Corporate Records Management Policy

Policy information

Policy number**:** **347**
Classification: Corporate
Supersedes: Previous Versions
Version number: 4
Date of Equality Impact Assessment: 19.02.2025

Approval information

Approved by: DDIC (Digital, Data and Innovation Committee)
Date of approval: 22.04.2025
Date made active: 23.04.2025
Review date: 22.04.2028

Summary of document:
The Corporate Records Management Policy sets out best practice for the creation, management, retention and disposal of corporate records

Scope:
This policy relates to all non-clinical operational records held in any format by HDUHB. These include: all administrative records (e.g., personnel, estates, financial and accounting records, notes associated with complaints, etc.).

To be read in conjunction with: (opens in a new tab)
193 – Retention and Destruction of Records Policy (Including Health Records) (opens in a new tab)
191 – Health Records Management Strategy (opens in a new tab)
192 – Health Records Management Policy (opens in a new tab)
291 – Personnel Employee Record Management Policy (opens in a new tab)
836 – All Wales Information Governance Policy (opens in a new tab)
238 – Information Governance Framework (opens in a new tab)
172 – Confidentiality Policy (opens in a new tab)
837 – All Wales Information Security Policy (opens in a new tab)
186 – Business Continuity Planning Policy (opens in a new tab)
173 – Freedom of Information Act Policy (opens in a new tab)

Patient information:
Not applicable

Hywel Dda University Health Board
Owning group:
Information Governance Sub-Committee

Executive Director job title:
Director of Finance

Reviews and updates:
Version 1- 25.6.2013
Version 2 – 25.4.2022
Version 3 – 22.4.2025

Keywords
Records Management, Corporate Records

Glossary of terms

Corporate records: are records (other than health records) that are of, or relating to, an organisation's business activities covering all the functions, processes, activities and transactions of the organisation and of its employees.

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". BS ISO 15489-1: 2001 Information and documentation – Records Management

Records management is about controlling the organisation's records to ensure authenticity, reliability, integrity and usability.

Welsh IG Toolkit: is an online self-assessment tool that allows organisations to measure their performance against the IG Standards and Regulations. All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practising good data security and that personal information is handled correctly.

Retention Schedule: is a document setting out what records the HDUHB 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

Critical Records: are records without which the HDUHB could not effectively function or be reconstructed in the event of a disaster. These include records the HDUHB requires to recreate its legal and financial status, to reserve its rights and to ensure that it can continue to fulfil its obligations to its stakeholders

Metadata: is the information attached to a record which describes technical aspects of the creation, use and retention of the record and its relationship with other records.

Contents

Introduction

Hywel Dda University Health Board (HDUHB) is dependent on its records to operate efficiently and account for its actions. An effective records management system is critical in the provision of effective and safe care to patients and to assist in the efficient running of the organisation. Corporate services must ensure that all records are created and maintained in accordance with legislations and standards guidance.

Policy Statement

This policy defines a structure for HDUHB to ensure adequate records are maintained and that they are managed and controlled effectively. This will support the confidentiality, integrity and availability of all information held and/or used by the HDUHB.

Scope

This policy relates to all non-clinical operational records held in any format by HDUHB. These include: all administrative records (e.g., personnel, estates, financial and accounting records, notes associated with complaints, etc.).

This policy applies to all staff employed (including volunteers) by or contracted to HDUHB and includes experts who the HDUHB might call upon in consultation.

Aim

This policy will define the way in which records will be managed throughout the organisation.

Objectives

This policy aims to ensure that records must be designed, prepared, reviewed and accessible to meet the required needs. Care treatment and decision making is supported by structured, accurate and accessible records documenting the conversation between people and health professionals and the resulting decisions and actions taken and reflects best practice founded on the evidence base.

The policy will ensure the following:

- **Records are available when needed** and shared when appropriate - from which HDUHB is able to form a reconstruction of activities or events that have taken place.
- **Records can be accessed** - records and the information within them can be located and displayed in a way consistent with its initial use, and that the current version is identified where multiple versions exist.

- **Records can be interpreted** - the context of the record can be interpreted: who created or added to the record and when, during which business process, and how the record is related to other records
- **Records can be trusted** – the record is accurate, up-to-date, complete and contemporaneous in accordance with professional standards and guidance. It reliably represents the information that was actually used in, or created by, the business process, and its integrity and authenticity can be demonstrated.
- **Records can be maintained through time** – the qualities of availability, accessibility, interpretation and trustworthiness can be maintained for as long as the record is needed, perhaps permanently, despite changes of format.
- **Records are secure** – they are stored securely and are secure from unauthorised or inadvertent alteration or erasure, that access and disclosure are properly controlled, and audit trails will track all use and changes. To ensure that records are held in a robust format which remains readable for as long as records are required.
- **Records are retained and disposed of appropriately** - using consistent and documented retention and disposal policies, which include provision for appraisal and the permanent preservation of records with archival value; records should only be destroyed with the consultation or approval of the relevant body/person.
- **Staff are trained and have guidance to refer to** - so that all staff are made aware of their responsibilities for record-keeping and record management.

Implementation of the policy

Record Creation

The HDUHB will apply good records management principles to information and records created or received as part of its activities.

- **Ownership** All records created by employees of the HDUHB in the course of their work remain the absolute property of HDUHB unless otherwise specifically agreed.
- **Evidential significance** Adequate records of all activities will be maintained to account fully and transparently for all actions and decisions of HDUHB.
- **Accuracy and authenticity** The HDUHB shall ensure records are complete and accurate and that the information they contain is reliable and its authenticity can be guaranteed
- **Accessibility** Records should be created using clear and unambiguous language appropriate to the subject, suitable fonts and font size, and relevant corporate templates where appropriate, so that records can easily be read and understood.
- **Legislative compliance** All the records created by the HDUHB may be used in requests for information under the Freedom of Information Act, Environmental Information Regulations and Data Protection Act. Employees must not create, delete or alter information that has been requested under legislation.

Hywel Dda University Health Board
Records Retention and records disposal
HDUHB will store records to maximise efficiency, reduce costs, enable sharing and minimise risks. All information must be held in secure environments regardless of medium. All records are subject to the HDUHB retention schedule found in 193 – Retention and Destruction of Records Policy (Including Health Records) . Any record which might be used as evidence in a legal or regulatory process should be subject to access and audit trail controls to ensure that its reliability, integrity and evidential value can be demonstrated.

Responsibility for record keeping All employees are responsible for the protection of records they process. It is employees' responsibility to ensure adequate secure storage arrangements are provided which protect records from unauthorised or inadvertent alteration or destruction, controls access and disclosure with appropriate audit trails, and maintains the records in a robust format which remains readable so long as the information and records are required. They should work with the Information Governance Team to achieve this outcome.

Arrangement of records Information will be arranged using appropriate naming conventions so they can be retrieved quickly and efficiently for the length of their lifecycle. Each service should take into account the legal and regulatory environment specific to their area of work.

HDUHB's Classification Scheme A classification scheme is a way of organising records to make the management of them easier. Classification schemes consist of classes that represent broad functions sub-divided into sub-classes. The HDUHB will develop a corporate classification scheme for the storage of records, and to facilitate the application of access control and retention schedules.

Access Control The security of the HDUHB records is essential. The security controls in place to safeguard the records of HDUHB are detailed in the 837 – All Wales Information Security Policy (opens in a new tab).

Records Storage
Storage of physical records Storage accommodation for physical records should protect the records from damage, accidental loss or destruction, and prevent unauthorised access. Records storage facilities, shelving and equipment must meet occupational health and safety requirements. Physical records that must be retained for legal or business purposes but are no longer required day to day should be placed in the care of one of the HDUHB approved storage areas, with access to the records provided on demand. Criteria for storage is detailed in the Corporate Records Management Procedure.

Storage of electronic records HDUHB will continue to develop appropriate solutions for the storage and preservation over time of electronic records in a structured and managed environment. The arrangements in place for managing electronic information in every service should be agreed with ICT and the IG, clearly documented and periodically reviewed.

Disposal and transfer Services must follow the arrangements for appraisal and selection of records for disposal and transfer laid out in the Corporate Records Management Procedure. All records should be managed in accordance with the HDUHB Retention Schedule outline in 193 – Retention and Destruction of Records Policy (Including Health Records) – opens in a new tab. Any divergence from the schedule should be authorised by the SIRO. Documentation of the disposal/transfer of records, for example to an external storage facility or to a Place of Deposit, must be completed and retained for audit purposes on the HDUHB destruction/transfer log. Mechanisms for the regular transfer of records selected for permanent preservation should be in place and agreed with HDUHB **Senior Corporate Records Management Officer.** Wherever records are held on corporate electronic data & records management systems [EDRMS], consideration must be given as to whether automated system retention, disposal & review dates should be used or whether manual ones should be given. Records subject to an open request under the Data Protection Legislation or Freedom of Information Act must not be destroyed.

Use of Records

Using physical records

Physical records are the responsibility of the user, who should ensure their safety and security at all times. Records should not be removed from the HB's premises except in cases of necessity, when adequate and appropriate security measures should be employed.

Use of the Internal and Off-site Storage

All records stored should be held within the HDUHB internal storage areas. The IG Service or Senior Corporate Records Management Officer should be contacted for advice.

Digital continuity

Electronic records are dependent on technology to access and read them. The IG service will work with ICT to ensure that information created digitally is accessible for as long as necessary. This may involve the use of non-proprietary formats and the use of PDF/A standards where necessary.

Critical Records

In the event of a disaster critical records will have the highest priority for preservation, rescue and / or restoration. The HDUHB must be aware of its critical records and services should have contingency plans in place.

Business Continuity and Recovery

If records are damaged the service area must contact the **Senior Corporate Records Management Officer** for immediate records recovery. Services must also undertake a risk assessment with the Senior Corporate Records Management Officer to decide whether restoration would be beneficial after the initial recovery of records. Advice should be sought from the IG Service or Business Continuity Service.

Risk Management
Records form part of the corporate assets of the HDUHB, and risks relating to confidentiality, integrity and availability of records must be managed appropriately. Risks relating to the management of records should be incorporated into the HDUHB risk management framework and included on each service's risk register for local management and escalated through their management structure where appropriate.

Partnership Working
Information sharing protocols will be drawn up with partners to reflect agreement in data sharing. The HDUHB will ensure that any partners involved in projects or the delivery of services have proper management with agreed standards in place for records created under partnership initiatives.

- **Partnership working where HDUHB is the lead partner:** Core records will be retained and managed by HDUHB under retention schedules agreed by the HDUHB. HDUHB's Corporate Records Management Policy will apply.
- **Partnership working where another organisation is the lead partner:** Core records will be retained by the other organisation. The HDUHB will identify and manage records relating to its role in the partnership under retention schedules agreed by the HDUHB.
- **Partnership working where no single organisation is the lead partner:** The HDUHB will ensure that an agreement is in place with one partner for the management of core records.

Responsibilities

Chief Executive – The Chief Executive takes overall responsibility for the HDUHB information governance performance and is required to ensure that:

- the HDUHB can demonstrate accountability against the requirements within the Data Protection Act;
- decision-making is in line with the HDUHB policy for information governance and any statutory provisions set out in legislation;
- the information risks are assessed and mitigated to an acceptable level and information governance performance is continually reviewed;
- suitable action plans for improving information governance are developed and implemented;
- ensure IG training is mandated for all staff and is provided at a level relevant to their role.

To satisfy the above, the Chief Executive has delegated this responsibility to the Director of Digital who will be accountable for the HDUHB overall information governance arrangements.

Senior Information Risk Owner (SIRO) – The Director of Finance is the identified Senior Information Risk Owner (SIRO), and will take ownership of information risk. The Director of Digital is appointed as Deputy SIRO. The SIRO is a key factor in successfully raising the profile of information risks and embedding information risk management into the HDUHB culture. The SIRO is the Chair of the Information Governance Sub-Committee.

Caldicott Guardian - The Medical Director has been nominated as the HDUHB Caldicott Guardian and is responsible for protecting the confidentiality and reflecting patients' interests regarding the use of patient identifiable information. The Caldicott Guardian is responsible for ensuring patient identifiable information is shared in an appropriate, ethical and secure manner.

Data Protection Officer – The Head of Information Governance has been appointed as the Data Protection Officer as required by UK Data Protection Legislation. This role plays a key part in fostering a data protection culture to help implement essential elements of the Data Protection Legislation such as, principles of data processing, data subjects' rights, data protection by design and by default – privacy impact assessments.

The Head of Information Governance – The Head of Information Governance will be responsible for the development, communication and monitoring of policies, procedures and action plans ensuring the HDUHB adopts information governance best practice and standards. This role will report to the Director of Digital and will be supported by the Information Governance Team who will also work in collaboration with the Information Asset Owners.

Director of Digital – The Director of Digital has overall responsibility for the technical infrastructure to ensure the security and data quality of the information assets and systems held within the Board.

Head of Digital Operations – The Head of Digital Operations is the HDUHB identified IT Security Lead and provides expert technical advice on matters relating to IT Security and ensures compliance and conformance against the NHS Wales Code of Connection and NIS Directive.

Health Records Manager – This role is responsible for the overall management and performance of the Health Records Service within HDUHB including the provision of organisation-wide access to health records.

Executive Director/Secondary Care Director/Area Director - Each Director is responsible for the information within their Directorate and therefore must take responsibility for information governance matters. In particular they must appoint an Information Asset Owners.

Information Asset Owners (IAOs) – The Information Asset Owner's role is to understand what information is processed by their department i.e., what information is held, added, removed, how it is moved, who has access to it and why. As a result, they are able to understand and address risks to the information, to ensure that information is processed within legislative requirements. The IAOs work with

the IG Team to ensure compliance with the HDUHB Retention Schedule, corporate IG policies, procedures, standards, legislation and to promote best practice.

Information Asset Administrators (IAAs) – The Information Asset Administrator will recognise actual or potential security incidents, consult with their IAO on appropriate incident management and ensure that information asset registers are accurate and up to date including retention review dates for declared records.

System Owners – The System Owners will be responsible for identifying and managing system risks; understand procurement requirements around contracts and licencing; put in place and test business continuity and disaster recovery plans, control access permissions and ensure the system asset record is regularly reviewed and updated on the asset register.

Freedom of Information (FOI) Officer - The Freedom of Information Officer is responsible for ensuring all Information requests are fulfilled within the statutory regulations. The FOI officer will work with departments to ensure that information required in response to requests is managed in the appropriate manner and is stored until such a time as it is no longer required to be protected by the requirements stated under the FOI Act.

Senior Corporate Records Management Officer - The Senior Corporate Records Management Officer is responsible for the management of corporate records, including training, destruction of records, and transfer of records to the HDUHB Places of Deposit and for oversight of the selection of records for permanent preservation.

All Staff - All employees, contractors, volunteers and students working for or supplying services for the HDUHB are responsible for any records or data they create and what they do with information they use.

Staff must attend mandatory information governance training and/or refresher/ awareness sessions to maintain their knowledge and skills every two years.

All staff have a responsibility to adhere to information governance policies and procedures and standards which are written into the terms and conditions of their contracts of employment and the organisations Staff Code of Conduct.

Third Party Contractors – appropriate contracts and confidentiality agreements shall be in place with third parties where potential or actual access to the HDUHB confidential information assets is identified.

Monitoring

Monitoring of this policy will be the joint responsibility of the Director of Digital and the Head of Information Governance. The policy will be disseminated throughout the organisation and training initiated. Escalation of issues will be through the Information Governance Sub-Committee to the Board as per the HDUHB Standing Orders.

This policy will be reviewed every 3 years. Review maybe invoked earlier if new legislation, new standards, or codes of practice are introduced.

Resources

The Information Governance Team should have sufficient resource to ensure the HDUHB remains compliant against its legislative requirements and timescales.

Directorates should ensure that their appointed, Information Asset Owners and System Owners have sufficient time and resource to execute the requirements within these job roles.

Training

All staff within HDUHB, are mandated to undertake Information Governance, Records Management and Cyber Security training. This training must be renewed every two years.

In addition to induction and mandatory training requirements, there are certain posts/job roles which require specialised IG training in order to fulfil their duties, for example: Caldicott Guardian, DPO, SIRO, IG Team, IAO, IAA, System Owners and staff who handle subject access requests.

The Information Governance Team are responsible for developing and delivering the IG training programme which is supported by a 3 year IG Training Strategy and action plan.

Audit

The HDUHB will respond to the Welsh Information Governance Toolkit on how we manage the processing of personal data, in particular looking at: Governance & Accountability; Records Management and Requests for Information.

The Information Governance Team will carry out audits to:

- review IG compliance across departments and teams within HDUHB;
- review and risk assess Information/System asset register submissions;
- assess the data protection impact of all new or revised system or service development.

References

The legislation and guidance supporting this policy includes:

- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Human Rights Act 1998
- Access to Health Records Act 1990
- Public Records Act 1958
- The Computer Misuse Act 1990
- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2000
- Records Management Code of Practice for Health and Social Care 2022 Caldicott: Principles into Practice (C-PIP) Foundation Manual for Caldicott Guardians
- Welsh IG Toolkit
- International Standard ISO, 15489, Records Management
- Information Security assurance - ISO 27001