COMMITTEE UPDATE REPORT/ ADRODDIAD DIWEDDARU'R

INFORMATION GOVERNANCE SUB-COMMITTEE COMMITTEE / IS-BWYLLGOR LLYWODRAETHU GWYBODAETH

Date of last meeting/ Dyddiad y cyfarfod diwethaf: 23 June 2026

Quoracy/ Cworwm: Not Quorate

Report by/ Adroddiad gan: Anthony Tracey, Digital Director

KEY DISCUSSION POINTS AND MATTERS FROM THE DISCUSSION AT THE MEETING/ PWYNTIAU TRAFOD ALLWEDDOL A MATERION I'W HUWCHGYFEIRIO O'R DRAFODAETH YN Y CYFARFOD:

Alert[1] (may require discussion)/ **Rhybuddio** (efallai y bydd angen trafodaeth)

The Information Governance Sub-Committee wish to note that there are no matters to **alert** members of the Digital Data and Innovation Committee (DDIC).

Advise[2] (to monitor)/ **Cynghori** (i fonitro)

The Information Governance Sub-Committee wishes to advise members of the DDIC that:

Overall compliance with mandatory Information Governance, Records Management and Cyber Security training has improved from 77% to 84.87%; however, the Health Board remains below the national target of 85%. Medical and Dental staff continue to be the lowest compliant staff group despite targeted interventions. The Sub-Committee will continue to monitor compliance and provide further updates.

The Welsh Government Records Management Code of Practice remains under review. Internal organisational changes within Welsh Government have delayed publication of the final version. Health Board policies have therefore been developed against the current interim version and may require review once the final national document is issued.

Due to IGSC not being quorate, the Sub-Committee scrutinised and supported the progression of the following policies and strategies to DDIC for approval:

- Health Records Management Strategy.
- Health Records Management Policy.
- Health Records Retention Policy.
- IT Procurement Policy.
- Acceptable Use of Digital Services Policy.

---

[1] *There is a lack of confidence that any action in place is sufficient to address the issue satisfactorily and/or within the scope of the operational team or executive to resolve. Engagement, action or intervention required.*
[2] *There are areas of concern where assurance has been taken on actions in place but requires close monitoring. An early warning of an emerging and potentially serious concern*.

- Information Quality Assurance Policy.

The Sub-Committee was assured that these documents had undergone organisational consultation and relevant amendments had been incorporated.

Assure[3] (to note)/ Sicrhau (i nodi)

The Information Governance Sub-Committee wishes to assure members of the DDIC that:

Information Governance Performance
The Sub-Committee received assurance through regular reports covering:
- Information Governance (IG) activity and performance.
- Data Protection Impact Assessments (DPIAs).
- Information Asset Register reviews.
- IG audit programme.
- Caldicott Guardian activity.
- IG compliance monitoring.

Clinical Coding Performance
Clinical Coding achieved:
- 99.3% completeness for 2025/26.
- Performance above the national completeness target.
- Continued achievement of coding accuracy standards.

The Sub-Committee recognised the significant achievement by the Clinical Coding Team and received assurance regarding ongoing improvement activity.

National and Local Governance Groups
The Sub-Committee received updates from:
- Information Governance Managers Advisory Group (IGMAG).
- Health Records Managers Advisory Group (HRMAG).
- Caldicott Guardian Group.
- Information Asset Owners Group.
- Cyber Security Assurance Group.

The updates provided assurance regarding ongoing governance arrangements, records management developments and cyber security activities across Wales.

Review of Risks/ Adolygiad o Risgiau

Not Applicable

Sharing of learning/ Rhannu dysgu

[3] *There is confidence that actions are robust and will be sufficient to address the issue or generally operating effectively. Routine monitoring.*

The Sub-Committee recommends sharing the following learning across the Health Board:

- Artificial Intelligence (AI) assisted phishing attacks are becoming increasingly sophisticated and may closely resemble legitimate communications. Staff should remain vigilant and report suspicious emails immediately.
- Cyber awareness campaigns and phishing reporting continue to improve organisational resilience.
- IG audit activity will now include questions relating to the use of AI in both clinical and administrative settings.
- Information Asset Registers have been amended to include a specific field relating to AI usage to strengthen oversight of emerging technologies.

Recommendation/ Argymhelliad

The DDIC is asked to:

- **Approve** the
- **Note** the items that the Sub-Committee is advising them of.
- **Receive Assurance** from the e items that the Sub-Committee is assuring them of.

Date of next meeting/ Dyddiad y cyfarfod nesaf: 28 July 2026

Agenda, papers and minutes are available on request.

Health Records Management Strategy

DRAFT

Policy information

Policy number: 191
Classification: Corporate
Supersedes: Previous Version
Version number: 5
Date of Equality Impact Assessment:

Approval information

Approved by:
Date of approval:
Date made active:
Review date:

Summary of document:
This strategy addresses the principles and practice for managing health records within Hywel Dda University Health Board**.**

Scope:
This strategy has been written to provide an overarching framework of professional advice and guidance for all Hywel Dda University Health Board staff, to ensure compliance with all legal requirements for the maintenance, storage and provision and security of records. The strategy defines standards for improving the quality, availability and effectiveness of records management activities. This strategy 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:
[192] – Health Records Management Policy – opens in a new tab
[193] – Retention and Destruction of Records Policy – opens in a new tab
[249] – Access to Health Records Policy – opens in a new tab
[172] – Confidentiality Policy – opens in a new tab
[836] – All Wales Information Governance Policy – opens in a new tab
[837] – All Wales Information Security Policy – opens in a new tab
[347] – Corporate Records Management Policy – opens in a new tab

Patient information:

Owning group: IGSC
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
5 – full review

Keywords
Health Records, Records Management

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”.

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 individual”. Anything that contains information that has been created or gathered as a result of any aspect of the work of NHS employees.

Data Protection Act 2018 - The Data Protection Act 2018 is a United Kingdom Act of Parliament which updates data protection laws in the UK. It is a national law which complements the European Union's General Data Protection Regulation and replaces the Data Protection Act 1998.

Information Security - The protection of information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Public Records Act 1958 - The Public Records Act 1958 is an Act of the Parliament of the United Kingdom forming the main legislation governing public records in the United Kingdom.

DRAFT

Contents

Policy information..... 1

Approval information 1
Introduction 4
Scope 4
Aim 5
Objectives 5
Responsibility and Accountability 6
Standards of Records Management 6
Training 9

DRAFT

Introduction

This strategy addresses the principles and practice for managing health records within Hywel Dda University Health Board (HDUHB). The organisation uses a hybrid of computer and paper records to support patient processes and patient care and the strategy establishes how all patient records will be managed. Health Records management is about the proper content, control, security, storage and ultimate destruction of records. Records created and held by HDUHB as part of its functions, are public records under the Public Records Act 1958. The Public Records Act 1958 requires that there is a systematic and planned approach to the management of records within an organisation.

Effective management of healthcare services can only be achieved if there are appropriate health records management policies and processes in place. Health records management falls within the remit of the Health Records service. The aim of the health records service is to ensure that procedures are in place to bring together the health professional and accurate, relevant patient information/documentation at the correct time and place, to support patient care. Records management is a key component of the health records service and an expert professional field. The correct creation, management and maintenance of the health record provides the communication tool between the health professional and the patient.

The strategy details the aims, aspirations and targets of what we want to achieve with our health records management programmes and provides direction within the organisation. The Board, Executive Team, senior management and all who work for the organisation have responsibilities to ensure that information is handled appropriately and functions are performed in line with the required records management standards, ensuring the accuracy and availability of records for patient care.

The strategy will be updated as required to include future developments such as updated health records management guidance, to reflect technological changes such as the introduction of scanning services and the possible migration to an electronic patient record or changes in legislation.

This strategy is based on the requirements of the Records Management Code of Practice for Health and Social Care. This document covers management of all types of NHS health records throughout their lifecycle, from their creation and use, to their final disposal. This strategy should be read in conjunction with other HDUHB policies e.g. HDUHB Health Records Management Policy, Retention and Destruction Policy, Access to Health Records Policy etc and also the Data Protection Act.

Scope

This strategy has been written to provide an overarching framework of professional advice and guidance for all Hywel Dda University Health Board staff, to ensure compliance with all legal requirements for the maintenance, storage and provision and security of records. The strategy defines standards for improving the quality, availability and effectiveness of records management activities. The strategy clearly identifies all critical elements of effective records management and identifies key individuals within HDUHB and their obligation to ensure records are managed in accordance with legal requirements and both national and local standards.

This strategy relates to all clinical operational records held in any format by the HDUHB. Within the strategy the terms 'Health Record', 'Patient Record' and 'Case record' are synonymous and include:

- Records of patients treated by HDUHB including health and care records
- Records of private patients treated on NHS premises
- Records of patients treated on behalf of the NHS in the private healthcare sector

Health Records may be held in many formats, for example:

- Personal health records (electronic, microfilmed, scanned images & paper based)
- Theatre Registers and all other registers that may be kept
- X-ray and imaging reports, output and images
- Photographs, slides and any digital images
- Audio and video tapes, cassettes
- Digitised images/Digital Records (scanned)
- Emails
- Text messages (SMS)

This list is not exhaustive.

This strategy applies to all permanent, temporary or contracted staff employed by Hywel Dda University Health Board (including Executive and Non – Executive Directors).

Aim

The aim of the Health Records Management Strategy is to provide an overarching framework for current records management activities and initiatives, as well as any new ones recommended in the future. The Strategy will ensure there is:

- a systematic and planned approach to health records management covering health records from creation to disposal.
- efficiency and best value for money through improvements in the quality and flow of information, and greater co-ordination of health records and storage systems.
- compliance and delivery with statutory and legislative requirements.
- awareness of the importance of health records management and the need for responsibility and accountability at all levels.
- appropriate archiving of non-current health records.
- improve data quality to ensure accuracy and consistency.
- provide assurance around governance, confidentiality and data protection.

Objectives

The objectives of the strategy is to define an agreed approach for improving the quality, availability and effective use of records in the HDUHB and provide a strategic framework for all records management processes and procedures. This will enable overall coordination of all records management activities and ensure alignment with the HDUHB's business model. The key objectives associated with the strategy is improved patient safety and quality of care with the deliverable benefits being:

- the improved maintenance of the history of patient care and better communication and information sharing between care providers and patients
- greater efficiencies from the improved management of clinical functions
- reduced duplication of effort
- greater accountability and corporate governance
- reduction in litigation costs through improved patient safety and ability to defend against claims
- compliance with legislation and best practice record standards.

Responsibility and Accountability

There should be a clear chain of management, accountability and responsibility for all records created and utilised within the HHDUHB. The Chief Executive has overall accountability for ensuring that records management operates appropriately and a duty to make arrangements for the adequate resourcing and safekeeping of all HDUHB records. The Chief Executive may delegate responsibility for records management arrangements within the organisation to a designated Executive, who is responsible for ensuring appropriate mechanisms are in place to support service delivery and continuity. The Medical Director has particular responsibilities for patient records as the Calidcott Guardian of the HDUHB.

The health records manager has strategic and operational accountability for the creation, retrieval, storage, archiving and disposal of all health records within the HDUHB. The HDUHB has in place a documented 191 - Health Records Management Policy and 193 - Retention and Destruction Policy – opens in a new tab - and detailed documented procedures, to support the life span of a health record from creation to disposal.

All staff should be aware of their individual responsibility and accountability in the creation, management, storage and access to all HDUHB records. More detailed information in regards specific HDUHB roles and responsibilities can be found in the 191 - Health Records Management Policy – opens in a new tab.

Standards of Records Management

The Health Records Management Strategy compromises of the following key elements.

Record Quality

The Health Records Management Strategy aims to provide assurance that policies and procedures are in place to ensure that the patient and health professional, together with accurate, relevant, reliable patient information and documentation are available at the correct time and place to support effective and safe patient care. HDUHB records should be accurate and complete, in order to facilitate audit and fulfil the HDUHB's responsibilities and protect its legal and other rights.

Records should show proof of their validity and authenticity so that any evidence derived from them is clearly credible and authoritative. Records should be retained securely and should only be shared or merged where appropriate. The 192 - Health Records Management Policy – opens in a new tab- and appendix of policies and procedures provide further detail specifically on standards for the management of health records. Health records are managed in accordance with the standards detailed in the introduction of this strategy.

Management

All health records are subject to the standards and legislation detailed in this strategy and the HDUHB is responsible for ensuring that health records are managed accordingly. Record-keeping systems should be easy to understand, clear, and efficient in terms of minimising staff time and optimising the use of space for storage. The 192 - Health Records Management Policy – opens in a new tab - details

DRAFT

procedures for the storage, retrieval, archiving and disposal of each record type. This strategy is in accordance with the Welsh Records Management Code of Practice for Health and Social Care.

There should be a consistent approach to records management across the HDUHB, which should be in line with external guidance. The HDUHB is responsible for ensuring that adequate resources are made available to support effective records management, including making adequate provision for records growth and technological developments which enable records to be stored or transferred to other media. Investment in the move from paper to electronic records will become critical and will support improved patient care and service delivery not only within the health records service but across the entire HDUHB.

Security
The HDUHB provides systems which maintain appropriate confidentiality, security and integrity for all health records including their storage and use. Records must be kept securely to protect the confidentiality and authenticity of their contents and to provide further evidence of their validity in the event of a legal challenge. No person identifiable information should be stored, transferred or accessed unless absolutely necessary.

Health records in any format are highly confidential documents and the HDUHB is responsible for ensuring that adequate physical controls are put in place to ensure the security and confidentiality of all patient identifiable information, whether they are held manually (physically) or on computer (electronically). Other relevant policies and procedures are documented, including the 837 All Wales Information Security Policy – opens in a new tab - and they should be utilised in conjunction with local departmental procedures.

Access
Access is a key part of any records management strategy. Fast, efficient access to records unlocks the information and knowledge they contain. There should be clear and efficient access for employees and others who have a legitimate right of access to HDUHB records. Access to all patient identifiable information is on a strict need to know basis in accordance with the Caldicott principles, Data Protection Act 2018, General Data Protection Regulation, Information Governance Standards and various codes of professional conduct. Health Records Policies, including the 249 Access to Health Records Policy – opens in a new tab - and supporting procedures governing access to patient identifiable information all comply with and are in accordance with these principles.

The public has rights of access to all information held by the HDUHB, unless that information is covered by an exemption. Not only must records be maintained appropriately, when it is necessary to pass them to another user or stakeholder, care must also be taken to ensure that they are dispatched in a manner suitable to the content of the records. All managers are responsible for ensuring that there is an appropriate system for tracking and retrieving records when requested legitimately and that non-legitimate requests for records are declined.

Health records and associated clinical information are released to patients, their representatives and legal bodies in accordance with relevant and current legislation, including:

- Access to Health Records Act 1990
- Data Protection Act 2018
- General Data Protection Regulation (UK GDPR)

DRAFT

This list is not exhaustive.
The Health Records Manager is responsible for the processing and release of clinical information in accordance with the 249 Access to Health Records Policy – opens in a new tab - and documented procedures.

Retention and Disposal
Retention is the holding of records after their creation in readiness for operational use. It is a fundamental requirement that all the HDUHB records are retained for a minimum period for legal, operational, research and safety reasons. The length of time for retaining records will depend on the type of record and its importance to the HDUHB's business and clinical functions. The Records Management Code of Practice for Health and Social Care establishes the minimum retention periods for a number of records and these requirements are reflected in the 193 Retention and Destruction Policy – opens in a new tab.

When considering how long to retain a record staff should first note any legal or HDUHB requirement. Records should be retained for the identified minimum requirements and storage in excess of the specified retention period is undesirable. During the retention period appropriate arrangements must be made for the safe storage and effective security of the record and considerations should be given to the storage medium (electronic or paper). Records no longer needed for operational or any other use should be destroyed. It is particularly important that the disposal of records, which is defined as the point in their lifecycle when they are either transferred to an archive or destroyed, is undertaken in accordance with clearly established policies and always through confidential processes.

Legislation
This strategy is based on current legal and statutory obligations and best practice and processes for records management. The Strategy also takes into account the recommendations and standards set by:

- Public Records Act 1958;
- Medical Reports Act 1988;
- The Computer Misuse Act 1990;
- Access to Health Records Act 1990;
- Data Protection Act 2018;
- Human Rights Act 2000;
- Freedom of Information Act
- Welsh Assembly Government (Ministerial Letters, Circulars and Policies);
- Caldicott: Principles into Practice;
- Information Sharing Protocols - Wales Accord on the Sharing of Personal Information
- Data accreditation and data quality

The strategy will be updated as required to include future developments such as updated health records management guidance, updates to statutory legislation, policies, protocols, Acts, etc and to reflect technological changes.

Risk Management and Patient Safety
Systems, policies, procedures and processes are in place to ensure that any risks to the record or the patient as a result of record issues, are identified, assessed and managed according to best practice.

DRAFT

Audit

This Health Records Management Strategy will be audited accordingly based on compliance against the aims, objectives and responsibilities outlined within the 192 - Health Records Management Policy – opens in a new tab.

Training

As the volume and complexity of clinical information increases, we demand the highest standards of performance in the way it is gathered, recorded, stored and transmitted. These requirements are set out in the Introduction of this strategy and throughout the document. Implementation of the strategy, within the HDUHB will put in place explicit guidance on legal and ethical responsibilities for all NHS staff involved with the creation, maintenance and ongoing management of health records. By utilising appropriately referenced publications, the Strategy will ensure compliance with legislation, nationally recognised standards and best practice.

Ongoing workforce education plays a major part in preparing NHS staff to deliver effective, high quality services. There are numerous reasons for providing education and training in information handling, including maintenance and improvement of services, respect to patients as well as the need to comply with legislation in respect of data collection, storage and use. 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. The Health Records service is able to support awareness sessions or bespoke sessions as and when required to increase the awareness of individual staff responsibilities in regards records management. Self-learning modules are available to all staff through the HDUHB's intranet and ESR application.

DRAFT

Health Records Management Policy

DRAFT

Policy information

Policy number: 192
Classification: Corporate
Supersedes: Previous Version
Version number: 5
Date of Equality Impact Assessment:

Approval information

Approved by:
Date of approval:
Date made active:
Review date:

Summary of document:
This policy sets out best practice for the creation, utilisation, retention and destruction of health records within Hywel Dda University Health Board (HDUHB).

Scope:
This policy has been written to provide advice and guidance for all Hywel Dda University Health Board staff dealing with operational records management issues on a daily basis. The Policy highlights the standards that should be attained by all staff when utilising records from creation until final disposal. This policy 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:
[192] – Health Records Management Policy – opens in a new tab
[193] – Retention and Destruction of Records Policy – opens in a new tab
[249] – Access to Health Records Policy – opens in a new tab
[172] – Confidentiality Policy – opens in a new tab
[836] – All Wales Information Governance Policy – opens in a new tab
[837] – All Wales Information Security Policy – opens in a new tab
[347] – Corporate Records Management Policy – opens in a new tab

Patient information:
Owning group: IGSC
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 27.6.2023

Keywords
Health Records, Records Management

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”.

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 individual”. Anything that contains information that has been created or gathered as a result of any aspect of the work of NHS employees.

Data Protection Act 2018 - The Data Protection Act 2018 is a United Kingdom Act of Parliament which updates data protection laws in the UK. It is a national law which complements the European Union's General Data Protection Regulation and replaces the Data Protection Act 1998.

Public Records Act 1958 - The Public Records Act 1958 is an Act of the Parliament of the United Kingdom forming the main legislation governing public records in the United Kingdom.

Subject Access Request – Individuals have the right to access and receive a copy of their personal data, and other supplementary information. This is commonly referred to as a subject access request or 'SAR'. Individuals can make SARs verbally or in writing, including via social media.

Data Protection Impact Assessment – Describes a process designed to identify risks arising out of the processing of personal data and to minimise these risks as far and as early as possible. DPIAs are important tools for negating risk, and for demonstrating compliance with the GDPR.

DRAFT

Contents

Policy information..... 1
Approval information..... 1

Introduction 4
Scope 4
Aim 4
Objectives 5
Health Records Resource 6
Roles and Responsibilities 6
Legal and Professional Obligations 9
Health Records Lifecycle 9
Training 12

DRAFT

Introduction

Hywel Dda University Health Board (HDUHB) will conduct its responsibilities for records management in accordance with relevant legislative requirements of the European Parliament, the United Kingdom and Welsh Government. HDUHB will also comply with any decisions or guidance issued by Welsh Government.

Health Records form an integral part of the clinical recollection of HDUHB, providing evidence of decisions, the rationale for decisions and supporting the HDDUB daily functions and operations. As contemporaneous records they form the basis for the organisations accountability for clinical care. Health records are also essential to protect the rights of patients, staff and members of the public who have dealings with the HDUHB. Health Records support consistency, continuity and efficiency and help the Board to deliver services to our patients in a consistent and equitable way.

Health Records management is about the proper content, control, security, storage and ultimate destruction of records. Records created and held by HDUHB as part of its functions, are public records under the Public Records Act 1958. The Public Records Act 1958 requires that there is a systematic and planned approach to the management of records within an organisation. Moving forward, the effectiveness, safety, care and efficient management of healthcare services, depends on the right information being available to the right people, at the right time. This can only be achieved if there are effective health records management policies and processes in place.

The Board, Executive Team, senior management and all who work for the organisation have responsibilities to ensure that information is handled appropriately and is not retained unnecessarily beyond its life cycle. We also have a responsibility to ensure the accuracy of records and to be able to identify and locate information that is critical for current decision making and available when required for patient care.

This document should be read in conjunction with other HDUHB policies e.g. HDUHB 191 Health Records Management Strategy, 193 - Retention and Destruction Policy, 249 - Access to Health Records Policy – all open in a new tab - etc and also the Data Protection Act.

Scope

This policy has been written to provide advice and guidance for all Hywel Dda University Health Board staff dealing with operational records management issues on a daily basis. The policy highlights the standards that should be attained by all staff when utilising records from creation until final disposal. This policy applies to all permanent, temporary or contracted staff employed by HDUHB (including Executive and Non – Executive Directors).

Aim

The aim of this Health Records Policy is to ensure that procedures are in place to bring together the health professionals and accurate, relevant and reliable patient documentation, at the correct time and place to support patient care. In achieving this aim, HDUHB employees should fulfil statutory and other legal requirements, ensuring patient safety and safe custody and confidentiality of patient information at all times.

The Health Records Management policy applies to all health records and personal information collated in relation to clinical activities and patient care. As the HDUHB utilises a hybrid of both paper and

electronic records to support clinical processes this policy and the agreed standards of records management will fully apply to both formats. The policy sets out best practice for the creation, utilisation, retention and disposal of health records. It applies to all health records regardless of format, of all types and in all locations where they are used to:

- to support patient care and the continuity of care
- to support evidence based clinical practice
- to assist clinical and other types of audits
- to support improvements in clinical effectiveness through research and support archival functions by taking account of the historical importance of material and the needs of future research
- to support the day-to-day business which underpins the delivery of care
- to support sound administrative and managerial decision making as part of the knowledge base for the NHS services
- to support patient choice and control over treatment and services designed around patients
- to meet legal requirements including requests from patients under subject access provisions of the Data Protection Act

Objectives

The objective of this policy is to ensure that health records management is applied consistently across the HDUHB and draws on best practice, as well as ensuring that our services meet the legal, professional and individual responsibilities associated with record keeping. It is designed to provide the staff who create, hold and utilise the health record in the course of their duties with their obligations and expectations and help to increase the confidentiality, integrity and availability of the health record.

The policy relates to all health records which are created carrying out the HDUHB business and captured in any readable form, providing evidence of the patient care delivered. The policy provides all HDUHB staff with clear guidance and standards to attain on a daily basis and robust assurance that health records management systems are able to ensure that:

- **health records are available when needed** – from which the HDUHB is able to form a reconstruction of activities or events that have taken place
- **health records can be accessed** – health records and the information contained within them can be located and displayed in a way which is consistent with the records initial use and that the current version is identified where multiple volumes exist;
- **health records can be interpreted** – the context of the record can be interpreted; who created or added to the health record and when, during which business process, and how the health record is related to other health records
- **health records can be trusted** – the health record reliably represents the information that was actually used in or created by the business process, and the record integrity and authenticity can be demonstrated;
- **health records can be maintained through time** – the qualities of availability, accessibility, interpretation and trustworthiness can be maintained for as long as the health record is needed, perhaps permanently despite changes of format;

DRAFT

- **health records are secure** – from unauthorised and inadvertent alteration and erasure. Access and disclosure are properly controlled and audit trails will track all use and changes to ensure that health records are held in a robust format;
- **health records are retained and disposed of appropriately** – using consistent documented retention and disposal procedures which include provision of appraisal and permanent preservation for health records with archival value;
- **staff are trained** – all staff within the organisation are made aware of their responsibilities for health record keeping and management.

Health Records Resource

Records are a valuable resource because of the information they contain. Information is only useful if it is correctly recorded in the first place, is regularly updated and is easily accessible when it is needed. Information is essential to the delivery of high quality healthcare and effective records management. The records and formats will include (but is not limited to):

- Records of patients treated by HDUHB including health and care records
- Records of private patients treated on NHS premises
- Records of patients treated on behalf of the NHS in the private healthcare sector
- Adult Service user records where there is integration with health services e.g. jointly held records

This list is not exhaustive.

A health record is everything (paper or electronic) that contains information which has been created or gathered as a result of any aspect of the delivery of patient care, including (but not limited to):

- Personal health records (electronic, microfilmed, scanned images & paper based)
- Theatre Registers and all other registers that may be kept
- X-ray and imaging reports, output and images
- Photographs, slides and any digital images
- Audio and video tapes, cassettes
- Digitised images/Digital Records (scanned)
- Emails
- Text messages (SMS)

This list is not exhaustive.

Roles and Responsibilities

All health and care employees are responsible for managing records appropriately. Health records management must provide a focus for all types of records, in any format to be managed from their creation to ultimate disposal. The health record management function must have clear responsibilities and accountability throughout the HDUHB.

Chief Executive

The Chief Executive has overall accountability and responsibility for ensuring that health record management operates correctly and legally within the HDUHB. The CEO may delegate responsibility for management and organisation of the health records services to the Caldicott Guardian or another Director who will be responsible for ensuring that appropriate mechanisms are in place to support service delivery and continuity.

DRAFT

Caldicott Guardian/SIRO
The Caldicott Guardian/SIRO are responsible for protecting the confidentiality of service user information. The Caldicott Guardian/SIRO have strategic roles which involve representing and championing information governance requirements and particular responsibility for reflecting patients' interest regarding the use of patient identifiable information.
The Caldicott Guardian has responsibility for:

- Ensuring the HDUHB is fulfilling all legal obligations in managing patients' health records
- Agreeing and reviewing internal protocols governing the protection and use of patient identifiable information by HDUHB staff
- Agreeing and reviewing protocols governing the disclosure of patient information across organisational boundaries e.g. with social services and other partner organisations, contributing to the local provision of care (WASPI)
- Developing the HDUHB security and confidentiality policies through the clinical and information governance frameworks
- Representing confidentiality requirements and issues to the HDUHB, advising on annual improvement plans and agreeing and presenting outcome reports

The SIRO is responsible for:

- Fostering a culture for protecting and using data
- Provides a focal point for managing information, risk and incidents
- Is concerned with the management of all information assets
- Acts as an advocate for information risk on the Board and provides written advice to the Accounting Officer on the content of their annual governance statement in regard to information risk

Executive Directors
All Executive Directors are responsible for implementing records management arrangements at Directorate level through the relevant committees and meeting forums and overseeing a programme of record management activities, in accordance with this policy.

Digital Director
The Digital Director is responsible for ensuring that regulations are in place to maintain the security of all electronically stored information, outlining the security responsibilities of management and staff. The Director is also responsible for the management of electronic/digital systems.

Information Governance Sub Committee
The Information Governance Sub Committee is responsible for ensuring that the Health Records Management Policy is implemented through its endorsement and approval and will take a lead role in its obligation to ensure robust records management arrangements are implemented across the HDUHB.

Head of Information Governance
The Head of Information Governance is the designated management advisor for the HDUHB and has responsibility for ensuring that the HDUHB complies with the developments in national guidance relating to information governance. They will have a responsibility to provide any specialised advice or guidance to other service areas as required and maintain an Information Asset register, which can be utilised for records management arrangements.

DRAFT

Health Records Manager
The Health Records Manager has professional responsibility and accountability for the overall development and maintenance of health records management practices within the organisation and for ensuring that related policies and procedures conform to the latest legislation and standards on data protection, UK GDPR, confidentiality and health records practice. They will have a responsibility to provide specialised leadership, guidance, advice and support in regards records management arrangements and processes within the HDUHB. They have responsibility for overseeing, directing and coordinating the day to day management of operational matters within the Health Records Service including the provision of patient records for inpatient, outpatient and day case attendances. They are responsible for ensuring that the release of all patient clinical information for data Subject Access Requests (SARs) and provision of records for medico-legal purposes is in accordance with the legislation.

Information Asset Owners & Information Asset Administrators
Information Asset Owners (IAO's) will delegate responsibility to Information Asset Administrators (IAA's), whose remit will also include responsibility for health record management arrangements within their service. The IAO's will ensure that the policy is implemented within their service areas and robust records management arrangements are in operation.

Professional Staff Groups
Professional staff groups must ensure that they maintain factual, clear, concise and unambiguous records to provide credible and authoritative evidence of services delivered. They must ensure that all contact with service users, carers or other relevant individuals is systematically recorded in keeping with agreed standards. Ensure that no action or omission on their part or within their sphere of responsibility is detrimental to the interests, condition or safety of service users, staff or the HDUHB and that records are always documented with a view that they can potentially be disclosed and read by the service user/patient.

Employees
All NHS employees and staff are responsible for any health records which they create or use. This responsibility is established and defined by the law and any records created by an employee are public records. All HDUHB staff, whether clinical or administrative, have an individual responsibility for records management and for the correct creation, use and retention of records in line with their job roles. Staff must ensure that they keep appropriate records of their work and manage those records in keeping with this policy and with any supporting policies or guidance subsequently produced.

Everyone working for or within the NHS who records, handles, stores or otherwise comes across patient information has a personal common law duty of confidence to patients and to his or her employer. The duty of confidence continues even after the death of the patient of after the employee or contractor has left the NHS. All staff must ensure that all confidential, patient identifiable information is retained in the appropriate records management system. Staff have a duty to read and understand the content of this policy and a Breach of this policy will mean that the HDUHB is not safeguarding information entrusted to it, which could render the HDUHB liable to prosecution. It is therefore essential that staff within the organisation with responsibility for record management comply with the policy or they may be subject to disciplinary procedures.

DRAFT

Legal and Professional Obligations

All health and care employees are responsible for managing records appropriately. Records must be managed in accordance with the law. All NHS Health Records are public records under the Public Records Act. The HDUHB will take actions as necessary to comply with legal and professional obligations such as:

- Public Records Act 1958 and Local Government Act 1972
- Freedom of Information Act 2000
- Records Management Code of Practice for Health and Social Care 2022
- UK GDPR and Data Protection Act 2018
- Access to Health Records Act 1990
- The Common Law Duty of Confidentiality
- Health and Social Act 2008
- Limitation Act 1980 and Consumer Protection Act 1987
- Caldicott: Principles into Practice
- Any new legislation affecting health records management as it arises

Health and care professionals also have professional responsibilities for example complying with the **record keeping standards** as set out by registrant bodies.

Health Records Lifecycle

Health records are confidential documents and should be clearly identifiable, accessible and retrievable. They should be authentic, meaningful, authoritative and adequate for their purpose and correctly reflect what was communicated, decided or done. They should be unalterable and after an action has occurred nothing from the health record should be deleted or altered. Information added to an existing hard copy health record should be signed and dated. Health records systems should be secure and their creation, management, storage and disposal should comply with current legislation.

Creation

A comprehensive health record is created and maintained for every patient attending health services to provide an up to date and chronological account of the patient's care.

- Patient demographic data for each registration should be recorded on the master patient index of the patient administration or departmental system
- The minimum patient demographic data should include: surname, forename, sex, date of birth, home address, postcode, NHS and or PAS/departmental number
- The organisation should use the NHS number as the main patient identifier and a partial validation tool
- Where there is more than one local identifier or case record per patient, a system is in place to ensure that the existence of all other health records is known
- The paper health record has a standard case record folder constructed of robust material which can withstand handling and transport and has secure anchorage points to protect against loss or damage to documentation
- There is a designated area within the health record for health professionals to record actual or suspected clinical alerts or risk factors

DRAFT

- There is a locally agreed format for the filing of the information in the health record which facilitates ease of access to all clinical information. Clear instructions regarding the order of filing is contained within the folder
- Machine generated reports and recordings such as CTG, ECG and laboratory reports are stored securely within the case note folder
- All electronic systems are password protected and passwords are changed at regular intervals. An audit trail of access, amendments or updates is available and reports can be taken from the system

Storage

Health record storage areas should provide a safe working environment with secure storage that allows health records to be retrieved as and when required. These areas should only be accessible to authorised staff and should conform to agreed standards e.g. BS 5454 to protect records from damp, fire, flood and chemical contamination.

- Health records storage areas and office accommodation should conform to all current legislation and guidance regarding health and safety
- Risk assessments are undertaken in line with the risk management strategy
- Racking, where this is in use, is stable and of strong enough construction to support the weight of the health records and mostly complies with current health and safety regulations
- There are safety step ladders and stools appropriate to the number of staff employed and to the size of the different storage areas
- The staff are trained in the manual handling procedures associated with the library areas
- Equipment within the department conforms to the appropriate legislation and equipment checks are conducted when necessary
- Access to the libraries is restricted to authorised personnel. The keys/access codes/swipes to areas that are locked are made available to staff to facilitate the retrieval of health records during the out-of-hours service
- The health records areas should be capable of accommodating the current needs and annual growth of health records
- Health records must be stored securely when in clinical areas, offices and arrangements made within these areas to allow retrieval of records when required

Management of Records (onsite & offsite)

Maintaining the health record is vital to patient care. The health records service has well defined procedures and systems in operation for the ongoing management of the health record from initiation to final disposal in accordance with legislation.

- Whenever possible, separate areas are maintained for current and non-current health records in use within the organisation;
- There are documented procedures for the safe storage and retrieval of health records;
- There are documented procedures for the tracking of records within the organisation and audit is used to highlight any issues that arise as a result of non compliance
- There is a documented procedure for the splitting of fat folders and cross referencing of the volumes. Closed volumes are suitably labelled.
- There is a documented procedure relating to the return of the patient held record when an episode of care is complete.

DRAFT

- The responsibility for the filing of loose documentation rests with the staff who generate the information.
- There are agreed processes and identified staff responsible for the filing of loose documentation.
- Each person who uses and adds to the record has the responsibility to maintain the record and file any information into the appropriate section and format. This is part of the overall record keeping standards of the organisation.
- Health records staff will routinely split large folders or provide a new folder if the outer cover is not of a good standard.
- There are documented procedures for the transportation of health records both within and outside of the HDUHB.
- There are documented procedures for the handling of subject access and Access to Health Records requests with clear responsibility for responding by fully trained, dedicated staff who process requests in accordance with the law;
- There are documented procedures for the retention, archiving and destruction of health records in accordance with national guidelines. The method of destruction ensures that confidentiality is maintained at all times.
- There is a set of performance indicators which demonstrate the efficiency of the health records service which include health record availability, incorrectly tracked records, SAR's compliance etc
- Offsite records requires that there is a full inventory of the records that are held offsite
- Retention periods require to be assigned to each record held offsite
- Evidence is obtained of secure disposal of records and information
- A Data Protection Impact Assessment (DPIA) must be conducted if moving records to an offsite storage contractor and the Health Records service contacted for advice and guidance on the factors to be taken into consideration prior to removal of records to an offsite store.

Creation and Maintenance of Patient Healthcare Records

The HDUHB uses the Welsh Patient Administration system (WPAS) to create a patient record. HDUHB policies and procedures specify clear standards that should used by all staff involved in maintaining the patient record.

Wherever possible all patient information should be centrally held as part of the main patient record. However the HDUHB acknowledges that in some circumstances it may be practical to generate or hold local patient records, for example emergency attendances. Where there are locally held patient records, all staff involved in the creation, use and/or management of these records should also ensure they meet the required standards and ensure that the record types are recorded on the Information Asset Register.

The Health Records Department are responsible for identifying main clinical records for retention or destruction and will apply the retention schedules as stipulated in the HDUHB 193 - Retention and Destruction Policy – opens in a new tab - and supported by the Record Management Code of Practice.

Tracking and Retrieval of Records

The movement and location of records should be controlled to ensure that a record can be easily retrieved at any time, that any outstanding issues can be dealt with and that there is an auditable trail of record transactions.

The HDUHB utilises the Welsh Patient Admin System **Intelligent Tracking** facility to monitor and records the movement of the main patient healthcare record within the organisation (paper). The objectives of this policy are to:

- Ensure all health records are tracked on WPAS
- Ensure the location of all health records are known at all times
- Establish and maintain standards for the use of health records
- Reduce the risk of health records not being available for patient consultations, subject access requests and legal requirements

Archiving and Disposal of Health Records

There is a detailed and agreed policy on the retention, destruction and/or archiving of health records, which operates in accordance with the Welsh Records Management Code of Practice. It is particularly important that the disposal of records, which is defined as the point in their lifecycle when they are either transferred to an archive or destroyed, is undertaken in accordance with clearly established policies.

It is a fundamental requirement that all the HDUHB records are retained for a minimum period for legal, operational, research and safety reasons. The length of time for retaining records will depend on the type of record and its importance to the HDUHB business and clinical functions. The HDUHB has a retention schedule which is set out in the HDUHB 193 - Retention and Destruction Policy – opens in a new tab. Records destroyed shall be recorded on WPAS. Destruction of eligible records shall be completed annually with archived records indicating the year for destruction, which will enable those pending destruction to be identified. Any decision to retain/destroy records outside of the periods specified will be approved and fully documented.

The Health Records Manager and Health Records Management team can offer advice on the requirements and procedure for dealing with the disposal of all records at this stage in the lifecycle.

Training

While some aspects of Information Governance is covered in the HDUHB Corporate Induction for all staff, it is expected that local induction arrangements will cover the specific roles and responsibilities of staff in relation to the lifecycle of records. 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. The mandatory training on Information Governance also includes elements of records management standards.

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. The Health Records service is able to support awareness sessions or bespoke sessions as and when required to increase the awareness of individual staff responsibilities in regards records management. Self-learning modules are available to all staff through the HDUHB's intranet and ESR application.

DRAFT

Retention and Destruction of Records Policy (Including Health Records)

Policy information

Policy number: *193*
Classification: Corporate
Supersedes: Previous versions
Version number: 5
Date of Equality Impact Assessment: 27th January 2026

Approval information

Approved by: Digital Data and Innovation Committee
Date made active:
Review 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 – opens in a new tab
[192] – Health Management Policy – opens in a new tab
Records Management Code of Practice for Health and Social Care 2022
[172] – Confidentiality Policy – opens in a new tab
[836] – All Wales Information Governance Policy – opens in a new tab
[347] – Corporate Records Management Policy – opens in a new tab
[224] – Information Classification Policy – opens in a new tab
[837] – All Wales Information Security Policy – opens in a new tab

Patient information:

DRAFT

Owning group: IGSC

Executive Director job title: Director of Digital

Reviews and updates:

1 New ;policy September 2012
2 Full review 23.2.2016
3 DPA update 26.6.2018
4 Full review 28.2.2023
5 Correction to the Records Management Code of Practice for Health and Social Care, published by the Welsh Government, retention period for sealed contracts changed from 6 years to 12 years

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

Policy information 1
Approval information 1
Introduction 4
Policy Statement 4
Scope of policy 4
Aim 5
Objectives 5
What is a Record 5
Retention 6
Destruction 6
Legislation 7
Responsibilities 7
Training 8
Retention Timescales 8

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 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 include decisions which relate to the physical and mental health of an individual which has been made by or on behalf of a health professional. A corporate record is any record relating to the business function of the organisation which is not considered a health record.

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 internally, from offsite storage or digitally, whenever they are required by a clinician.

Corporate records also need to be easily retrievable and securely retained throughout their lifecycle to enable day to day business function to be conducted and evidenced.

It is important to note that the Health Board no longer uses external/non Health Board storage providers/facilities and any storage requirements should be discussed with both the Health Records Manager and the Information Governance Service. In emergency circumstances 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 health 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 digital 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.
- All corporate records should be reviewed at the end of their retention schedule (laid out in Records Management Code of Practice for Health and Social Care – A guide to the management of health and care records). The disposal outcome should be reviewed by the Information Asset Owner and the Senior Corporate Records Management Officer. The Senior Corporate Records Management Officer will work with teams to arrange the transport of records identified for transfer to an archive. 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 their 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.

The Senior Corporate Records Management Officer has professional and operational responsibility for the secure retention and destruction of the Health Boards corporate records and ensuring these records are managed in accordance with legal timeframes. The Senior Corporate Records Management Officer is responsible for ensuring only appropriate records are destroyed and all inquiries regarding the destruction of corporate records, must be directed to Information Governance Team and any destruction authorised by the Senior Corporate Records Management Officer.

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 (opens in a new tab) – A guide to the management of health and care records and information for all Health Board staff on nationally agreed retention guidelines .

Digital Procurement and Requests Procedure

DRAFT

Policy information

Policy number: 240
Classification: Corporate
Supersedes: Previous versions (previously named Informatics Procurement & Request Procedure)
Version number: 4
Date of Equality Impact Assessment:

Approval information

Approved by: Digital Data and Innovation Committee
Date of approval:
Date made active:
Review date:

Summary of document:
Hywel Dda University Health Board is committed to ensuring all Digital purchases align with both local and national strategies and that they represent value for money to public funds.

This procedure sets out a series of steps to follow to ensure all Digital purchases meet the requirements above and satisfy both the technical infrastructure and security requirements of the Health Board.

The procedures in this document are to be followed to ensure all requests for new Digital projects follow the correct governance and assurance arrangements before being committed into the Digital Operational Plan.

Scope:
This procedure covers everyone that is employed by Hywel Dda University Health Board who may request Digital services. The definition of Digital includes the following services: -

- Telecommunications (Telephones, paging and mobiles).
- Desktop Equipment (PC's, printers, scanners, projectors, and other peripherals).
- Mobile Equipment (Tablets, Android / Apple devices, carts).
- Medical equipment which connects to the Health Board network or includes software which needs to be assessed from an Information Governance / Cyber Security perspective.

- Audio-Visual equipment.
- Equipment to support health & safety assessments in relation to the use of display screen equipment regulations.
- Office moves and refurbishments.
- New Builds.
- Requests for new Digital Services.

To be read in conjunction with:
Digital Health Strategy (opens in a new tab)
837 – All Wales Information Security Policy (opens in a new tab)
Health Board's Standing Financial Instructions (opens in a new tab)
Standing Orders (opens in a new tab)
Capital Investment Procedure (opens in a new tab)
Our Digital Response

Owning group: Information Governance Sub-Committee

Executive Director job title: Director of Finance

Reviews and updates:
Version 1 – new policy 6.9.2011
Version 2 – revised and amended 26.2.2017
Version 3 – full three yearly review 25.4.2023
Version 4 – full review

Keywords: Digital procurement procedure

Glossary of terms
DHCW – Digital Health and Care Wales
DCP - Discretionary Capital Programme
ICT – Information & Communications Technology

DRAFT

Contents

Policy information 1
Approval information 1
1. Aim 4
2. Objectives 4
3. Scope 4
4. Procurement of Standard Digital Equipment 4
5. Procedure for Adhoc Departmental Moves 6
6. New Digital Project Approval Procedure 6
7. Determining the Priorities for a Project 7
8. Responsibilities 7
9. Training 8
Appendix A – Digital Requesting and Project Approval Flowchart 9

DRAFT

1. Aim

It is the responsibility of the Digital Senior Management Team to oversee the implementation of the Digital Strategy, including commissioning additional developments and resources as required. This document sets out the method by which Digital and System procurements, new Digital projects, adhoc departmental moves and changes as well as enhancements to existing systems will be approved, allocated resources, and ensuring that appropriate governance and assurance is sought.

The procedure for gaining approval for Digital initiatives is dependent on the context of the project. If the project is: -

- **Procurement of standard ICT equipment** (purchasing of standard hardware, software, mobile phones / smartphones, and peripherals such as printers and scanners) should follow the "Procurement of Digital Equipment" procedure outlined in section 4.
- **Adhoc departmental moves and changes** should follow the 'Adhoc Departmental Moves" procedure outlined in section 5.
- **Digital project approval** (New Digital projects, new builds, major refurbishments, and upgrades/enhancements to existing systems) should follow the "Digital Project Approval" procedure outlined in section 6.

This procedure should be read in conjunction with the Health Board's Standing Financial Instructions, Standing Orders, the Policy for Procurement and Life Cycle Management of Equipment and where relevant, the Capital Investment Manual.

Templates and electronic links for the submission of projects are provided in the ICT Forms Library on the Health Board's Intranet site or through requests to the Informatics Service Desk.

Any project which may impinge on National Strategy may need to be submitted to the relevant Digital Health and Care Wales (DHCW) governance committees.

2. Objectives

The main objective of this procedure is to ensure employees of the Health Board are aware of the procedure to follow when requesting Digital equipment, software, services and new projects.

3. Scope

This procedure covers everyone that is employed by Hywel Dda University Health Board who may request Digital services.

4. Procurement of Standard Digital Equipment

This covers the purchase of all Digital standard hardware, software, peripherals (scanners, printers etc.) and mobile phones in addition to related professional services. This procedure does not include purchases which are part of an already approved capital programme, business case or DHCW funded projects.

Advice from Digital Services should also be sought where network attached equipment is being procured. This includes medical devices, laboratory analysers, security systems and CCTV.

DRAFT

All Digital equipment purchases will conform to Digital Services specifications and will be authorised prior to ordering by the Digital procurement team.

All Digital purchases should be channelled through Digital Services, if bypassed any Digital purchases should be clearly identifiable by Procurement who will forward such requisitions to the Head of Digital Operations to ensure that the processes in this procedure are followed.

Replacement Programme
When equipment is assessed as being "end of life" it will be replaced under the replacement programme subject to available funding levels. This will include but is not restricted to PCs, printers, scanners, servers, network devices, infrastructure components, software and telecommunications (including mobile phones).

The replacement programme is funded from the Health Board's Discretionary Capital Programme (DCP) and will be managed by Digital Services. This does not exclude the funding of replacement equipment from departmental budgets (if less than £250) and Charitable Funds as required in line with the Health Board's standing financial instructions.

New Equipment
The procurement of new Digital equipment will be from departmental budgets following approval and providing it doesn't fall under the remit of the "New Digital Project" procedure requirements.

It is important to note that items over £250 in value and connected to the network are classed as capital assets (not revenue) and as such can only be funded from the Health Boards capital allocations and local charitable funds. This will include many pieces of Digital equipment including high end printers, PC's, laptops and tablets.

All requests for software packages, computer hardware, peripherals (scanners, printers etc.) or network / telecommunication services should be made by completion of the request forms via the Digital Services Portal which is available under the "Request a service" link:

Welcome to the Digital Services Portal (opens in a new tab)

All sections in the form require completion for the procurement to progress and once received Digital Services will process in line with local procedures. The request must be authorised by the responsible officer (e.g. budget holder or service manager) and a notification will be received via Microsoft Teams to approve or deny the request.

Any request "deemed" as non-standard will be forwarded to the Head of Digital Operations for consideration and may fall under the remit of the "New Digital Project Approval" procedure as outlined in Section 8.

External Funding
Occasionally the Health Board will receive external funding which is placed into ring fenced budgets (Welsh Government R&D for example), requests utilising these monies will be managed as per this procedure and Digital Services will discuss with Finance on a case-by-case basis the funding arrangements and any revenue / capital transfers.

DRAFT

5. Procedure for Adhoc Departmental Moves

This section outlines the procedure that will be followed to gain approval for Digital to support departmental moves / changes and office moves. The scope includes Health Board employees requiring: -

- New data points for network access.
- New telephone points, handsets, and numbers.
- Moving of extension numbers between locations.
- Move of Digital equipment (PC's / Printers etc.) between locations.

It is important that Digital Services should be engaged as soon as possible using the process below to ensure any associated works can be scheduled in and completed prior to any staff moving offices.

All requests for departmental moves should be made by completion of the relevant electronic form on the Digital Services Portal. The link to the form is also provided below: -

Adhoc Network Moves and Changes : Hywel Dda University Health Board (wales.nhs.uk) (opens in a new tab)

All sections in the form require completion for Digital Services to process and once received the request will be completed in line with local procedures. The request must be authorised by the responsible officer (e.g., budget holder or service manager) and a notification will be received via Microsoft Teams to approve or deny the request.

On receiving the request Digital Services will review and respond to the requester when the work can be completed and details of any associated costs. If the number of resources required by Digital is extensive then the "New Digital Project Approval" will be followed.

Once the budget holder has approved the work, Digital Services will complete a schedule for completion and any moves and changes requested which don't follow this procedure will be potentially rejected.

6. New Digital Project Approval Procedure

This section outlines the procedure that will be followed to gain approval and funding for a new Digital project which would be added to the Digital Operational Plan. Examples of such new projects include: -

- New builds or refurbishments of Health Board property which have a Digital element.
- Requests for upgrades to existing systems.
- Requests for new Digital system or service.
- Any requests received through the "Standard Digital Equipment Procedure" where the Head of Digital Operations determines it needs to follow the formal approval process.

Any such requests must be via the online request form available on the Digital Services Intranet Pages:

DRAFT

Digital Project / Support Request (opens in a new tab)

More information on the Health Boards Digital Response and framework can be found below:

Delivering the Digital Response (opens in a new tab)

The Digital project proposal once submitted will be discussed by the Digital Services Senior Management Team for consideration, prioritisation and acceptance.

If approved by the Digital Senior Team and the project has already been funded and approved by the relevant assurance committee the project will have a priority set, be scheduled and have resources allocated by the digital delivery team. If there is a conflict in priorities these will be considered and deconflicted at the Digital Service Programme Group, based on business impact and funding.

If no funding / approval has been approved, then the request will be deferred to the Digital Programmes Group as required for consideration.

Further information regarding the priority of digital project can be found in the Digital Response document.

7. Determining the Priorities for a Project

The following criteria will be used by the Digital Senior Team in assessing what priority should be given when approving and progressing projects: -

- The priority in this area / activity in the Health Board's IMTP.
- The project's time constraint.
- The potential savings that would be lost or additional cost incurred if the project was delayed.
- The resources required and any conflicts with other projects.
- Other projects / activities / initiatives dependent on the completion of this project.
- Any external influences on the project's implementation date.
- Risks incurred or changed by the implementation.
- The project's fit with national strategies if relevant.

8. Responsibilities

Head of Digital Operations

The Head of Digital Operations shall have overall responsibility for the implementation of this procedure and will delegate responsibility to ensure appropriate departmental procedures are in place to aid its implementation.

The Head of Digital Operations will escalate any issues as appropriate to the Digital Director.

Digital Senior Team

All members of the Digital Senior Team will be made aware of this procedure to ensure they are aware of their roles and responsibilities in the approval process for Digital projects.

NHS Wales Shared Services Partnership

The NHS Wales Shared Services Partnership will be required to be aware of this procedure to ensure any requisitions they receive for Digital related equipment is not processed unless this procedure has been followed (where requisitions are not received through designated Digital requestors).

DRAFT

Director of Estates
The Director of Estates will be responsible for dissemination of this procedure to relevant Estates staff to ensure it is considered when planning new builds and refurbishments of Health Board property.

Executive Directors / County Directors / Service Delivery Managers
Will be required to be aware of this procedure to ensure Digital implications are considered when planning service change, new projects, and new services.

Information Asset Owners
Information Asset Owners will be responsible for considering this procedure when planning any system upgrades or enhancements with 3rd party suppliers.

Heads of Department / Budget Holders
Will be required to be aware of this procedure to ensure it is followed when requesting Digital services.

9. Training

All staff will be made aware of this procedure through a communications plan and availability to view on the Health Board Intranet site.

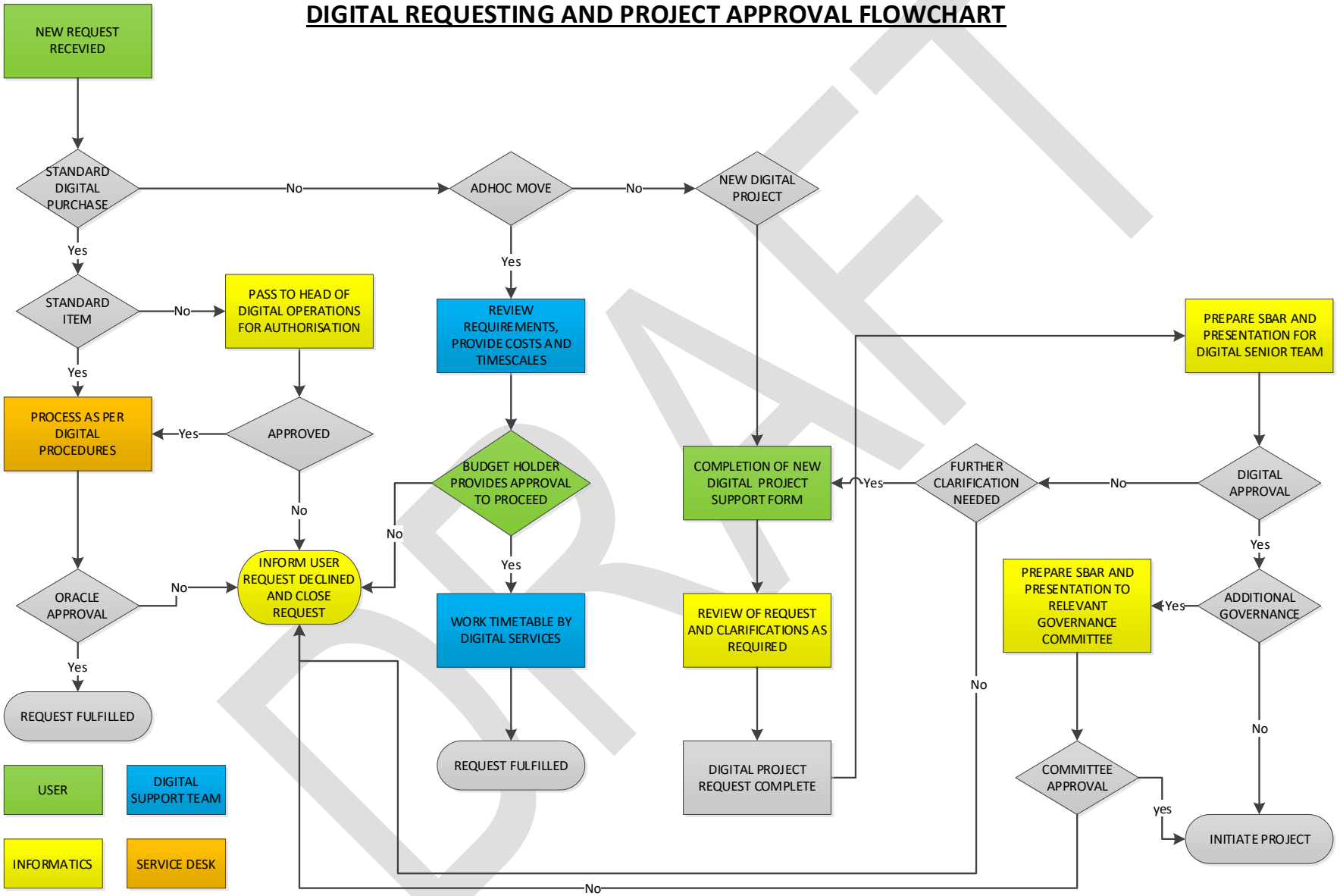
Awareness will also be promoted by the Digital Service Desk when requests are received and through membership of the relevant governance groups of the Health Board.

Targeted communications will also be undertaken to the groups identified in the Responsibilities Section.

Support will be provided by Digital Services Department as required to support Health Board staff in ensuring they meet the requirements of this procedure.

DRAFT

Appendix A – Digital Requesting and Project Approval Flowchart



DRAFT

DRAFT

Acceptable Use of Digital Services Policy
DRAFT

Policy information

Policy number: 320
Classification: Corporate
Supersedes: Previous versions
Version number: 4
Date of Equality Impact Assessment:

Approval information

Approved by: Digital Data and Innovation Committee
Date of approval:
Date made active:
Review date:

Summary of document:
This policy outlines standards for the appropriate and inappropriate use of Health Board digital systems and networks. It clarifies permitted activities, including personal use; identifies prohibited actions, such as personal use during working hours and accessing indecent, obscene, or offensive material; and details the consequences for violating these guidelines.

The policy describes how the Health Board has established systems to track users and their activity, as well as measures that block access to indecent, obscene, or offensive content. It also states that any violations will be addressed promptly and according to disciplinary procedures when appropriate.

Scope:
This policy applies to all employees of the Health Board, volunteers, other NHS and health organisations, and other contracted staff; having the facility to use the Health Board's e-mail and internet services, plus anyone granted access to the Health Board network whilst engaged in work for the Health Board at any Health Board occupied location, and/or on any Health Board owned or Health Board approved computer asset.

This policy applies to all users of Digital Services in relation to:

- The use of digital equipment.
- The use of digital communication tools.
- Digital systems connected directly or remotely to the Health Board NHS managed network or used on the Health Board's premises.

To be read in conjunction with other Digital Policies and Procedures.
201 – AW Disciplinary Policy – opens in a new tab

Owning group: Information Governance Sub-Committee

Executive Director job title: Director of Finance

Reviews and updates:
Version 1 – new policy 28.91.2013
Version 2 – revised and amended 21.5.2018
Version 3 – full review
Version 4 – full review

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

Glossary of terms
DHCW – Digital Health and Care Wales
DCP - Discretionary Capital Programme
ICT – Information & Communications Technology

Contents

Policy information 1
Approval information 1
Aim 4
Objectives 4
Scope 4
Becoming and Authorised User 4
Acceptable Use 5
Unacceptable Use 5
The Use of the Organisations Name 6
Unintentional Breaches of Digital Security 7
Acceptable Network and System Usage 7
Responsibilities 7
Training 9

Aim

The aim of this policy is to ensure all users of Health Board services do so in a safe and secure manner ensuring compliance with relevant legislation.

Objectives

The objectives of this policy are to: -

- Clarify Health Board policy regarding acceptable and unacceptable use of Digital services, and Health Board network access.
- Reduce or avoid security threats by increasing awareness and disseminating good practice.
- Cease the copying/distribution of copyrighted materials.
- Encourage effective use of Health Board resources.
- Protect the Health Board against potential liability.

Scope

This policy applies to all employees of the Health Board, volunteers, other NHS and health organisations, and other contracted staff; having the facility to use the Health Board's e-mail and internet services, plus anyone granted access to the Health Board network whilst engaged in work for the Health Board at any Health Board occupied location, and/or on any Health Board owned or Health Board approved computer asset.

This policy applies to all users of Digital Services in relation to:

- The use of digital equipment.
- The use of digital communication tools.
- Digital systems connected directly or remotely to the Health Board NHS managed network or used on the Health Board's premises.

Becoming an Authorised User

Every member of staff or contractor who requires access to Digital systems must complete the relevant online form available on the Digital Services Portal to request an account with the necessary access to Digital systems. If the account is approved by their line manager, the user will be set-up with a username and password by the Digital Service Desk.

In the unlikely event of the application being turned down, the staff or contractor will be contacted to communicate the reasons for rejection. Access to Digital systems will only be through the following means:

- Health Board NHS managed network which is protected by perimeter firewalls, anti-virus software and content filters.
- Authorised remote access using Cisco Anyconnect, Citrix Gateway, or Microsoft Office 365.

Acceptable Use

Access to Digital systems is primarily for business related purposes. Personal use is permitted provided this does not interfere with the performance of your duties, those of other staff or contractors or the business of the Health Board in general. Personal access to Digital systems can be limited or denied by your manager. Staff and contractors must act in accordance with Health Board Policy.

However, there can be no expectation of the privacy of personal e-mails. In certain circumstances and following the processes contained in the Information Commissioner's code of practice on staff data, the organisation may, in a proportionate manner, view personal e-mails as legislation or the Health Board's Disciplinary procedures permit. In such circumstances, the Regulation of Investigatory Powers Act (2000) and the Lawful Business Practices Regulations (2000) confirms that the organisation's responsibilities may prevail over a member of staff's individual rights to confidentiality of correspondence. The Health Board reserves the right in these circumstances to view the content of an individual's mailbox.

Unacceptable Use

This policy sets the common minimum standards for the acceptable use of Digital systems and services. Set out below are examples of activities and uses which are specifically excluded. The list is not comprehensive and is divided into two sections ("Unacceptable" and "Forbidden") to help highlight the most serious activities. The consequences of undertaking any of the activities listed below (or other instances) will be determined through the normal disciplinary procedures. All such activities are serious and are likely to be viewed as misconduct. It is likely that undertaking a forbidden activity, or repeating an unacceptable activity, will be viewed as gross misconduct.

Any unacceptable use will be reported as per the Information Governance incident procedure, and it is the responsibility of the investigating officer to ensure that the matter is dealt with in line with current Information Governance and Digital policies and procedures. This may result in a full enquiry that could result in disciplinary action being taken and access of the staff or contractor involved may be suspended pending the enquiry conclusion at which point it may be terminated.

Unacceptable use of Digital systems provided by the Health Board are shown below:

- Spending more than permitted amounts of working time making personal use of the internet, e-mail, and other Digital Systems and services.
- Transmitting, downloading or storing any material such that this infringes the copyright of the owner.
- Purchasing goods or services or entering any contract via the Internet or any other Digital system on behalf of the Health Board without the necessary authority and not in accordance with the Health Board's standing financial instructions.
- Business advertisements or trading, i.e., sale of any goods purchased with the sole intention of making a profit.
- Using an unauthorised electronic communication mechanism for the transmission to a third party of personal identifiable data or confidential material concerning the activities of the Health Board.
- Using unauthorised external email accounts for Health Board activities such as Outlook.com or icloud.com.
- Using cloud-based services where Health Board confidential data or person identifiable information could be stored outside of the European Union or European Economic Area.

- Unauthorised redistribution of email.
- Sending or forwarding spam emails.
- Making your Cymru or any other system username and password (also known as a 'user account') available for other people to use on your behalf.
- Accessing another individual's data, Digital systems, or service without appropriate authorisation.
- Deliberately creating, storing, or transmitting information which infringes the Data Protection Act/General Data Protection Regulations 2018 or any subsequent legislation to the same effect.
- Knowingly allowing the use of Health Board's Digital resources by unauthorised third parties.
- Disabling, altering bypassing, or circumventing any measures put in place by the Health Board to maintain the safe and secure operation of Digital systems and services.
- Failing to follow Health Board advice on how to protect, store, transmit, share, and access sensitive information.
- Failing to purchase and dispose of Digital systems and services in line with Health Board policies.
- To load software / apps for which no legitimate licence is held or software / apps that are unapproved.
- Unauthorised removal or relocation of hardware, software, documentation, or media associated with the Health Board's Digital systems.

Forbidden uses of Digital systems provided by the Health Board are shown below:

- Using another person's identity to appear to be someone else.
- Attempting to gain or facilitate unauthorised access to a computer system or information.
- Attempting to or deliberately corrupting, destroying, or denying access to another user's e-mail, data files, information, Digital system, or service.
- Deliberately accessing, viewing, receiving, downloading, sending, or storing material:
    - with pornographic, offensive, obscene, or indecent content.
    - related to criminal skills or terrorist activities.
    - that promote or encourage discrimination, racism, or intolerance.
    - that facilitates illegal activity in the UK or the host country.
    - that is illegal in the UK or the host country.
    - that is defamatory, threatening, harassing, offensive or abusive.
    - that will, or is likely to, bring the Health Board and its staff into disrepute.
    - that is known to be infected with a virus, worm, Trojan or any form of malicious software or code; that infringes the privacy and data protection rights of individuals.
    - that could endanger the health and safety of any other individual.

The Use of the Organisations Name

If staff or contractors join an Internet forum, they are expected to conduct themselves in an honest and professional manner. Individuals are responsible for what they write and should be always courteous and inoffensive. Staff and contractors are reminded to carefully consider whether to contribute to an Internet forum. Unless currently authorised to do so, staff and contractors are not permitted to write or present views on behalf of the Health Board. For example, staff and contractors cannot join an Internet forum in the name of the Health Board, nor can they design a web site and publish it under the name of the Health Board.

Staff and contractors are also reminded to carefully consider whether to distribute or publish their Health Board e-mail address (such as when registering on third-party websites) as this may lead to the staff or contractors mailbox being targeted by spam (commercial unsolicited e-mail) and phishing (fraudulent e-mails designed to aid identity theft) attacks or the Health Board's systems being subject to attacks designed to prevent legitimate access and cause general disruption (Denial of Service).

E-mails sent using the Health Boards e-mail system include the organisations name and may be held to represent the Health Board and its values. In exchanges of e-mails, staff could accidentally tarnish the image of the Health Board and this policy aims to assist with the understanding of e-mail good practice to avoid this. Use of Digital systems in such a way as to expose the Health Board to risk of claims for defamation is prohibited.

Unintentional Breaches of Digital Security

If staff or contractors find themselves unintentionally viewing material, which may be inappropriate, they must make all reasonable attempts to close the application concerned immediately and inform the Digital Service Desk. A note of this unintentional access will be recorded, and any content filtering rules modified where necessary to ensure that further unintentional access does not take place.

Acceptable Network and System Usage

It is the responsibility of all users to ensure that they adhere to the guidelines laid down in this policy. Before a new user can be allocated an account, they must have signed, understood and agreed to the terms of this policy, indicating that they are aware of their responsibilities. A record of which will be retained by the Informatics Department.

The instructions contained in the policy are special restrictions in force with regard to the Health Board related computer systems and network and, are clarifications or additions to the normal security measures in force within the Health Board. All usual security precautions must be taken in addition to these specific requirements.

Responsibilities

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.

Digital Services

Digital Services will be responsible for maintaining the hardware and software components of the Digital and communications infrastructure and, implementing all necessary technical and physical security controls; in summary the department will: -

- Ensure the availability of Digital services and their supporting infrastructure.

- Managing the security and integrity of data, via anti-virus, mail content, web filtering and content, and anti-spam products.
- Managing and monitoring the e-mail quarantine area and releasing appropriate messages.
- Reporting non-compliance to this policy and other security violations via the Health Board risk management procedure.
- Maintaining technical and engineering safeguards in accordance with this Policy and according to the allocated resources.
- Advise Executive Directors and Line Managers on matters relating to Information security.

Heads of Department / Line Managers

- Ensure all staff read, understand, and abide by this policy and any associated policies.
- Ensure that awareness to this policy is highlighted at their local induction programme.
- Monitoring staff compliance to the policy.
- Monitoring staff time spent on personal use of Digital services and systems.
- Instigating further investigations arising out of suspected misuse.
- Investigation and follow up of misuse in accordance with the Health Board's 201 – All Wales Disciplinary Policy (opens in a new tab).
- Reporting non-compliance to this policy and other security violations via the Health Board risk management procedure.
- Ensure the Digital Service Desk is made aware of new starters, users changing roles and leavers of the Health Board using the appropriate electronic forms on the Digital Services Portal.

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 and contractors who are authorised to access Digital systems have a responsibility to ensure that any usage conforms to policy and legislation relating to Digital security, confidentiality, and data protection.

Digital systems are a business tool that should be treated like any other tool in the workplace. Staff and contractors should be aware that their manager and colleagues may need to gain access to an individual's Digital systems under certain circumstances. Staff and contractors are therefore advised to carefully consider the use of Health Board provided Digital systems for personal use.

Digital systems are a shared resource, and each user has responsibility to learn how to use them appropriately.

Staff must:-

- Comply with this policy and associated guidelines.
- Reporting non-compliance to this policy and other security violations via the Health Board risk management procedure.

Training

All staff will be made aware of this procedure through a communications plan and availability to view on the Health Board Intranet site.

Targeted communications will also be undertaken to the groups identified in the Responsibilities Section.

Support will be provided by Digital Services Department as required to support Health Board staff in ensuring they meet the requirements of this policy.

Information Quality Assurance Policy

Policy information

Policy number: 250
Classification: Corporate
Supersedes: previous versions
Version number: 4
Date of Equality Impact Assessment: 25.02.2026

Approval information

Approved by: Digital Data & Innovation Committee DDIC
Date of approval:
Date made active:
Review date:

Summary of document:
This document is written to provide information on the Policy for ensuring Information Assurance across the Health Board.

Scope:
All Staff, across all areas relating to patient information.

To be read in conjunction with:
837 – Information security policy – opens in a new tab
275 – Secure transfer of personal information policy – opens in a new tab
494 – All Wales email use policy – opens in a new tab
281 – Mobile working policy – opens in a new tab
282 – Network security Policy – opens in a new tab
836 – All Wales Information Governance policy – opens in a new tab

Owning group: Information Governance Sub-Committee
Executive Director job title: Executive Director of Finance

Reviews and updates:
Full review

Keywords; Data Quality, Information, Assurance, Data

Glossary of terms ; IQA – Information Quality Assurance

DRAFT

Contents

Introduction 3
Policy statement 3
Scope 4
Aim 4
Objectives 4
Policy 5
Why does the quality of information matter? 5
Causes of poor information quality 6
Electronic Records and Information Quality 6
Information Quality Assurance through Information Governance 6
Definition of Data Quality 6
The Six Dimensions of Data Quality 7
What is Information Quality Assurance (IQA) 8
Procedures 8
Measurement of Data Quality 8
Local Data Quality Procedures 9
Failure to Maintain Data Quality 9
Training 10
Monitoring 10
Responsibilities 10
Chief Executive 10
Executive Director of Finance 10
Caldicott Guardian 11
Senior Information Risk Officer 11
Digital Director 11
Head of Information Services 11
Clinical Coding Manager via the Data Quality Improvement manager 11
Departmental Data Quality Leads 11
Information Asset/System Owners 12
Information Governance Sub-Committee 12
Data Quality Steering Group 12
Audit Committee 13
Employees 13

DRAFT

Introduction

Good quality information underpins sound decision making at every level in the NHS and most importantly contributes to the improvement of health care. This document outlines the LHBs policy for improving the quality of information in the Health Board. Major drivers include:

- The national service frameworks
- Quality & outcomes assessment in patient care
- The requirements of Service Line Reporting
- Pressure from clinical communities and Ministers to produce high quality information on the quality of care;
- The inability of the LHB to properly monitor quality of service and clinical outcomes.

The starting point of this policy is the recognition that efforts to secure quality must be directed appropriately and that this should start with patient data collected for clinical and operational purposes. Whilst this policy is equally applicable to all information collected and used by the LHB, the initial focus is on information used to support clinical care. Information Quality needs to be addressed within existing working practices and work plans, such as those required to comply with the Information Governance Toolkit rather than as a standalone initiative, though it does need to be managed in a focused way. In particular, the policy seeks to build on two key initiatives:

I. The recognition of, and the drive to reduce, 'adverse health events'
II. The modern approach to error prevention and risk management

'Data quality' is a term that has often been used in the past as if it were interchangeable with information quality, but it is actually a more limited term. Data quality relates to the building blocks of information, i.e. data items. Until data is assembled and interpreted it is not information. Considerable attention has also been focused upon readily measurable aspects of data quality, namely the validity and completeness of data items, whilst harder to measure but perhaps more important aspects in the context of overall information quality, such as accuracy, have been neglected. Data quality is an important component of information quality but there are other components that influence just how useful the information is to a particular user.

Policy statement

This policy provides a framework for Information Quality Assurance (IQA). It also outlines the roles and responsibilities of key roles within the organisation to ensure that the information quality policy is realised.

The tools, techniques and interventions that can lead to improved information quality, the options for their deployment and the process of learning from outcomes, are the elements of the IQA framework. The key application of the framework is the development of IQA templates to support specific work areas and/or information flows. The framework will evolve as our understanding improves, both centrally and locally,

The policy reinforces basic principles, namely that:

DRAFT

- High quality clinical information underpins high quality clinical care;
- Information should be captured once only;
- Information should be accurate and complete the first time it is recorded;
- Information for management purposes should be, wherever practicable, derived from the information collected to support care.

Scope

For use in all areas; by all Staff; for use for all patient information

All authorised staff involved in the collection of data are responsible for accurate and timely records to ensure that Health Board information is correct and available. This is required to ensure seamless care from teams within the Health Board and to enable the Health Board to accurately report activity. This Policy is intended to be a comprehensive guide to all staff involved in managing data associated with Clinical Information Systems both electronic and manual.

The purpose of this policy is to set out the strategic direction for further developing information assurance capability and effectively embedding an Information Assurance culture across the Health Board.

This policy describes the measures that all the Health Board's information systems must implement to achieve appropriate levels of quality in normal operation.

The policy supports the eHealth Policy and aims to guide improvement in three broad areas: availability, integrity and confidentiality.

Confidentiality: We protect information from unauthorised disclosure and ensure that we only hold information that we need and have a right to retain

Integrity: We ensure that the data we hold is correct, current, & can only be modified by authorised users with clear audit trails

Availability: We ensure that the data needed is there when its needed

Aim

The aim of this document is to:

- Define the organisational structures within which data quality is managed, monitored, reported and improved.
- Outline main responsibilities and accountabilities, together with the appropriate reporting mechanisms for providing feedback
- Confirm Health Board policies and procedures relating to data quality
- Allocate responsibility for reviewing, updating and amending such documents, with an established timetable and monitoring system, ensuring compliance with written policies and procedures

Objectives

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

- Mandate the use of validated NHS Numbers as the unique identifier on all patient records

DRAFT

- Ensure compliance with data standards and all legal obligations
- Create a framework within which information quality issues can feed into training programmes, to address any recurrent problems
- Raise awareness of information quality issues with clinical and nursing staff, and ensure that information systems meet clinical needs.
- Compliance with Freedom of Information legislation, which substantially increases the public visibility of information quality issues.

Policy

Why does the quality of information matter?

High quality information is vital to safe and effective patient care and for this purpose 100% accuracy 100% of the time must be the goal. The model of care is changing and broadening to rely upon inter-disciplinary care pathways and clinical networks that transcend organisational boundaries. Information is increasingly used in new and different ways, in a range of different settings, underpinning the continuity and quality of care, for example information provided through forecasting and machine learning models are only as good as the underlying data they have learnt from. These developments create pressure to improve the quality and standardisation of existing information collections but also lead to new and greater demands for information to be made available to different users.

Poor quality information impacts directly upon each and every use made of that information. For example:

- In clinical care, poor quality information may:
    - o result in patients being harmed or distressed
    - o undermine the Health Board clinicians place in recorded information
- In disease surveillance, poor quality information may:
    - o undermine the validity of conclusions drawn
    - o obscure facts and put the public at risk
- In medical research, poor quality information may:
    - o undermine the credibility of evidence based care
    - o cause the validity of findings to be questioned
- In health service management, poor quality information may:
    - o prevent understanding of best clinical practice
    - o result in resources being poorly targeted

Clinical audit and governance processes require that clinical practice be monitored and reviewed and the performance management of clinicians is receiving increased attention. All this activity is dependent upon the availability of high quality information. High quality information should be produced as part of the routine daily activity within a hospital, or other healthcare setting.

DRAFT

Causes of poor information quality

Poor information quality may be due to errors in systems design, the way the information is processed or the way it is interpreted or a combination of all 3. Whilst error is not the sole cause of poor information quality it is by far the most significant. The prevention, and where this fails, detection and correction of error, is a key goal of the Information Quality Assurance Policy.

Poor information quality may be due to errors in systems design, the way the information is processed or the way it is interpreted. Errors will be taken seriously within the Health Board and with the use of DATIX the Health Board will be able to assess the numbers of adverse events and also the lessons learnt from such occurrences. These lessons will form part of the workplan for Information Quality Assurance within the Health Board.

Most errors can be attributed to faulty systems, unhelpful processes and poor training and guidance for staff. This policy therefore needs to be set within a programme of work that seeks to improve organisational performance across a wide range of traditionally distinct disciplines.

Electronic Records and Information Quality

Over recent years attempts have been made to introduce universal electronic medical records. Through the National Programmes in the NHS there is now a centrally driven concerted effort to have an electronic record for every patient.

Amongst the benefits electronic records bring is the potential for a fundamental improvement in information quality. However, without agreed standards for recording and exchanging health data, computerisation can significantly increase the risk of poor quality data leading to misinterpretation and adverse events. Equally, the skills to effectively capture information, manipulate data, present data meaningfully and realise the benefit from improved information quality must be developed and effectively supported.

Information Quality Assurance through Information Governance

It has become clear that whilst data, information, quality, information quality and data quality are all frequently used terms, there is no general agreement on definitions.

Whilst this policy is unlikely to resolve this, in order to avoid confusion and unhelpful debate it is necessary to clarify the way that these terms are used here and to set them within the, perhaps less familiar, concepts of information governance and information quality assurance.

Data; Facts, readings, measurements – items that are essentially ‘value free’
Information; Data that has been interpreted or to which commentary has been added by a user for a purpose, making it ‘value-laden’.
Quality (has two aspects); i. The characteristics that meet user needs and thereby provide user satisfaction. Ii. The absence of deficiencies that result in user dissatisfaction.

Definition of Data Quality

According to J.M. Juran (1951), data are of high quality “if they are fit for their intended uses in operations, decision making and planning.” Alternatively, data is deemed of high quality if it correctly represents the real-world construct to which it refers. Within an organisation, acceptable data quality is crucial to operational and transactional processes and to the reliability of business analytics / business

DRAFT

intelligence reporting. Data quality is affected by the way the data is entered, stored, analysed, managed and reported.

Consideration of information and data quality are made more complex by the general agreement that there are a number of different aspects to information/data quality but no clear agreement as to what these are. When assessing data within any dataset, it is important to acknowledge that there are several dimensions to its quality, all of which impact on the usability of the information it represents. These can be summarised as follows:

The Six Dimensions of Data Quality

Data quality in essence is the foundations of information. The six dimensions of data quality are defined as:

- Timeliness: Data must be available quickly and frequently enough to support information needs and to influence the appropriate level of service or management decisions.
- Completeness: Data requirements will be clearly specified and based upon the information needs of the organisation and data collection processes matched to these requirements.
- Accuracy: Data should be sufficiently accurate for its intended purposes and captured as close to the point of activity as possible.
- Consistency: Data will reflect stable and consistent data collection processes across collection points and over time. Managers and stakeholders should be confident that progress toward performance targets reflects real changes rather than variations in data collection methods.
- Precision: Data captured will be relevant to the purposes for which it is used, capable of evolving to reflect changing needs. Quality assurance and feedback processes are needed to ensure the quality of such data.
- Validity: Data will be recorded and used in compliance with relevant requirements, including the correct application of any rules or definitions.

When addressing the issue of data quality, it is common for only one or two of these dimensions to be taken into account. However, to gain a full understanding of the quality of data, all of the above dimensions need to be considered as a whole, even if this is not always done at the same time.

The dimensions arguably increase in complexity and detail as one moves from examining the basic dimensions focussed on whether the data is valid and submitted on time, to whether the data actually paints an accurate and consistent picture of the activity it represents.

As it is not always possible, for a variety of reasons, to adhere to all the principles in every case, a judgement must be made by each information Asset Owner to the relative importance of individual data items. This will depend on the intrinsic nature of the data, as well as the use to which the application is put. High priority items could include important clinical details such as allergies, chronic disease factors or current medication. Other examples might include identification data, financial transactions, etc. However, lower priority items should not be considered as optional for data collection (unless defined as such), merely that the consequences of being unable to collect the data are less serious.

DRAFT

What is Information Quality Assurance (IQA)

Information quality assurance is a cycle process that aims to assess performance and deliver improvement. Improvements relate both to the quality of the information but also, a means of developing and reinforcing an information quality culture, to improve compliance with information quality standards. In line with the approach adopted for broader information governance, these standards relate to:

a) The management of Information Quality
b) The requirements for systems that process information
c) Organisational processes and working practices
d) The training and guidance that should be provided to staff

IQA requires the assessment of compliance with information quality standards and an assessment of outcomes in terms of improved information quality. A generic model of information quality with standards, guidelines and measurement tools is necessary. Whilst the assessment of compliance against information quality standards is relatively straightforward – attainment levels are either achieved or they are not –the measurement of information quality is more complicated. On the one hand information quality can be measured with subjective perceptions (qualitative) from information users. On the other hand there are approaches developed on the basis of quantitative characteristics such as completeness and accuracy.

IQA proposes a measuring system for information quality that assesses both qualitative and quantitative aspects in the context of key information pathways.

Procedures

The complex nature of patient data: the volume, circulation, confidentiality requirements, legal obligations and associated administrative and management issues makes it essential that procedures are in place which will ensure that the patient and the Health Board are protected from risk. The Health Board is committed to ensuring that procedures are in place to minimise risk and provide an efficient and effective information service through access to high quality patient data.

Measurement of Data Quality

The assessment of whether data quality is of sufficiently high standard is dependent on the data in question and the purpose for which it is collected and utilised. Typical measures may include the following:

- All mandatory data collection is complete, accurate and up to date
- Manual data is readable and stored in a structured filing system
- Duplication of records is minimised
- Data is collected in accordance with documented procedures and guidelines meeting national/local standards
- Percentage of completed and valid coded data regularly monitored
- Random audits on data for accuracy, timeliness and completeness

DRAFT

A scoring mechanism will be used to benchmark certain systems and modules against each other in an attempt to provide information asset owners and secondary users of the data a picture of the data quality of the datasets they are using.

Local Data Quality Procedures

All local procedures should comply with and/or map back to national data standards and coding and will be subject to control processes within the Health Board as well as to external scrutiny.

Each information system must implement well documented and clearly understood local data quality procedures with a view to ensuring that high level of data quality is maintained at all times.

It is the responsibility of the relevant named Information Asset Owner to ensure that local data quality procedures are produced and maintained and monitored. Manual recording of data is not excluded from this process.

Procedures should assess levels of risk associated with different data items, identifying high priority data items and noting the consequences of missing data.

Procedures must specify where applicable what enforcement mechanisms are available to ensure adherence.

Data quality procedures should be reviewed on a regular basis to ensure that they still meet the business requirements of the Health Board.

Regular auditing against local internal targets to monitor data quality compliance, and clear processes on handling poor data quality outcomes to ensure improvement.

Where data errors and/or corruption of data are identified, clear processes must be in place to identify implications and immediate correction of such data.

In certain circumstances, systems may have specific resources allocated for the maintenance of data quality. Local data quality procedures must specify under what circumstances those resources should be used.

Failure to Maintain Data Quality

All instances of failure to maintain adequate data quality in Health Boards systems (for example, by entering incorrect data) will be dealt with as follows:

- First Instance – The individual responsible for the data quality failure will be contacted to inform them of the error and will be offered further training.
- Second Instance – The individual responsible for the data quality failure and their Line Manager will be contacted to inform them of the error and the individual will be notified that they will need to attend further training. A support process will be developed around the individual along with a monitoring and validating routine of the individual's data entry.
- Third Instance – The individual responsible for the data quality failure and their Line Manager will be contacted to inform them of the error. Access to the relevant information system will be reviewed for the individual concerned until they have successfully completed further training and further adjusted working practices to minimise future errors.

DRAFT

- Fourth and Subsequent Instances – The individual responsible for the data quality failure and their General Manager will be contacted to inform them of the error. The Divisional Manager will be expected to consider initiating the Health Board's Capability Procedure to deal with the inability of the individual to maintain adequate data quality.

Training
Training of staff in data quality awareness, security and confidentiality issues, and use in electronic systems is a cornerstone of promoting data quality across the Health Board.

1. Established processes will enable training needs to be linked to any issues highlighted during data validation, to ensure common errors in data recording are eliminated at both individual and group level
2. Comprehensive training records will be kept to ensure progress can be demonstrated, and to assist in recall of staff in the future, including user evaluation feedback to monitor the effectiveness of the training programmes available
3. Training documentation will include a section on security and confidentiality, and will provide guidance over relevant data definitions and the importance of validating, correctly classifying and recording activity information
4. Training in understanding and utilising information should also be provided for the Health Board's decision makers
5. All staff will be provided with appropriate and relevant training before they are issued with access to the electronic systems

Monitoring
The Health Board will, as a matter of routine, monitor performance by collecting and processing data according to nationally defined standards and provide appropriate feedback to all staff.

Internal data quality spot checks and local audits are undertaken by the Data Quality Improvement Manager. The Health Board will put in place mechanisms to ensure there is feedback to the individual divisions where necessary, on data quality issues and of any remedial actions that may be needed to improve the quality of the data.

Responsibilities

Chief Executive
As Accountable Officer, the Chief Executive has overall responsibility for ensuring the health board has appropriate WCDs in place. These WCDs must comply with legislation, meet mandatory requirements, and provide services that are safe, evidenced-based and sustainable.

Executive Director of Finance
Formal responsibility for Data Quality lies with the Executive Director of Finance who is responsible for reporting on data quality to the Board.

DRAFT

Caldicott Guardian

The Health Board's Caldicott Guardian has a responsibility for reflecting service users' interests regarding the use of patient identifiable information and is responsible for ensuring patient identifiable information is shared in an appropriate and secure manner.

Senior Information Risk Officer

The accountable director for the policy is the Senior Information Risk Officer (SIRO). The SIRO takes ownership of the Health Board's information risk policy and acts as an advocate for information risk on the Board. The SIRO works closely with Information Asset Owners to ensure Health Board information systems are fit for purpose.

Digital Director

The Digital Director has delegated professional responsibility for information assurance and data quality within the Health Board. They are also responsible for the Data Quality Team and their annual programme of work, clinical information systems and the reporting of management information. They act as an advocate for Data Quality and is responsible for reporting on Data Quality to the Executive Director of Finance.

Head of Information Services

The Head of Information Services has delegated responsibility for the management of data quality across the Health Board. Key roles will be the promotion of data quality and include:

- Providing direction and responsibility for the Data Assurance Lead
- Highlighting the importance of data quality at Management Team, Operational Services Managers meetings and other relevant committees and groups

Data Assurance Lead via the Data Quality Improvement manager

The Data Assurance Lead via the Data Quality Improvement Manager is directly responsible to the Head of Information Services for the day-to-day management of data quality across the Health Board.

- Ensuring the quality of data produced meets the requirements of the Health Board and ensuring sufficient mechanisms are in place to ensure this happens
- Developing a culture where there is an appreciation of the importance of high standards of data quality across all relevant staff groups, involved in the production and collation of data
- Ensures that through increased confidence in the quality of data reports and analyses of the data, they can be relied upon for use in better management and clinical decision making
- Provide all relevant staff with sufficient guidance and appropriate training to ensure data is collected in a consistent and accurate manner, ensuring training is updated as required
- Establish a departmental/unit data quality group to identify and address data quality issues which feeds into Health Board wide groups such as Information Asset Owners group, Transformation Working Groups, Directorate meetings etc

Departmental Data Quality Leads

Health Board Managers have a responsibility for ensuring that staff working for them:

- Record accurate and complete data in a timely manner
- Are aware of their responsibilities with regard to checking and updating any inaccuracies and missing data items in service user records

DRAFT

- Address any data quality issues as soon as possible and escalate appropriately
- Ensure all local procedures are documented and updated regularly and are available to all staff
- Ensure all staff are familiar with and adhere to current legislation, Health Board and local policies, procedures etc.
- Ensure all staff meet the Health Board's Data Quality Standards
- Monitor staff competencies and training needs and ensure staff attend appropriate training including refresher as appropriate for both clinical information systems and record keeping/data quality.
- Ensure staff deal with data in a secure and confidential way to comply with Information Governance standards.

Information Asset/System Owners

IAO's have responsibility for the quality of the data held within their systems. This will be achieved by setting data quality standards for the systems and routinely measuring performance against those standards. Where the standard is not being achieved, it is the responsibility of the Information Asset Owner to put in place an action plan to address. Where this requires Health Board wide action, the IAO will be supported by the Assistant Director of Informatics to ensure that the action plan is agreed and implemented at the appropriate level within the Health Board.

For each information system in the Health Board, there is a named person who is ultimately accountable for the quality of information held in that system. This register of system responsibilities, informed by the Information Asset Register, will be monitored and updated on a routine basis. In accordance with the Policy, the named individual will be responsible for:

- Reviewing policies and procedures and ensuring they are kept up to date in line with system changes
- Ensuring compliance with written policies and procedures – via spot check, and rolling programmes of audit
- Ensuring staff receive adequate training in the use of the system
- Monitoring and communicating error rates – informed via the System Administrators own localised Data Quality regime
- These responsibilities should be explicitly identified in the job descriptions for these posts and should form part of the post holder's Appraisal and Development Review.

Information Governance Sub-Committee

The Information Governance Committee is responsible for monitoring the outcomes of the Data Quality Steering Group Audits, Action Plan etc

Data Quality Steering Group

The Data Quality Steering Group will meet on a quarterly basis and is accountable to the Information Governance Sub-Committee.

The group is made up of representatives that have responsibility within their division to cascade relevant information to staff and to report any data quality issues as appropriate to the attention of

DRAFT

divisional managers or to the Data Quality Steering Group as appropriate, to implement measures to address them, ensure the Data Quality Policy is followed locally, Participate in audits etc. as requested by the Steering Group.

The group has overall responsibility for the implementation of this policy and the Data Quality work plan; it will manage and monitor the Data Quality Report, audit reports and action plans and feedback to the Information Governance Sub-Committee. It is the responsibility of the Divisions to ensure representation and attendance at the steering Group and to participate in audits as appropriate.

The Data Quality Steering Group will oversee and monitor the progress of this policy and the annual Data Quality Action Plans.

Audit Committee
The Audit Committee receives assurance in respect of data quality from Internal and External Audit

Employees
All Health Board staff including clinicians and administrative staff, who collect and record data both manually or on the Health Board clinical information systems must:

- Ensure timely, accurate and complete recording of data in service user records
- Update any inaccuracies and/or missing data in service user records
- Address any data quality issues as soon as possible and escalate appropriately
- Be aware of and comply with legislation, Health Board and local procedures etc.
- Ensure they meet the Health Board's Data Quality Standards
- Monitor own competencies and access training where necessary both for clinical information systems and record keeping/data quality
- Ensure all data is dealt with in a secure and confidential way to comply with Information Governance standards.

DRAFT