so that the organisation is aware of those records that have been destroyed and are therefore no longer available. Disposal schedules would constitute the basis of such a record.

All records falling into the category of being selected for destruction will be destroyed after meeting relevant criteria, such as:

- All retention categories have been complied with
- Records will be identified either by manual or computer methodology
- All Hywel Dda University Health Board systems have been checked for most recent activity
- Records will be physically checked to ensure that there are no entries relating to a later date
- Records will be marked as destroyed on the relevant computer systems on which details of the patient records are held e.g. Welsh Patient Administration System (WPAS)
- Records for destruction will be destroyed in accordance with the appropriate Confidential Waste Process.

Legislation

This policy and the guidelines provided take into account and must be applied in conjunction with the laws relating to confidentiality, data protection, the patient's rights of access to his/her health records and the staff's duty of care to patients to make proper records. The Health Board and Managers within services must ensure staff are also aware and familiar with such laws, guidance and governance principles.

Responsibilities

Records management should be recognised as a specific corporate responsibility within every organisation. It should provide a managerial focus for records of all types, in all formats throughout their lifecycle, from creation through to ultimate disposal. The records management function should have clear responsibilities and objectives and be adequately resourced to achieve them.

The Chief Executive has overall accountability for ensuring the effective implementation of this policy and ensuring records are retained securely and disposed of in a timely and confidential manner, in accordance with the identified legal guidance and information governance standards. The Chief Executive may delegate responsibility for management and organisation of retention and destruction service to a designated Executive/Caldicott Guardian who is responsible for ensuring appropriate mechanisms are in place to support service delivery and continuity.

The Health Records manager has professional and operational responsibility for the security, retention and destruction of health records ensuring practices within the organisation are managed in accordance with legal timescales and that related policies and procedures conform to the latest legislation and standards. The Health Records Manager is accountable for ensuring only appropriate records are destroyed and for reviewing destruction processes to maintain confidentiality at all times

All Health Board staff have an individual responsibility for the records they create and use. All staff must ensure all records and patient information, which is extremely confidential is destroyed by utilising the confidential waste process available to them and in line with Health Board standards.

Training

All staff employed by the NHS in Wales will receive information on their personal responsibilities for record keeping in contracts of employment. This includes the creation, use, storage, security and confidentiality of health records. Appropriate training will be given to all health records staff on the systems used to maintain records and these will meet local and national standards. All new employees to NHS organisations in Wales will be given basic records practice training as part of the induction process.

Professional standards of record keeping are governed by the associated Royal colleges. These standards should form part of the professional practice review.

Training in the specifics of confidentiality and data protection will be identified through the agreed Information Governance training sessions.

Retention Timescales

Retention timescales can vary quite significantly across the various record types. It is essential that staff only review retention timescales associated with the record types they utilise within their roles and responsibilities within the Health Board. Retention guidance is provided in Appendix ii and iii of the

Records Management Code of Practice for Health and Social Care – A guide to the management of health and care records and information for all Health Board staff on nationally agreed retention guidelines can be located at:

https://gov.wales/sites/default/files/publications/2022-03/records-management-code-of-practice-for-health-and-social-care-2022.pdf

Reuse of Public Sector Information Policy

Policy information

Policy number: **174**

Classification:
Corporate

Supersedes:
Previous versions

Version number:
3

Date of Equality Impact Assessment:
18/01/2023

Approval information

Approved by:
Sustainable Resources Committee
Date of approval:
Enter approval date

Date made active:
Enter date made active (completion by policy team)

Review date:
Enter review date (normally three years from approval date)

Summary of document:
The purpose of this policy is to ensure that requests for the re-use of public sector information are managed in accordance with the Re-use of Public Sector Information Regulations 2005 (the Regulations

Scope:
This policy applies to:

- All employees, including permanent, temporary, contractual and agency, and Independent Members;
- Volunteers, students or any other authorised people working with or for the UHB
- Those who hold information on behalf of the UHB.

To be read in conjunction with:
173 – Freedom of Information and Environmental Information Policy – opens in a new tab
224 – Information Classification Policy – opens in a new tab

Patient information:
Include links to Patient Information Library

Owning group:
IGSC
Date signed off by owning group

Executive Director job title:
Joanne Wilson, Board Secretary

Reviews and updates:
1 – new policy 1.3.2011
2 – revised 2.12.2014
3 – full review

Keywords
Re-use, public sector information, RPSI

Glossary of terms
UHB – Hywel Dda University Health Board
OGL - Open Government Licence
URI - Uniform Resource Indicator
URL - Uniform Resource Locator
SIRO - Senior Information Risk Officer

Contents

INTRODUCTION

The purpose of this policy is to ensure that requests for the re-use of public sector information are managed in accordance with the Re-use of Public Sector Information Regulations 2015 (the Regulations). The purpose of the Regulations is to establish a framework that provides for effective re-use of public sector information and is based on the principles of fairness, transparency, non-discrimination and consistency of application.

Most information supplied in response to information access regimes such as the Freedom of Information Act 2000 and the Environmental Information Regulations 2004 will be protected by copyright and permission to re-use it will be required as the provision of information does not confer any automatic right to re-use the information. The Regulations provide a framework for re-use of information once access has been obtained. However, the Protection of Freedoms Act 2012 which amends S102 of the Freedom of Information Act contains provisions under which certain public sector owned datasets will be reusable at the point of access by means of a specified licence.

Re-use of information occurs where information is used for a purpose other than the original purpose for which it was created by a public sector body within its public task. Re-use helps to deliver three key government priorities: public sector transparency; increased public involvement in achieving government objectives; and increased economic growth (UKGLF, 2013).

SCOPE

This policy applies to:

- All employees, including permanent, temporary, contractual and agency, and Independent Members;
- Volunteers, students or any other authorised people working with or for the UHB
- Those who hold information on behalf of the UHB.

AIM

This policy is to ensure that Hywel Dda University Health Board (UHB) is compliant with the Re-use of Public Sector Information Regulations 2015.

OBJECTIVES

This policy will set out the arrangements for the following:

- Dealing with applications for re-use within 20 working days in a non-discriminatory way
- To publish terms of re-use, usually in the form of a licence
- Not to enter into exclusive arrangements other than in exceptional circumstances
- To provide information about what information is available for re-use. This should be in the form of an information asset list

DEALING WITH APPLICATIONS FOR RE-USE

<u>Copyright</u>

Most information produced by the UHB is subject to copyright protection and the UHB has the right to authorise the re-use of the information it produces under UK copyright legislation. The Regulations only apply to copyright and related rights (database rights, publication rights and rights in performances). They do not apply to other intellectual property rights such as patents, trade marks and design rights.

Documents

All documents held by the UHB fall within the scope of the Regulations with the exception of those which:-

- fall out of the public task of the UHB
- contain content in which the relevant intellectual property rights are owned or controlled by a person or controlled by a person or organisation other than the UHB, eg photographs
- are exempt from release under the Freedom of information Act (except where s21 applies), Environmental Information Regulations and any other access legislation

The Regulations define 'document' by relating it to 'content' which is information recorded in any form.

Request for re-use

The provision of information does not confer any automatic right to re-use the information. Regulation 6 state that applicants should:

- Make requests for re-use in writing, including email. Requests must be legible and usable for subsequent reference
- Provide their name and address
- Specify which documents they want to re-use
- State the purpose for which the document is to be re-used

Where the requester cannot provide the request in writing, assistance can be provided to the applicant whereby the request can be drafted and confirmed with them. Once confirmation is received, it is considered to be a written request and the UHB is obliged to respond.

Requests in Welsh and other languages will also be accepted and the UHB will adhere to relevant equality legislation when providing information requested. (See section also 'processing requests for reuse')

Responding to a request for re-use

Regulation 8 sets out how public sector bodies should respond to requests, including timescales. In response to requests for re-use, the UHB can issue one of the following responses:

- A refusal to give permission to re-use
- Supply the document to the applicant, if it has not already been supplied under access to information legislation, ie Freedom of Information.
- Offer terms and conditions for re-use, often in form of a licence

In terms of timescales, documents will fall under 2 broad categories:

Readily available documents

This covers documents which have already been made available and would include those which have already been published or are identified as being available for re-use on an asset list. These must be responded to within 20 working days.

Under the Regulations, the UHB is allowed up to 20 working days following the date of receipt of the request for re-use to finalise any licence offer.

Previously Unreleased Documents

This covers unpublished documents and information that has not been identified as being available for re-use. Permission for re-use is subject to access issues being resolved.

If the request for access and re-use is combined, it must be dealt with fully in terms of access to the information before a final decision on re-use can be taken. Where requests for re-use are extensive in terms of the number of documents requested, or raise complex issues, the UHB may extend the response time. However, it must be prepared to justify that the time taken to respond is reasonable. The UHB must also inform the applicant before the expiry of the 20 working days that it is unable to respond to the request within the standard timeframe and provide an indication of when a response can be expected.

Notification of Refusal

Under Regulation 9, when the UHB refuses a request for re-use, it must:-

- Set out the reasons for refusal in writing
- Explain what forms of redress are open to the applicant, both internal and independent
- Where the refusal is based on the fact that copyright or other relevant intellectual property rights (IPRs) are owned by a third party, the owner must be identified (where known)
- Where the owner of the third party copyright is not known, the name of the person from whom the document was obtained should be provided (where known). If it is not known, this fact should be stated.

Processing requests for re-use

Under Regulation 10, requests for re-use should be dealt with electronically, where possible, and should take advantage of existing licensing systems that are available. However Regulation 11 does not require public bodies to make documents available in a format other than the format or language in which the document already exists (unless it has duties to do so under other legislation such as the Equality Act and the Welsh Language Standards). Regulation 11 also confirms there is no obligation to:

- create or adapt a document to comply with a request for re-use
- provide extracts of documents where this would entail disproportionate effort
- continue producing a document purely for re-use by others

Conditions

Regulation 12 allows the UHB to set conditions on the re-use of documents. Conditions should not unnecessarily restrict the way in which a document can be re-used nor should it seek to restrict competition between re-users.

Terms and conditions are set out within the licences below. There are 3 different types of licence which can be issued:-

Open Government Licence (OGL)

The Open Government Licence is an open licensing model and tool for public sector bodies to license the re-use of their information and data easily. It consists of a simple set of terms and conditions to which public sector bodies simply point as the relevant licence. Use of information under the OGL is free and allows information to be used and re-used for commercial and/or non-commercial purposes. Licensees are required to include an attribution statement in any use of the information. An attribution statement identifies the name, creator and date of information, and acknowledges them appropriately. It demonstrates further the source of the information and its use under the OGL. Public bodies are encouraged to use the OGL symbol on their websites and in publications wherever possible.

Templates on how to apply the OGL to UHB online information resources and print publications can be found at Appendix 1 – opens in a new tab.

Non-Commercial Government Licence

The default position is that public sector information should be licensed for use and re-use free of charge under the OGL. However there are specific circumstances where information may only be released for use and re-use for non-commercial purposes. The Non-Commercial Government Licence has been developed to meet those circumstances.When a public sector body licenses its information under the Non-Commercial Government Licence, it should insert a visible statement asserting this and provide the Non-Commercial Government Licence URI (Uniform Resource Indicator) or URL (Uniform Resource Locator) in the information.

Templates on how to apply the Non-Commercial Government Licence to the UHB online information resources and print publications can be found at Appendix 2.

Charged Licence

As indicated in previous sections, public sector information should be licensed for use and re-use free of charge under the OGL. However there are circumstances where it is appropriate to charge for use and re-use. The Charged Licence is designed for use in situations such as the context of s102 of the Protections of Freedoms Act 2012. Legal advice should be sought before offering information for use and re-use where charges are made.

Licensing software and source code

The public sector produces software or source code as well as types of content such as documents and data. Software is protected by copyright and this make licensing considerations important. Many developers release their work under open source licences which enable software to be re-used freely and free of charge.

Public sector bodies that are involved in developing their own software and source code are encouraged to make them available as openly as possible. Developers may choose to release their software and source code under OGL or alternatively the Open Source Initiative maintains a list of approved open source licences covering software and source code that can be used (http://opensource.org/licenses).

Non-discrimination

Under Regulation 13, the UHB must not discriminate in the conditions applied between applicants who re-use documents for similar purposes. The emphasis is on the use of the documents rather than the re-user. The only exception to this is where a particular user or groups of users have a statutory right to re-use material. For example, libraries, archives and educational establishments enjoy special privileges under the Copyright, Designs and Patents Act 1988, which also includes special provisions for the reproduction of material for visually impaired persons.

Prohibition of Exclusive Arrangements

Under Regulation 14, the UHB should not enter into exclusive arrangements as it prevents others from re-using the document and inhibits competition. This covers appointing publishers to publish versions of documents. An important exception to this is where a service in the public interest cannot be provided other than by means of granting an exclusive licence. However the terms of the arrangement must be published and the justification regularly reviewed (at least every 3 years).

Charging

Although there is no obligation on the UHB to charge for re-use, it retains the right to do so, and where a charge is made it will be noted on the UHB Publication Scheme. Under the Regulations the UHB is permitted to charge for re-use. However the total income should not exceed the cost of collection, production, reproduction and dissemination of documents and a reasonable return on investment. As much of the information held by the UHB is available in digital format, the costs of allowing for re-use will often not involve any additional costs.

The UHB should be able to justify any charges that are applied for re-use and if the charge includes supplying of the document, or that it has been subject of a request under Access to Information Legislation (ie Freedom of Information Act) then the access fee should be deducted from the fee for re-use.

Nominal charges may cover basic costs relating to:

- The collection, production, reproduction and dissemination of the documents including relevant copyright work, eg, copying, printing and postage
- The cost of conversion of the information to a different format or extraction from a larger dataset

Information to be published by the UHB

Public bodies must be open, transparent and fair in processing applications for re-use. Under Regulation 16, the UHB is required to publish asset lists, standard licence terms and details of any charges, electronically where possible.

Internal review procedure

The Regulations require that the UHB has an effective procedure to consider any complaints that arise from the application of the Regulations. Regulation 17 requires that complaints are responded to ‘within a reasonable time’. The UHB aims to provide a response to a complaint relating to re-use within 20 working days unless there are good reasons why this is not possible.

All complaints must be made in writing to the UHB in the first instance, providing all the relevant information. The UHB response must also be in writing clearly setting out the reasons behind its decision, within the timeframe outlined above. If the internal process fails to resolve the issue, the complainant can refer the issue to the Office of Public Sector Information at the National Archives (Further information can be found on the following link: http://nationalarchives.gov.uk/documents/information-management/psi-complaints-procedure.pdf).

RESPONSIBILITIES –

Chief Executive

Overall responsibility for compliance with the Regulations lies with the Chief Executive.

Executive Director of Finance/Senior Information Risk Officer (SIRO)

The responsibility for ensuring arrangements are in place for compliance with the Regulations has been devolved to the Executive Director of Finance/Senior Information Risk Officer (SIRO).

Head of Corporate Legal Services and Public Affairs

The responsibility for ensuring that there are day to day arrangements in place for managing requests for re-use and reviews into complaints received in relation to the re-use of information lies with the Head of Corporate Legal Service and Public Affairs.

Freedom of Information Team

The responsibility for the day to day management of requests for re-use and providing advice to UHB staff lies with the Freedom of Information Team. This involves developing and maintaining this policy, managing requests for re-use, maintaining a record of requests for re-use, issuing licences and any related fees notices.

All staff

Staff are responsible for ensuring that requests for re-use are passed to the Freedom of Information Team and that documents are appropriately licensed before publication.

TRAINING

The Freedom of Information Team can provide advice and assistance to staff on the management of requests for re-use and licensing arrangements.

IMPLEMENTATION

The Freedom of Information Team will be responsible for implementing this policy ensuring that requests for re-use are managed in accordance with the Regulations.

FURTHER INFORMATION

The Re-use of Public Sector Information Regulations 2015
National Archives
UK Government Licensing Framework for Public Sector Information 2013

REVIEW

This Policy will be reviewed after 3 years, or sooner, as required.

APPENDIX 1 – TEMPLATE COPYRIGHT NOTICES AND STATEMENTS UNDER OGL

Online information resources (including website statements)

© Hywel Dda University Local Health Board

This [*insert name of information resource*] is licensed under the Open Government Licence 2.0 OGL - opens in a new tab

When you use this information under the Open Government Licence v2.0, you should include the following attribution: [*Insert name of information resource*, Hywel Dda University Local Health Board, *date of publication*], licensed under the Open Government Licence.

Print publications

This information is licensed under the Open Government Licence v2.0. To view this licence, visit www.nationalarchives.gov.uk/doc/open-government-licence/version/2 OGL - opens in a new tab - or write to the Information Policy Team, The National Archives, Kew, Richmond, Surrey, TW9 4DU.

Any enquiries regarding this publication should be sent to: Hywel Dda University Local Health Board, Corporate Governance Department, Springfield Block, Withybush General Hospital, Fishguard Road, Haverfordwest, SA61 2PZ.

When you use this information under the Open Government Licence v2.0, you should include the following attribution: [*Insert name of information resource*, Hywel Dda University Local Health Board, *date of publication*], licensed under the Open Government Licence - opens in a new tab.

APPENDIX 2 – TEMPLATE COPYRIGHT NOTICES AND STATEMENTS FOR NON-COMMERCIAL GOVERNMENT LICENCE

Online information resources (including website statements)

© Hywel Dda University Local Health Board

This [*insert name of information resource*] is licensed under the Non-Commercial Government Licence - opens in a new tab

When you use this information under the Non-Commercial Government Licence, you should include the following attribution: [*Insert name of information resource*, Hywel Dda University Local Health Board, *date of publication*], licensed under the Non-commercial Government Licence - opens in a new tab.

Print publications

This information is licensed under the Non-Commercial Government Licence. To view this licence, visit http://www.nationalarchives.gov.uk/doc/non-commercial-government-licence/non-commercial-government-licence.htm - opens in a new tab - or write to the Information Policy Team, The National Archives, Kew, Richmond, Surrey, TW9 4DU.

Any enquiries regarding this publication should be sent to: Hywel Dda University Local Health Board, Corporate Governance Department, Springfield Block, Withybush General Hospital, Fishguard Road, Haverfordwest, SA61 2PZ.

When you use this information under the Non-Commercial Government Licence, you should include the following attribution: [*Insert name of information resource*, Hywel Dda University Local Health Board, *date of publication*], licensed under the Non-commercial Government Licence - opens in a new tab.

Network Security Policy

Policy information

Policy number: 282

Classification:
Corporate

Supersedes:
Previous versions

Version number:
3

Date of Equality Impact Assessment:
18/01/2023

Approval information

Sustainable Resources Committee

Date of approval:
28/02/2023

Date made active:
Enter date made active (completion by policy team)

Review date:
Enter review date (normally three years from approval date)

Summary of document:
This policy states the network security requirements for the Health Board

Scope:
This policy applies to all users of the Health Board's digital networks.

To be read in conjunction with:
183 - Information Security Policy

Patient information:

Owning group:
Information Governance Sub-Committee
31/01/2023

Executive Director job title:
Director of Finance

Reviews and updates:
1 – new policy 26.6.2012
2 – revised 29.3.2016
3 – full review

Keywords
Network, security, access, computing

Glossary of terms
None

Keypoints:
To ensure the security, integrity and availability of the Health Board’s digital networks used to support our clinical and administrative services.

Contents

INTRODUCTION

This document defines the computer network security policy for Hywel Dda University Health Board and this policy applies to all business functions and information contained on the network, the physical environment and relevant people who support the network.

It sets out the policy for the protection of the confidentiality, integrity, and availability of the network as well as security responsibilities for ensuring the security of our networks.

The network for the purpose of this policy is a collection of communication equipment such as servers, computers and printers which are connected using our local and wide area networks.

POLICY STATEMENT

The overall Network Security Policy for the Health Board is described below.

The Health Board's information network will be available when needed, can be accessed only by legitimate users, and will contain complete and accurate information. The network must also be able to withstand or recover from threats to its availability, integrity, and confidentiality. To satisfy this the Health Board will undertake the following: -

- Protect all hardware, software, and information assets under its control. This will be achieved by implementing a set of well-balanced technical and non-technical measures.
- Provide both effective and cost-effective protection that is commensurate with the risks to its network assets.
- Implement the Network Security Policy in a consistent, timely and cost-effective manner.
- Where relevant comply with the legal, regulatory, and internal policy requirements.

If a user is found to have breached this policy, they may be subject to the Health Board's disciplinary procedure. – opens in a new tab.

If a user does not understand the implications of this policy or how it may apply to them, they should seek advice from the Health Board's Cyber Security Team.

SCOPE

This policy applies to all networks within Hywel Dda Health Board both wired and wireless used for: -

- The storage, sharing and transmission of non-clinical data and images
- The storage, sharing and transmission of clinical data and images
- Printing or scanning non-clinical or clinical data or images
- The provision of Internet systems for receiving, sending, and storing non-clinical or clinical data or images

AIMS

The aim of this policy is to provide assurance through relevant controls and procedures that our networks are secure and the information on them is kept confidential.

OBJECTIVES

The objectives to be achieved by this policy are: -

- Suitable controls exist to secure our networks.
- Ensure all those accessing and managing the network understand their roles and responsibilities.
- Ensure suitable procedures are in place.

Risk Assessments

Hywel Dda University Health Board will carry out security risk assessment(s) in relation to all aspects of the network that are used to support business processes. The risk assessment will identify the appropriate security countermeasures necessary to protect against possible breaches in confidentiality, integrity, and availability.

Formal risk assessments will be conducted in line with Health Boards Risk Assurance Framework.

Physical and Environmental Security

The following Physical and Environmental security mechanisms will be employed: -

- Network computer equipment will be housed in a controlled and secure environment that is monitored for temperature, humidity, and power supply issues.
- Critical network equipment will be housed in dedicated secure areas protected by physical locks and access control mechanisms.
- The Deputy Digital Director is responsible for ensuring the suitability of these security measures.
- Network equipment will be protected from power supply failures.
- Critical network equipment will be protected by intruder alarms and fire suppression systems.
- Various technical controls will be in place to secure the network including security patching, firewalls, and network admission control.
- All visitors to secure and critical network areas must be authorised by the Infrastructure Operations Manager.
- The Infrastructure Operations Manager will ensure that all relevant digital employees are made aware of procedures for visitors and those visitors are escorted when necessary.

Access Control to the Network

Entry to secure areas housing critical or sensitive network equipment will be restricted to those whose job requires it. A log is maintained of all access to such areas. Ordinarily, such access is supervised but there may be occasions when trusted engineers may require unsupervised access. The Infrastructure Operations Manager will maintain and periodically review a list of those with unsupervised access.

Access to the network will be via secure methods and authentication against our directory service. Remote access to the network will conform to the Health Board’s Mobile Working Policy.

There must be a formal, documented user registration and de-registration procedure for access to the network. All users on the network will have their own individual user identification and password and are ensuring their password is kept confidential. Users must ensure that they protect the network from unauthorised access. They must log off the network when finished working and workstations must be locked if a workstation is left unattended.

User access rights will be immediately removed or reviewed for those users who have left the Health Board or changed jobs.

Any device connecting to the main corporate network must comply with the Health Board's domain membership, anti-virus, and patching procedures.

Clinical devices and Internet of Things (IoT) equipment connecting to the network must be placed in a segregated virtual network to ensure they are protected from the wider network and have controlled access control lists.

Third Party Access to the Network

If external third-party devices require access to the corporate network this will be allowed only once the device has been checked for suitable anti-virus protection and security patching and where possible the free public and patient guest Wi-Fi service should be used ("Hywel Dda Public").

All third-party access to the corporate network must be logged and access to Hywel Dda Health Board's systems must be always audited.

Third party users must have an Active Directory account created for them for the duration of their stay with appropriate permissions and will not use generic accounts or service accounts.

External Network Connections

Any external network connections must only be through approved access methodologies and following the Code of Connection assurance process. These will be managed by the Digital Services department to ensure they can be appropriately secured and monitored.

Any connections not formally approved my put the Health Board at risk by disconnection from the Public Sector Broadband Aggregated Network (PSBA).

Maintenance Agreements

The Deputy Digital Director will ensure that maintenance contracts are maintained and periodically reviewed for all network equipment. All contract details will constitute part of the Digital Department's Configuration Management Database.

Operating Procedures

Documented Security Operating Procedures will be created for the network that reflects this policy and changes to these procedures must be authorised by the Infrastructure Operations Manager.

Change Control

Any changes proposed to the network must consider the security of the network.

Changes must be in line with the Hywel Dda change control procedure and must be reviewed by the Digital Change Advisory Board and approved by the Change Manager.

As part of acceptance testing of all new network systems the Cyber Security Operations Manager will undertake security tests to ensure compliance with this policy.

Security Monitoring

The network will be monitored for potential security breaches and automated alerts will be generated to highlight potential issues.

All potential security breaches must be reported to the Cyber Security Team using the Digital Portal. The Cyber Security Manager is responsible for auditing the network to ensure it meets agreed security standards.

RESPONSIBILITIES

Proper definitions of roles and responsibilities are essential to assure compliance with this Policy. In summary these are: -

Users
The health Board will ensure that all users of the network are provided with the necessary security guidance, awareness, and where appropriate training to discharge their security responsibilities.

All users of the network must be made aware of the contents and implications of the network security policy and that irresponsible or improper actions by users may result in disciplinary actions(s).

All users should safeguard hardware, software and information in their care and prevent the introduction of malicious software onto the organisation's digital systems.

They also have an obligation to report on any suspected or actual breaches in security.

Digital Operations
Digital Operations will be responsible for: -

- Management of our network servers
- Manage our network security including that of the Wireless LAN and any external connections not a part of the PSBA network.
- Be responsible for Disaster Recovery and Business Continuity Plans and for the testing of those plans.
- Provide support to users in gaining access to the network and their use of services provided over the network.
- Periodic penetration testing to ensure the security of our networks.

Deputy Digital Director
Will be responsible for implementing an effective framework for the management of network security and ensure the production of all relevant security documentation, security operating procedures and contingency plans reflecting the requirements of this policy.

Infrastructure Operations Manager
Will be responsible for the implementation of effective security countermeasures contacting the Cyber Security Operations Manager when incidents or alerts have been reported that may affect the security of the Health Board's networks.

Responsible for ensuring all network components will have effective configuration management procedures in place in line with the Hywel Dda Configuration Management Procedure.

Cyber Security Operations Manager
The Cyber Security Operations Manager will be responsible for: -

- Will be responsible for the mandating of effective security countermeasures.
- Acting as a central point of contact for cyber security within the organisation.
- Assisting in the updating of this policy and related policies for approval by the Information Governance Sub-Committee.
- Produce organisational standards, procedures, and guidance on cyber security matters.
- Liaise with external organisations on cyber security matters, including representing the organisation on the national Operational Security Service Management Board and associated sub-groups managed by Digital Health & Care Wales (DHCW).
- Advising the Deputy Digital Director on cyber security breaches and recommended actions.
- Encouraging, monitoring, and checking compliance with this policy.
- Promoting awareness and providing guidance on this policy.
- Creating, maintaining, and giving guidance on and overseeing the implementation of network security.

Line Manager's Responsibilities
Ensuring all employees are made aware of their security responsibilities as indicated in this policy.

TRAINING

All staff will be required to have appropriate information governance training which will include guidance on network security.

IMPLEMENTATION

All staff must adhere to this policy and failure to follow these policies may lead to disciplinary action being taken. This policy will be disseminated through global email and through periodic Information Governance training.

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

Disposal of Digital Assets Policy

Policy information

Policy number: 319

Classification:
Corporate

Supersedes:
Previous versions

Version number:
3

Date of Equality Impact Assessment:
18/01/2023

Approval information

Approved by:
Sustainable resource Committee
Date of approval:
Enter approval date

Date made active:
Enter date made active (completion by policy team)

Review date:
Enter review date (normally three years from approval date)

Summary of document:
The purpose of this policy is to outline the steps that need to be taken to ensure that all digital equipment is disposed of in the appropriate manner in terms of confidentiality and Waste Electrical and Electronic Equipment (WEEE) legislation and regulations.

Scope:
This policy covers the disposal of all digital equipment in particular the disposal of any computer related equipment computer media, audio tapes and removable media.

The policy applies to all materials which contain confidential information for example: paper records, photographs, computer media and audio tapes

To be read in conjunction with:

183 - Information Security Policy
275 - Secure Transfer of Personal Information
494 - All Wales E-mail Policy
281 - Mobile Working Policy
282 - ICT Security Policy

Patient information:
Not applicable

Owning group:
IGSC
31/01/2023

Executive Director job title:
Director of Finance

Reviews and updates:
1 – new policy 28.1.2023
2 – revised policy 26.6.2018
3 – revised policy 18.1.2023

Keywords
Information, Personal Data, Personal Information, Informatics, Transfer of Information, Mobile Working, Screensaver, Information Technology, Acceptable Use Equipment, Information Asset, ICT Asset, Digital

Glossary of terms
ICT – Information and Communication Technology
PC – Personal Computer
WEEE – Waste Electrical and Electronic Equipment
PAT – Portable Appliance Test

Keypoints:
Please summarise key points of the document

Contents

1. Introduction

The Health Board has a duty of care to ensure that the disposal of digital equipment, especially those with disks or removable media containing information and data is undertaken with due care and attention. If any files contain personal or other sensitive or confidential data, then special care must be taken to ensure that this information cannot be accessed by anyone. There have been high profile cases where this care has not been adequately exercised; the Data Protection Act/General Data Protection Regulations 2018 or any subsequent legislation to the same effect requires that these issues are given serious consideration.

In addition, there are obligations that must be met for any person receiving the equipment in relation to its electrical safety that may represent a continuing liability or environmental implications in disposing of computer equipment.

2. Scope

This policy covers the disposal of digital equipment, in particular: -

- The disposal of any computer related equipment. This includes Personal Computer's (desktop or laptop), mobile devices (tablets, smartphones), mobile phones, printers, scanners, and any other peripheral devices such as memory sticks.
- The policy applies to all materials which contain confidential information for example computer media and audio tapes.

This policy links to the Health Boards policies covering - Confidentiality, Data Protection, Records Management, and Information Security. Together these policies form an integral part of the Health Boards approach to Information Governance and Cyber Security.

3. Aim

The aim of this policy is to outline the steps that need to be taken to ensure that all digital equipment is disposed of in the appropriate manner in terms of confidentiality and Waste Electrical and Electronic Equipment (WEEE) legislation and regulations.

4. Objectives

The aims of this policy will be achieved through: -

- Effective communication with Health Board employees so they are aware of the procedures to follow.
- Digital department procedures to cover the effective disposal of equipment.

5. Definitions

5.1 Hardware

By its own nature digital equipment is constantly evolving and this can therefore become a very broad category making it impossible to list every single item or group of items within this policy document; however physical assets can be summarised as follows: -

- A Personal Computer (PC) or Workstation
- A Laptop or Tablet Computer including Apple and Android devices
- Infrastructure Components (servers and storage systems)
- Backup Devices and Tapes
- A Local or Network Printer
- A Local or Network Scanner
- A USB Removable Device or Portable Hard Disk
- A Video Camera
- A Smart Phone
- Other Network Devices (such as a switch, router, or firewall)

5.2 Software

To list all applications in use by Hywel Dda University Health Board would be inappropriate and to list all instances of acceptable use associated with each application would be a never-ending task, however software can be summarised as follows: -

- Desktop Software – all applications and related data loaded onto a Desktop or Laptop computer.
- Server Software – all applications and related data loaded onto a server.
- Hosted Solution – all applications and related data (owned by Hywel Dda UHB) hosted off site either in the National Data Centres or in a third-party provided Data Centres.
- Software as a Service – all applications and related data hosted in public cloud services such as Microsoft Azure and Amazon Web Services.

5.3 Electronic Data

Electronic Data can be summarised as follows: -

- CD’s / DVD’s
- Backup Tapes
- Memory Sticks
- Videos

6. Disposal of Digital Equipment Procedure

The Digital Operations department will assess whether equipment is redundant for its original use. This will be following discussion with the system owner and/or departmental manager. The disposal of Digital equipment procedures will cover all Health Board Equipment.

6.1 Equipment Disposal

Upon request an assessment will be made on the equipment which will be via the Digital Portal or by a digital engineer as part of a related job. Where possible equipment will be redeployed throughout the Health Board, however if there is a need to condemn a piece of equipment this may not always be decided there and then as often equipment is returned to the engineers who then further diagnose the problem and if possible, investigate the cost of repair.

Regardless of the path the equipment has taken there are only three reasons for disposing of equipment, they are as follows: -

- Redundant (fully functioning / not functioning)

- Broken (reasons known / reasons unknown)
- End of Life / Support and hence a Cyber Security Risk

Generally, Digital equipment will reach its natural end of life when it is between five and seven years old, however there are likely to be some exceptional circumstances where equipment becomes redundant mid-term due to specific machines (PCs and Laptops) needing to run specialised software where the specification of the machines has been exceeded.

In all instances an assessment (triage) must be undertaken to determine the validity of disposal of the equipment and to ensure authorisation is granted for the removal of the equipment from the asset system.

Where equipment is determined to be redundant an assessment will be made to determine whether the equipment can be used for digital inclusion

6.2 Redundant Equipment

This is equipment that is no longer fit for purpose and is incapable of running the standard software deployed at the time. Typically, this will be the equipment that is five years of age or older. Redundant equipment that is not working will automatically qualify as scrap.

6.3 Broken Equipment

This is obviously equipment that is not working and is out of warranty. Broken equipment that cannot be repaired will automatically qualify as scrap. It is also possible that broken equipment that can be repaired will qualify as scrap when the cost of repair is greater than, equal to or just less than the cost of replacement. It may also be where the cost of repair is financially inappropriate, such as equipment which is nearing five years old is therefore due to be replaced soon.

6.4 End of Life

This is equipment which may be functioning correctly but has reached its end of life and is no longer supported by the manufacturer. Such equipment may no longer receive security updates or pose a risk to the Digital Operations of the Health Board. In such circumstances the equipment may be disposed of and replaced as required from available funds.

6.5 Disposal Method

In all instances all Health Board owned equipment will disposed via the Keep Wales Tidy Scheme. Appendix A outlines their procedures, and a contract exists between Keep Wales Tidy and Hywel Dda UHB that outlines their responsibility as a data processor for any data remaining on storage devices.

However, for redundant functioning equipment owned by the UHB, it would be appropriate for this equipment to be reused in another suitable scenario or broken down as spares for other units that may yet have a small element of life within them. If no spares can be claimed from the unit, then it will automatically be scrapped.

Under absolutely no circumstances can any computer equipment be directly sold (or given) to any individual or other organisation. The procedure contained within Appendix A must be followed for all equipment and under no circumstances should any computer equipment be disposed of via undesignated skips, recycling centres or landfill.

All equipment disposals will be undertaken within current and future Waste Electrical Equipment (WEEE) legislation. However, Digital Services reserves the right to review this arrangement, with prior notification, as more equipment falls within the WEEE directive.

When re-deploying equipment, the Digital Operations Department will, if required, arrange for all equipment that does not have an up-to-date Portable Appliance Test (PAT) certificate to be tested prior to redeployment by the Estates Department.

7. Digital Inclusion

Where equipment is determined to be redundant an assessment will be made to determine whether the equipment can be used to support the Health Board's digital inclusion agenda. If so, the equipment will be securely wiped and provided for use by the digital inclusion team in our local communities to help improve digital accessibility and digital skills.

8. Media Destruction

Media, which is no longer required (or has passed its effective reuse period), should be dealt with as outlined below.

All media including CD-ROM's, DVD's, Hard Drives, USB memory keys and tapes will be dealt with by Keep Wales Tidy and will be shredded and therefore destroyed using industry standard equipment.

9. Incidents

It is the responsibility of ward / department / unit managers to report incidents. Advice and guidance regarding confidential waste or record storage can be sought from the Head of Medical Records.

The Health Boards Risk Incident Reporting Procedures, DATIX, and security incidents must be followed, and the investigation / action accurately documented.

10. Responsibilities

Proper definitions of roles and responsibilities are essential to assure compliance with this Policy. In summary these are.

10.1 Executive Directors

Executive Directors are responsible for the management of risk within their control and in particular are responsible for ensuring their staff are aware of the risks identified within this policy and take responsible action to mitigate them.

Executive Directors must: -

- Ensure procedures are in place within their sphere of responsibility to enable the identification and assessment of risks, including staff training and awareness to mitigate the risks.

10.2 Digital Services

Digital Services are responsible for: -

- For assessing whether the equipment could be suitably redeployed in another department or used for digital inclusion.
- Before disposal Digital Services will confirm with the user that no data is held locally which needs to be retained.
- In the event of such data being discovered then the data will be copied for safe storage and security onto network file storage.
- The equipment maybe dismantled and used for spare part purposes. In this case the hard disk will be erased to a complete and unrecoverable state.
- If any equipment is un-repairable or has no other useful life it will be disposed of, and the hard disk will be physically destroyed.
- After disposal Digital Services will record disposal on the relevant asset register, including the reason and method of disposal and which technician undertook the task.
- Physical disposal of assets must adhere to WEEE Regulations and ensure that disposal is both secure and environmentally responsible.

10.3 Line Managers

Managers are responsible for ensuring that all their staff have read and understood this policy. They must ensure that staff work in compliance with this policy and other appropriate legislation and Health Board policies.

Inform the Digital Service Desk of any digital equipment which require disposal.

10.4 All Staff

All staff, permanent, temporary, or contracted, must be aware of their own individual responsibilities for the maintenance of confidentiality, data protection, and information security management and information quality and understand they are required to comply with this policy. Failure to comply with this policy may result in disciplinary action being taken.

Staff must: -

- Confirm to their line manager that they understand this policy and their responsibility for the protection and security of the Health Board information they access.
- Be responsible for ensuring that unauthorised individuals are not able to see any confidential Health Board information or access Health Board systems.
- Should staff become aware that a breach of confidential information has taken place the Health Boards Information Governance incident response process should be followed immediately.

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

Consumer Device Policy (Smartphones / Tablets)

Policy information

Policy number: 422

Classification:
Corporate

Supersedes:
Previous versions

Version number:
3

Date of Equality Impact Assessment:
19/01/2023

Approval information

Sustainable Resources Committee
Detail which group/committee has approved this document
Date of approval:
Enter approval date

Date made active:
Enter date made active (completion by policy team)

Review date:
Enter review date (normally three years from approval date)

Summary of document:
The policy relates to any staff member (or manages a staff member) who uses the Choose Your Own Device (COYD) or Bring Your Own Device (BYOD) scheme in Hywel Dda University Health Board

Scope:
All staff that are part of the scheme or manage staff that are part of the scheme needs to adhere to this policy (i.e., users of smartphones and tablets for Health Board business).

To be read in conjunction with:
183 - Information Security Policy
281 - Mobile Working Policy
280 - Email Policy
108 - Internet Access and Usage Policy

Patient information:

Owning group:
IGSC
31/01/2023

Executive Director job title:
Director of Finance

Reviews and updates:
1 – new policy 28.4.2015
2 – updated 28.08.2018
3 – full review

Keywords
Information, Digital, Mobile Working, CYOD, BYOD, Tablet, Smartphone, IT, ICT, Apple, Andriod

Glossary of terms

MDM	Mobile Device Management, software that provides features that enables a device to be used in a secure manner.
CYOD	Choose Your Own Device
BYOD	Bring Your Own Device
GDPR	General Data Protection Regulations
ICT	Information & Communication Technologies
Jail Broken	Apple device that has been modified to install apps and make configuration changes not authorised by Apple.
Rooted	Android device where access has been given to modify the software on the device to make unauthorised changes.
WPAS	Welsh Patient Administration System.

Keypoints:

Please summarise key points of the document

Contents

1. Introduction

The Health Board has the goal to enable greater flexibility to allow the use of Smartphones and Tablets to access health board data and applications. These could be both corporately owned devices (Choose Your Own Device – CYOD) and personally owned devices (Bring Your Own Device – BYOD).

This policy will therefore use the terms BYOD and CYOD throughout and are clarified below: -

- BYOD – refers to Bring Your Own Device and is the scenario where a health board employee chooses to use their own smartphone or tablet to access health board information and systems.
- CYOD – refers to Choose Your Own Device and is the scenario where the health board has purchased a smartphone or tablet (non-Microsoft) for the use by the employee whilst undertaking Health Board business.

This will allow you to access: -

- Your work emails
- Your work calendars
- Your work contacts
- A secure work web browser (Access to internal web sites)
- Access to OneDrive
- Microsoft Teams
- Other O365 applications (e.g. Yammer)
- Citrix based applications
- Public applications available in App Stores which maybe of relevant to your role
- Private applications which might be developed in the future by Hywel Dda and/or its partners.

The use of portable devices and mobile platforms is now commonplace in our personal lives and during the pandemic the use of these technologies in the NHS has grown considerably. The adoption of tablets and smartphones has the potential to deliver many benefits to health board staff especially those which are mobile.

This mobile device use however poses a substantial risk in that devices may be lost, damaged, or stolen, potentially resulting in loss or inappropriate disclosure of data. When using mobile devices, the risks of working in an unprotected environment must be considered and mitigated where possible using appropriate security systems and the procedures outlined in this policy.

It is noted that some staff may use their own device for work business outside of this scheme, all staff are reminded that it is not permitted to use consumer applications such as WhatsApp, Dropbox and Snapchat etc. for the transfer of Person Identifiable Information (PII) or confidential Health Board information. These activities could result in a breach of the Data Protection Act / General Data Protection Regulations or any subsequent legislation to the same effect and enforcement activities against the Health Board and disciplinary procedures against the individual.

2. Policy Statement

To utilise any of these services to access corporate data and applications, all users of the service will need to understand the following terms and conditions. There is no registration required for the BYOD scheme and it is available to all staff once they have setup Microsoft Multi-Factor Authentication (MFA).

All users of this service will fully comply with corporate policies on appropriate mobile phone, e-mail, and internet usage. These can be found on the Health Board's Intranet or Internet site.

All users of the service must familiarise themselves with the corporate Information Governance policies and ensure they are adhered to.

- All staff will need to register for Microsoft Multi-Factor authentication and either use the app on the smartphone / tablet, receive SMS messages or automated phone calls.
- All users of this service will need to adhere to the security policies of the health board ensuring safe access to corporate data and applications.
- A security application will provide the health board with the ability to lock down and secure the device such as enforcing a password and encrypting the device on CYOD devices. No applications are installed on personal devices using the BYOD scheme.
- Policies enforced on your device are aimed at managing corporate data and applications, your personal information on BYOD devices will not be affected.
- Policies on CYOD which are corporately owned will be aimed at managing the device and whilst personal information can be stored on these devices it is done so at your own risk and digital will not be able to recover any personal information lost.
- You will keep your password / passcode secret and not allow anybody else to access the information. Where possible use biometric authentication such as your thumb print where the device supports this.
- Should you lose or have your BYOD device stolen you will need to report this to Digital immediately so that we can revoke access to corporate data remotely. It will be the user's responsibility to report the theft of the device to the authorities.
- Should you lose or have your CYOD device stolen you will need to report this to digital immediately so that we can wipe the device remotely. The health board will then report the theft of the device to the relevant individuals in the health board.
- In the unlikely event that personal data on the BYOD device is affected or lost, HDUHB will not be held responsible or liable for any damages or compensation. Any personal data on the CYOD device will be lost if the device is stolen or lost as the device will be wiped completely.
- You accept that the HDUHB will not be liable for any charges relating to the handset hardware, tariff, insurance, call, or data charges incurred when using BYOD devices.
- You accept that the HDUHB offers no support or maintenance for the phone/tablet and it is your responsibility to maintain or repair it as and when required for BYOD devices. CYOD will be fully supported by the Digital Service Desk.
- No cloud services should be used to store health board data such as Apple's iCloud, GoogleDrive and Dropbox. Separate services are available to enable data to be shared with third parties or for home access. Please contact the Digital Service Desk to access these.

Failure to adhere to these protocols will result in the withdrawal of the service.

3. Scope

All staff that are part of the scheme or manage staff that are part of the scheme needs to adhere to this policy.

4. Aim

The aims of this policy are:

- To ensure that the Health Board complies with its legal obligations against the Data Protection Act including UK GDPR (2018) and the Network & Information System Regulations (2018).
- To promote the safe and secure use of mobile equipment in support of the clinical and operational work of Hywel Dda University Health Board.
- To provide a secure working environment for personnel working remotely on corporate / public wireless networks and 4G/5G mobile connections.
- To ensure that resources provided to staff are not misused.
- To ensure that the security of mobile systems and the information they contain is not compromised in any way.

The policy applies to all full-time and part-time employees of the Health Board, Independent Members, contracted third parties (including agency staff), students/trainees, bank staff, staff on secondment and other staff on placement with Hywel Dda University.

5. Objectives

The Health Board's approved method of enabling the required security is through Microsoft Intune which is part of the Microsoft 365 suite of productivity tools.

Mobile phones and similar devices used for application / data access must have a security PIN number, passcode enabled, or biometric security such as fingerprint / facial recognition.

Patient identifiable information (PII) or other confidential Health Board data must not be stored permanently on mobile devices or media. Where possible information should be transferred to the Health Board's systems and deleted from the device as soon as possible.

All devices will be enrolled onto the system using the vendor's current enterprise deployment method such as Apple Deployment Enrolment Programme or Android Enterprise.

6. Service Policy

6.1 <u>Applying for the Service</u>

Please use the online form to access the CYOD scheme. Your manager will need to approve this spend and provide Digital with a cost code.

All users have automatic access to the BYOD scheme and it is personal preference whether a member of staff chooses to use or not.

6.2 Acceptable Use

- The Health Board defines acceptable business use as activities that directly or indirectly support the services within HDUHB.
- Acceptable use for Internet and E-mail use is available in the relevant existing policies.
- For BYOD the Health Board defines acceptable personal use on company time as reasonable and limited personal communication. Policies will ensure Health Board data cannot be shared outside of corporate apps such as Outlook.
- CYOD devices may not be used at any time to: -
  - Store or transmit illicit materials.
  - Harass others, particularly on the grounds of any protected characteristic as defined in the Equality Act 2010.
  - Engage in outside business activities.
- A list of applications will be maintained and these maybe pushed directly to the device on registration.
- CYOD will have policies applied to ensure a blacklist of applications are maintained so that these cannot be used on health board devices.
- Employees may use their mobile device to access the following Health Board resources: email, calendars, contacts, documents, websites, Microsoft 365 applications and other approved applications.
- HDUHB has a zero-tolerance policy for texting or emailing while driving.

6.3 Devices and Support

- Smartphone's including iPhone and Android are allowed to use this service.
- Tablets including iPad, Windows and Android are allowed to use this service.
- Health Board app issues are supported by Digital Services; employees should contact the device manufacturer or their carrier for operating system or hardware-related issues for BYOD devices.
- NO "jail broken" or rooted devices are allowed and will be automatically rejected and will not connect to the service.

After a licence is purchased and a user account is setup on the system you will be sent instructions on how to add your device to the service.

- Microsoft Outlook
  - Email – you will have access to work email and lookup users from the directory.
  - Calender – access to your work appointments
- Task Management
  - Microsoft ToDo and Microsoft Planner
- Microsoft Teams
- Secure web browser (Microsoft Edge) – this will allow access to work SharePoint sites e.g., the Intranet.
- Access to work files and the ability to create docs (using Word, PowerPoint, Excel etc.).
- Please note there are limitations with the degree of functionality of internal applications. This relates to how the application has been designed to function in a traditional PC/Laptop environment with larger screens. If you still wish to access applications via Citrix (HDDVAPPS)

such as WPAS, you can do but in the knowledge that full functionality may not be available and navigation may be difficult.

7. Responsibilities

7.1 Reimbursement

- The Health Board will not reimburse the employee for a percentage of the cost of the BYOD device.
- The Health Board will not reimburse the employee for data charges on BYOD devices.

7.2 Security

- For BOYD devices the following is employed:
  - conditional access policies are in place to protect Health Board data
  - staff must use Microsoft Authenticator to access Health Board data
- For COYD devices the following is employed:
  - To prevent unauthorized access, devices must be password protected using the features of the device.
  - The device will lock itself if it's idle for five minutes.
  - After 11 failed login attempts, the device will lock. Contact the Digital Service Desk to regain access.
  - The minimum password length is 6 characters and must be complex.
  - Password expiry is 90 days.
- Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the service and are blocked by default.
- Employees are automatically prevented from downloading, installing, and using any app that does not appear on Health Boards list of approved apps on CYOD devices.
- For CYOD the device may be remotely wiped if 1) the device is lost, 2) the employee terminates their employment, 3) ICT detects a data or policy breach, a virus or similar threat to the security of the Health Boards data and technology infrastructure.
- For BYOD the users account will be removed from the license group therefore removing access to health board data and applications, personal data will not be affected.

7.3 Data Security

The device is fully encrypted and all data in transit to and from the device is fully encrypted. The device integrity and authenticity are continually checked for any security risks and immediately blocked if detected.

Should you lose your device you must inform the Digital Service Desk immediately and we will remove access. This will NOT interfere with any personal data of the device for BYOD devices. If you forget your password after 10 attempts, it will delete the corporate device and all work data within it. Digital Services do not have sight of the password and cannot recover it

7.4 Risk / Liabilities / Disclaimers

- The Health Board can accept no liability for the loss of any private information held on a BYOD or CYOD device such as documents and photos.
- While Digital Services will take every precaution to prevent the employee's personal data from being lost it is the employee's responsibility to take additional precautions, such as backing up your personal device using the iCloud for example.
- The health board reserves the right to disconnect devices or disable services without notification.
- Lost or stolen devices must be reported to the Health Board immediately. Employees are responsible for notifying their mobile carrier immediately upon loss of a BYOD device. A self-service portal will also be available for employees to disable their own devices if required.
- The employee is expected to always use their device in an ethical manner and adhere to the Health Boards acceptable use policy.
- The employee is personally liable for all costs associated with their BYOD device.
- The employee assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.
- HDUHB reserves the right to take appropriate disciplinary action for noncompliance with this policy.

8. Roles & Responsibilities

8.1 Directors

Directors are responsible for the management of information risk within their control and in particular are responsible for ensuring their staff are aware of the information risks identified within this policy and take responsible action to mitigate them.

Directors must: -

- Ensure procedures are in place within their sphere of responsibility to enable the identification and assessment of information risks of mobile computing and the implementation of control measures, including staff training and awareness to mitigate the risks.

8.2 Line Managers

Managers are responsible for ensuring that all their staff have read and understood this policy prior to authorising mobile computing arrangements. They must ensure that staff work in compliance with this policy and other appropriate legislation and Health Board policies. This includes the responsibility for ensuring that risk assessments are or have been carried out and that suitable controls are put in place and remain in place to either eradicate or minimise any identified risks to the security of Health Board information.

Line managers **must** inform the Digital Service Desk when a member of staff leaves the Health Board or changes role.

8.3 All Staff

All staff, whether permanent, temporary, or contracted, must be aware of their own individual responsibilities for the maintenance of confidentiality, data protection, and information security management and information quality and understand they are required to comply with this policy. Failure to comply with this policy may result in disciplinary action being taken, which may result in the withdrawal of authorisation and the service.

Staff shall inform their manager if they have any concerns about any issues that would constitute an information risk. This covers not only risks to resources or confidentiality of data, but also personal risk, risk to others and risk to the Health Boards reputation.

Staff need to confirm to their line manager that they understand this policy and their responsibility for the protection and security of the Health Board information they access.

Health Board information must only be used for Health Board related purposes in connection with Health Board work.

Staff are responsible for ensuring that unauthorised individuals are not able to see any confidential Health Board information or access Health Board systems.

Users of information will: -

- Keep usage to a minimum in public areas.
- Only use information off-site/at home for work related purposes.
- Ensure security of information within the home.
- Not send patient identifiable or confidential data to home (internet) e-mail addresses.

8.4 Digital Services

- Fulfil requests to access the scheme.
- Provide advice and direction on the use of this scheme.
- Ensure adequate security controls are implemented in support of this policy.
- Provide reports on usage of the scheme and retire inactive devices from the service.