

INFORMATION GOVERNANCE SUB-COMMITTEE COMMITTEE UPDATE REPORT

Date of last meeting: 26 March 2025

Quoracy: Met

Report by: Anthony Tracey, Digital Director, Chair

KEY DISCUSSION POINTS AND MATTERS TO BE ESCALATED FROM THE DISCUSSION AT THE MEETING:

Alert (may require discussion)

Information Governance Sub-Committee wish to **alert** members of the Digital, Data and Innovation Committee that:

- **Corporate Records Management Policy (Policy Number 347)** – the Sub-Committee approved the updates changes to the policy, following confirmation that the revised policy has been through the policy 190 process and been out for global consultation (Appendices 1 and 2).
- **Information Governance Toolkit Submissions for 2024/25** – the Sub-Committee approved the submissions of the Information Governance Toolkits for the Health Board, and Managed Practices.

Advise (to monitor)

Information Governance Sub-Committee had no matters that they wish to **advise** members of the Digital, Data and Innovation Committee that:

Assure (to note)

Information Governance Sub-Committee wish to **assure** members of the Digital, Data and Innovation Committee that:

- **IGSC Terms of Reference** – Reviewed and approved by the Sub-Committee (Appendix 3)
- **Corporate and Medical Records Storage Assurance Report** – The Sub-Committee received an update report on the storage of records within external facilities. The Sub-Committee were pleased to note the number of records that have been moved back to the internal records facilities reducing our reliance on external suppliers.

Review of Risks

The Sub-Committee reviewed the two risks which are aligned to Sub-Committee. As part of its review, the Sub-Committee considered the status of each risk, and the current score was deemed in tolerance. However, the Sub-Committee did recognise the work that had been done by the Information Governance and Health Records Teams in reducing the risk of inappropriate storage facilities.

Sharing of learning

The Information Governance Sub-Committee had no matters to alert the Group on this occasion.

Recommendation

The Committee is asked to:

- **APPROVE** the Corporate Records Management Policy (Policy Number 347) (Appendices 1 and 2)
- **APPROVE** the Information Governance Sub-Committee Terms of Reference (Appendix 3)
- **NOTE** the Information Governance Sub-Committee Report and **TAKE ASSURANCE** from the actions and oversight of the Sub-Committee.

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:

Date made active:

Review date:

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 -

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	4
Policy Statement.....	4
Scope.....	4
Aim	4
Objectives	4
Implementation of the policy	5
Record Creation.....	5
Records Retention and records disposal	6
Records Storage	6
Use of Records.....	7
Using physical records.....	7
Use of the Internal and Off-site Storage.....	7
Digital continuity	7
Critical Records.....	7
Business Continuity and Recovery.....	7
Risk Management	8
Partnership Working.....	8
Responsibilities.....	8
Monitoring	11
Resources.....	11
Training	11
Audit.....	11
References.....	12

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.

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

Hywel Dda University Health Board
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

Equality Impact Assessment (EqIA) Screening Template

When to complete an EqIA Screening

An EqIA Screening Template must be completed when reviewing, changing and developing procedures/ proposals/ projects/ policies. This is a first step and is used to consider whether there are any negative impacts that may arise.

Purpose of an EqIA Screening Template

The purpose of this short exercise is to ensure that you have shown appropriate due regard when considering the impact for people with protected characteristics in your decision making. The screening process is designed to help you consider the circumstances and to inform evidence-based decisions.

If the proposal is of a significant nature and it is apparent from the outset that a full EqIA will be required, then it is not necessary to complete this Screening Template, you can proceed to complete the full [EqIA](#).

If no negative impacts are identified following completion of the EqIA screening then it is not necessary to undertake a full EqIA however, the decision and justification must be clearly recorded in this document.

On completion of the Screening Template:

- Ensure that all the white boxes within the screening are completed.
- Ensure that the Procedure/ Project/ Proposal/ Policy owner has signed and dated the Screening Template.
- Send a copy of the completed template along with the related policy or project proposal to Inclusion.hdd@wales.nhs.uk for the Diversity & Inclusion Team to review.
- Each Screening Template will be reviewed by the Diversity & Inclusion Team and feedback will be provided to the Procedure/ Project/ Proposal/ Policy owner. This may include recommendations for further action to inform robust decision-making.

Support

For further support please visit the [EqIA Sharepoint](#) or contact:

Email: Inclusion.hdd@wales.nhs.uk

Tel: 01554 899055

Director and Directorate	Director of Finance, Finance
Service Area	Information Governance

Title of Procedure, Project, Proposal, Policy being screened:	Corporate Records Management Policy & Strategy
--	--

Description of the Procedure/ Project/ Proposal/ Policy being screened (including key aims and objectives)

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 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.

Evidence considered (including staff and population data, relevant research, expert and community knowledge 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.

Assess which protected characteristics will potentially be affected by the proposal in the table below (please ✓ the relevant box to confirm positive, negative or no impact).

If at any point a negative impact has been identified (actual or potential), you do not need to proceed with the completion of this form, as a full EqlA must be undertaken: [Equality Impact Assessments \(EqlAs\) \(sharepoint.com\)](https://sharepoint.com)

Age				
Is it likely to affect older and younger people in different ways or affect one age group and not another?				
Positive Impact	<input type="checkbox"/>	Negative Impact	<input type="checkbox"/>	No Impact
				x
Justification of impact identified: This is an admin policy and strategy which do not negatively impact patients or staff. The policy is already in place and has had no complaints from protected groups. This policy has the same impact on a person regardless of their age, therefore no impact identified.				
Disability				
Is it likely to affect those with a physical disability, learning disability, sensory loss or impairment, mental health conditions, long-term medical conditions such as diabetes?				
Positive Impact	<input type="checkbox"/>	Negative Impact	<input type="checkbox"/>	No Impact
				x
Justification of impact identified: This is an admin policy and strategy which do not negatively impact patients or staff. The policy is already in place and has had no complaints from protected groups. This policy has the same impact on a person regardless of their disability, therefore no impact identified.				
Gender Reassignment				
Is it likely to affect those who either:				
<ul style="list-style-type: none"> • Have undergone, intend to undergo or are currently undergoing gender reassignment. • Do not intend to undergo medical treatment but wish to live in a different gender from their gender at birth 				
Positive Impact	<input type="checkbox"/>	Negative Impact	<input type="checkbox"/>	No Impact
				x
Justification of impact identified: This is an admin policy and strategy which do not negatively impact patients or staff. The policy is already in place and has had no complaints from protected groups. This policy has the same impact on a person regardless of their gender, therefore no impact identified.				
Marriage / Civil Partnership				
Under the Equality Act, the characteristic of Marriage and Civil Partnerships is only protected in the workplace/ employment.				
Is it likely to affect those who are married or in a Civil Partnership? This means someone who is legally married or in a civil partnership.				
Positive Impact	<input type="checkbox"/>	Negative Impact	<input type="checkbox"/>	No Impact
				x
Justification of impact identified: This is an admin policy and strategy which do not negatively impact patients or staff. The policy is already in place and has had no complaints from protected groups. This policy has the same impact on a person regardless of their marital status, therefore no impact identified.				
Pregnancy and Maternity				
Is it likely to affect those who are pregnant or have recently had a baby? Maternity covers the period of 26 weeks after having a baby, whether or not they are on Maternity Leave.				
Positive Impact	<input type="checkbox"/>	Negative Impact	<input type="checkbox"/>	No Impact
				x
Justification of impact identified: This is an admin policy and strategy which do not negatively impact patients or staff. The policy is already in place and has had no complaints from protected groups. This policy has the same impact on a person regardless of their health, therefore no impact identified.				
Race / Ethnicity				
Is it likely to affect people of a different race, nationality, colour, culture or ethnic origin including non-English / Welsh speakers, Gypsies/Travellers, asylum seekers and migrant workers?				

Positive Impact	<input type="checkbox"/>	Negative Impact	<input type="checkbox"/>	No Impact	x
Justification of impact identified: This is an admin policy and strategy which do not negatively impact patients or staff. The policy is already in place and has had no complaints from protected groups. This policy has the same impact on a person regardless of their race, therefore no impact identified.					
Religion or Belief Is it likely to affect people who have a religion or belief? The term 'religion' includes a religious or philosophical belief.					
Positive Impact	<input type="checkbox"/>	Negative Impact	<input type="checkbox"/>	No Impact	x
Justification of impact identified: This is an admin policy and strategy which do not negatively impact patients or staff. The policy is already in place and has had no complaints from protected groups. This policy has the same impact on a person regardless of their religion, therefore no impact identified.					
Sex Is it likely to affect people who are mostly male or female. Where it applies to both equally does it affect one differently to the other?					
Positive Impact	<input type="checkbox"/>	Negative Impact	<input type="checkbox"/>	No Impact	x
Justification of impact identified: This is an admin policy and strategy which do not negatively impact patients or staff. The policy is already in place and has had no complaints from protected groups. This policy has the same impact on a person regardless of their sex, therefore no impact identified.					
Sexual Orientation Whether a person's sexual attraction is towards their own sex, the opposite sex or either.					
Positive Impact	<input type="checkbox"/>	Negative Impact	<input type="checkbox"/>	No Impact	x
Justification of impact identified: This is an admin policy and strategy which do not negatively impact patients or staff. The policy is already in place and has had no complaints from protected groups. This policy has the same impact on a person regardless of their sexual choices, therefore no impact identified.					
Armed Forces Community Consider whether this impacts on members of the Armed Forces and their families, whose health needs may be impacted long after they have left the Armed Forces and returned to civilian life. Also consider their unique experiences when accessing and using day-to-day public and private services compared to the general population. It could be through 'unfamiliarity with civilian life, or frequent moves around the country and the subsequent difficulties in maintaining support networks, for example, members of the Armed Forces can find accessing such goods and services challenging.' For a comprehensive guide to the Armed Forces Covenant Duty and supporting resource please see: Armed-Forces-Covenant-duty-statutory-guidance					
Positive Impact	<input type="checkbox"/>	Negative Impact	<input type="checkbox"/>	No Impact	x
Justification of impact identified: This is an admin policy and strategy which do not negatively impact patients or staff. The policy is already in place and has had no complaints from protected groups. This policy has the same impact on a person regardless of their previous job roles, therefore no impact identified.					
Socio Economic Duty Consider those on low income, economically inactive, unemployed or unable to work due to ill-health. Also consider people living in areas known to exhibit poor economic and/or					

health indicators and individuals who are unable to access services and facilities. Food / fuel poverty and personal or household debt should also be considered.

For a comprehensive guide to the Socio-Economic Duty in Wales and supporting resources please see:

[more-equal-wales-socio-economic-duty](#)

Positive Impact	<input type="checkbox"/>	Negative Impact	<input type="checkbox"/>	No Impact	<input checked="" type="checkbox"/>
-----------------	--------------------------	-----------------	--------------------------	-----------	-------------------------------------

Justification of impact identified:

This is an admin policy and strategy which do not negatively impact patients or staff. The policy is already in place and has had no complaints from protected groups. This policy has the same impact on a person regardless of their income or where they live, therefore no impact identified.

Welsh Language

Is it likely to impact on opportunities for people to use the Welsh language? The Welsh language should be treated no less favourably than the English language.

Positive Impact	<input type="checkbox"/>	Negative Impact	<input type="checkbox"/>	No Impact	<input checked="" type="checkbox"/>
-----------------	--------------------------	-----------------	--------------------------	-----------	-------------------------------------

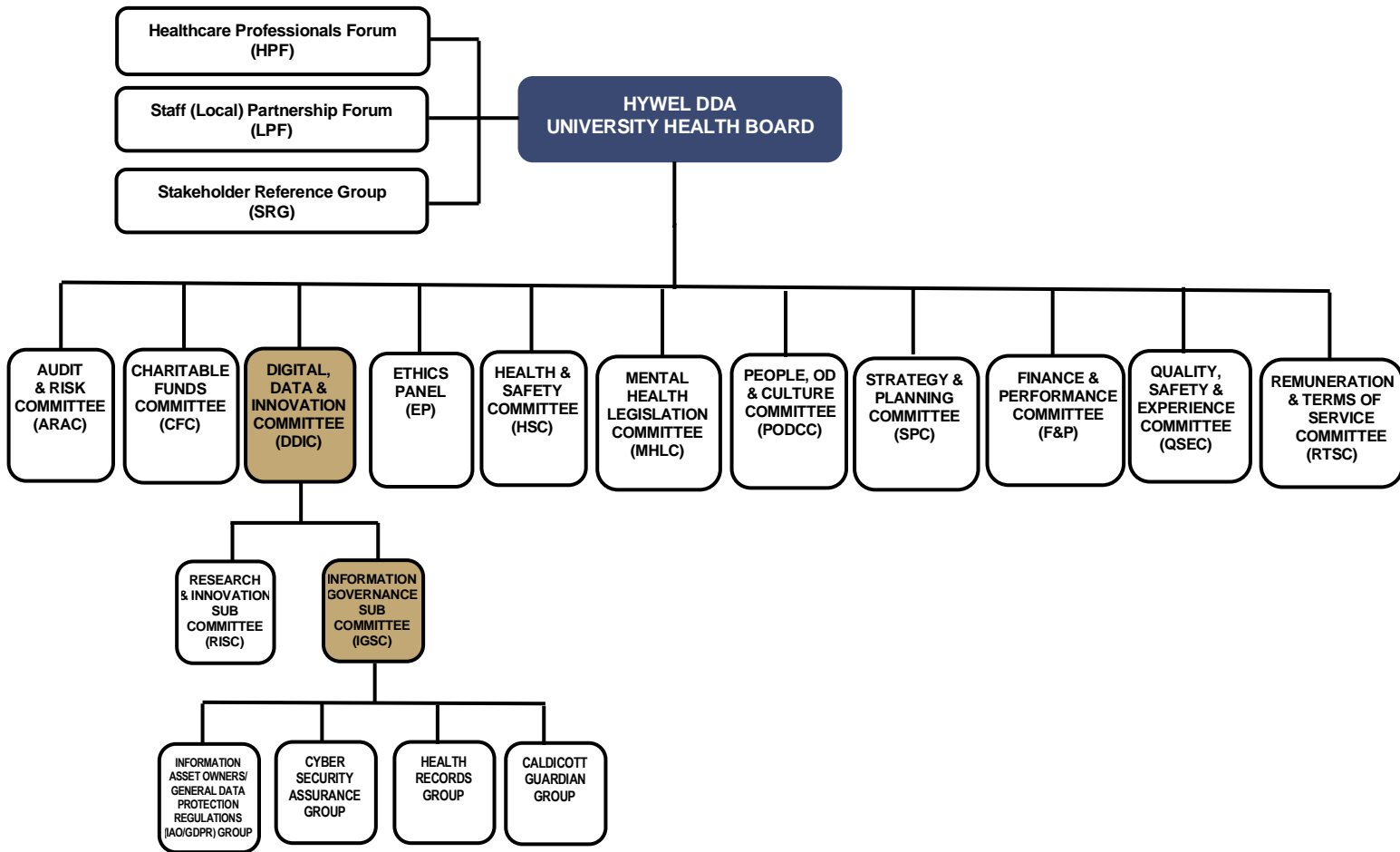
Justification of impact identified:

This is an admin policy and strategy which do not negatively impact patients or staff. The policy is already in place and has had no complaints from protected groups. Justification of impact identified: This policy has the same impact on a person regardless of their language, therefore no impact identified.

If a negative impact has been identified, you are not required to complete this form as a full EqlA must be undertaken. A full EqlA template and guidance can be found on the following link: [Equality Impact Assessments \(EqlAs\) \(sharepoint.com\)](#)

Screening Completed by:	Name	Siân Faiththorne
	Title	Senior Corporate Records Management Officer
	Contact details	Sian.Faiththorne@wales.nhs.uk
	Date	19 th February 2025
Screening Authorised by: (Directorate level owner of the procedures/ proposals/ projects/ policy)	Name	Patrycja Duszynska
	Title	Head of Information Governance
	Contact details	patrycja.duszynska@wales.nhs.uk
	Date	19 th February 2025
Guidance has been provided by Diversity & Inclusion Team:	Name	Kylie Daniels
	Title	Senior Diversity and Inclusion Officer
	Contact details	Kylie.daniels@wales.nhs.uk
	Date	19/02/2025
Diversity and Inclusion Team additional Comments:		

Please note: The D&I team will save a copy of the completed form for reference. If any changes are made after the date of review, it is the directorate’s responsibility to update the EqlA and inform the D&I team.



TERMS OF REFERENCE

INFORMATION GOVERNANCE SUB-COMMITTEE (IGSC)

Version	Issued to:	Date	Comments
V.1	Information Governance Sub Committee Integrated Governance Committee	25 th November 2010 21 st December 2011	Approved Approved
V.2	Information Governance Sub Committee Integrated Governance Committee	11 th November 2011 20 th December 2012	Approved Approved
V.3	Information Governance Sub Committee Integrated Governance Committee	14 th March 2013 23 rd April 2013	Approved Approved
V.4	Information Governance Sub Committee Integrated Governance Committee	14 th March 2014 22 nd April 2014	Approved Approved
V.5	Information Governance Sub Committee Integrated Governance Committee	13 th March 2015 28 th April 2015	Approved Approved
V.6	Information Governance Sub Committee	19 th June 2015	Approved
V.7	Information Governance Sub Committee	27 th July 2015	Approved
V.8	Business Planning & Performance Assurance	25 th August 2015	Approved

	Committee		
V.9	Information Governance Sub-Committee	27 th November 2015	Approved
V.10	Business Planning & Performance Assurance Committee	22 nd August 2017	Approved
V.11	Information Governance Sub-Committee	30 th July 2018	Approved
V.12	Information Governance Sub-Committee	11 th December 2019	Approved
V.12	Business Planning & Performance Assurance Committee	17 th December 2019	Approved
V.13	Information Governance Sub-Committee	2 nd September 2020	Approved
V.14	People Planning & Performance Assurance Committee	Via Chair's Action	Approved
V.15	Information Governance Sub-Committee	12 th October 2021	Approved
V.15	Sustainable Resources Committee	28 th October 2021	Approved
V.16	Revised by Digital Director	17 th May 2022	Approved
V.16	Information Governance Sub-Committee	11 th October 2022	Approved
V.16	Sustainable Resources Committee	10 th November 2022	Approved
V.17	Revised by Digital Director	07 th February 2024	Approved
V.17	Information Governance Sub-Committee	07 th February 2024	Approved
V.17	Sustainable Resources Committee		
V.17	Information Governance Sub-Committee	26 March 2025	Approved
V.17	Digital, Data and Innovation Committee	22 April 2025	For Approval

INFORMATION GOVERNANCE SUB-COMMITTEE (IGSC)

1. Constitution

- 1.1 Information Governance Sub-Committee (IGSC) has been established as a Sub-Committee of the Digital, Data & Innovation Committee (DDIC), and was constituted from 25th November 2010.

2. Principal Duties

- 2.1 The purpose of the Information Governance Sub-Committee is to provide assurance to the Sustainable Resources Committee (SRC), which is a Committee of the Board, on compliance with information governance legislation, guidance, and best practice, and to:
- 2.2 The Sub-Committee will:
- 2.2.1 Provide evidence based and timely advice to assist the University Health Board (UHB) in discharging its functions and meeting its responsibilities with regard to the quality and integrity; safety and security; and appropriate access and use of information (including patient and personal information) to support its provision of high-quality healthcare.
 - 2.2.2 Provide assurance in relation to the Board's arrangements for creating, collecting, storing, safeguarding, disseminating, sharing, using and disposing of information in accordance with its stated objectives; legislative responsibilities, e.g., the Data Protection Act 2018, UK General Data Protection Regulations 2016 (implemented May 2018), Freedom of Information Act 2000 and Network and Information Systems Regulation 2018; and any relevant requirements, standards and codes of practice.
 - 2.2.3 Provide assurance that risks relating to information governance are being effectively managed across the whole of the UHB's activities (including for hosted and contracted services, through shared services, partnerships, independent contractors, and Joint Committees as appropriate).

3. Operational Responsibilities

- 3.1 The Sub-Committee will, in respect of its provision of assurance/advice to the Digital, Data and Innovation (DDIC) Committee, ensure that:
- 3.1.1 Promote and develop a robust information governance and security framework within the UHB and encourage a strong information governance and security culture across the organisation.
 - 3.1.2 Ensure that good information governance practice is integrated into service and project delivery plans and pathways across the UHB.
 - 3.1.3 Ensure openness, security, quality, and legal compliance in all information produced, utilised and reported by the UHB and its partners.

- 3.1.4 In conjunction with key Committees / sub-committees / groups develop appropriate systems, policies, work plans, procedures and accountability based on innovation and best practice for the effective management of information, including (but not restricted to) the areas of:
- Information and Cyber Security (Inc. SIRO related issues)
 - Information Sharing Protocols
 - Contracts, partnership and third party and supplier agreements
 - Confidentiality and Data Protection
 - Freedom of Information
 - Subject Access Requests
 - Records Management
 - Information Quality Assurance / Data Quality
 - Risk Management and Incident Management
 - Data Protection Impact Assessments
 - Patient records
 - Clinical Coding
- 3.1.5 The Sub-Committee is responsible for recommending policies and procedures relating to information governance to the Digital, Data and Innovation Committee, for approval.
- 3.1.6 Monitor the UHB's compliance against relevant statutory requirements, internal and external standards and assessment criteria, via the Information Governance Toolkit, Cyber Assessment Framework (CAF) any other relevant requirements / assessments, and Internal / External Audit reviews including the implementation of Welsh Audit Office, Health Inspectorate Wales and Internal Audit recommendations.
- 3.1.7 Provide appropriate information governance assurance in relation to any high-level projects and plans that are monitored through and reported to the Digital, Data and Innovation Committee including the UHB's performance management framework and reporting template.
- 3.1.8 Develop, and performance manage action plans to achieve information governance and security objectives and direct and co-ordinate the work of the individuals and Groups involved with aspects of information governance within the UHB. Ensure that action plans and work programmes align with the UHB's Integrated Medium Term Plans (IMTP) where appropriate.
- 3.1.9 Inform and report the UHB's performance, action plans, and identified risks connected to information governance and information security to the Digital, Data and Innovation Committee (DDIC).
- 3.1.10 Provide assurance to the Digital, Data and Innovation Committee in relation to the organisation's arrangements for managing information and cyber security incidents including emergency preparedness, resilience and response and business continuity.

- 3.1.11 Provide a forum for discussion and debate on any ad-hoc information governance issues. This will include receiving and enacting information governance issues arising from the implementation of national systems directed for use within the UHB.
- 3.1.12 Develop an annual work plan and report, for sign off by the Digital, Data and Innovation Committee that addresses identified risks and priorities, meets relevant statutory and good practice requirement and is consistent with the strategic direction and organisational objectives of the organisation, including the IMTP where appropriate.
- 3.1.13 Provide assurance to the Digital, Data and Innovation Committee that, wherever possible, work plans are aligned with partnership plans and developed with Local Authorities, Universities, Collaboratives, Alliances, and other key partners.
- 3.1.14 Take forward any work identified by the Digital, Data and Innovation Committee as required to feed into the UHB's planning cycle.
- 3.1.15 Agree issues to be escalated to the Digital, Data and Innovation Committee with recommendations for action.
- 3.1.16 Consider the information governance implications for the Health Board of review reports and actions arising from the work of external reviewers.
- 3.1.17 Ensure that there is a process of Data Protection Impact Assessment in accordance with Information Commissioner's guidance.
- 3.1.18 The Health Board is meeting its legislative responsibilities, e.g., Data Protection and Freedom of Information Legislation, as well as complying with national Information Governance policies and Information Commissioners Office guidance.

Cyber Security

- 3.1.19 The promotion of information security throughout the Health Board.
- 3.1.20 The review and recommendation for the approval of all information security related policies and procedures.
- 3.1.21 The monitoring of progress in programmes to achieve compliance / certification with ISO27001.
- 3.1.22 The monitoring of progress in programmes to achieve compliance / certification with Cyber Essentials Plus.
- 3.1.23 The review and monitoring of security incidents both locally and nationally, identifying their root cause, any resolution and future prevention.
- 3.1.24 Reviewing information security risk assessments and improvement plans.

- 3.1.25 Consideration of solutions to improve security.
- 3.1.26 Monitoring and auditing compliance with standards and policies.
- 3.1.27 Receiving and reviewing information security related reports (e.g. internal audit).
- 3.1.28 Reviewing and commenting upon the security impact of information system development.
- 3.1.29 Reviewing, and recommending for approval, the information security elements of the annual IG toolkit submission.

4. Membership

4.1 The membership of the Sub-Committee shall comprise:

Title
Digital Director (Deputy SIRO) (Chair)
Medical Director (Caldicott Guardian)
Associate Medical Director for Professional Standard /Deputy Caldicott Guardian (Vice Chair)
Independent Member
Head of Information Governance
Head of Information Services
Health Records Manager
Information Governance Manager(s)
Assistant Director of Workforce and OD
Head of Digital Operations
Cyber Security Manager
Mental Health Representative
Nursing Representative
Therapies & Health Sciences Representative
County/Community Representative
Primary Care Representative
Risk and Assurance Representative
Legal Services Representative
Freedom of Information Service Representative
Estates and Facilities Representative
Clinical Engineering Representative
Corporate Archivist
In Attendance
Information Governance Officer(s)
Information Asset Owners

4.2 The membership of the Sub-Committee will be reviewed on an annual basis.

5. Quorum and Attendance

- 5.1 A quorum shall consist of no less than 6 and must include as a minimum either the Chair (Digital Director) or the Vice Chair (Associate Medical Director for Professional Standard), either the Caldicott Guardian (Medical Director) or the Deputy Caldicott Guardian (Associate Medical Director for Professional Standard) and the Independent Member for scrutiny
- 5.2 An Independent Member shall attend the meeting in a scrutiny capacity.
- 5.3 Additional members may be co-opted to contribute to specialised areas of discussion.
- 5.4 Any senior officer of the University Health Board, or from a partner organisation may, where appropriate, be invited to attend.
- 5.5 Should any member be unavailable to attend, they may nominate a deputy to attend in their place, subject to the agreement of the Chair.
- 5.6 The Head of Internal Audit shall have unrestricted and confidential access to the Chair of the Information Governance Sub-Committee.
- 5.7 The Sub-Committee may ask any or all of those who normally attend but who are not members to withdraw to facilitate open and frank discussion of particular matters.

6. Agenda and Papers

- 6.1 The Sub-Committee Secretary is to hold an agenda setting meeting with the Chair and/or Vice Chair and the Lead Executive Director (Digital Director, at least **six** weeks before the meeting date
- 6.2 The agenda will be based around the Sub-Committee work plan, identified risks matters arising from previous meetings, issues emerging throughout the year and requests from Sub-Committee Members. Following approval, the agenda and timetable for papers will be circulated to all Sub-Committee Members.
- 6.3 All papers should have relevant sign off before being submitted to the Sub-Committee Secretary.
- 6.4 The agenda and papers for meetings will be distributed seven calendar days in advance of the meeting.
- 6.5 The draft minutes and table of actions will be circulated to Members within fourteen/seven calendar days to check the accuracy.
- 6.6 Members must forward amendments to the Sub-Committee Secretary within the next seven calendar days. The Sub-Committee Secretary will then forward the final version to the Sub-Committee Chair for approval.

6 Frequency of Meetings

- 7.1 The Sub-Committee will meet bi-monthly and shall agree an annual schedule of meetings. Additional meetings will be arranged as determined by the Chair of the Sub-Committee in discussion with the Sub-Committee Lead.
- 7.2 The Chair of the Sub-Committee, in discussion with the Sub-Committee Secretary, shall determine the time and the place of meetings of the Sub-Committee and procedures of such meetings.

8. Accountability, Responsibility and Authority

- 8.1 The Sub-Committee will be accountable to the Digital, Data and Innovation Committee for its performance in exercising the functions set out in these terms of reference.
- 8.2 The Sub-Committee shall embed the University Health Board's vision, corporate standards, priorities and requirements, e.g. equality and human rights, through the conduct of its business.
- 8.3 The requirements for the conduct of business as set out in the University Health Board's Standing Orders are equally applicable to the operation of the Sub-Committee.

9. Reporting

- 9.1 The Sub-Committee, through its Chair and Members, shall work closely with the Board's other committees, including joint /sub committees and groups to provide advice and assurance to the Board through the:
 - 9.1.1 Joint planning and co-ordination of Board and Committee business;
 - 9.1.2 Sharing of information.
- 9.2 In doing so, the Sub-Committee shall contribute to the integration of good governance across the organisation, ensuring that all sources of assurance are incorporated into the Board's overall risk and assurance framework.
- 9.3 The Sub-Committee, may, subject to the approval of the Digital, Data and Innovation Committee, establish groups or task and finish groups to carry out on its behalf specific aspects of Sub-Committee business. The Sub-Committee will receive updates following each meeting, detailing the business undertaken on its behalf. Groups reporting to this Sub-Committee are:
 - 9.3.1 Information Asset Owners/General Data Protection Regulations (IAO/GDPR) Group
 - 9.3.2 Cyber Security Assurance Group
 - 9.3.3 Health Records Group
 - 9.3.4 Caldicott Guardian Group
- 9.4 The Sub-Committee Chair, supported by the Sub-Committee Secretary, shall:
 - 9.4.1 Report formally, regularly and on a timely basis to the Digital, Data and Innovation Committee on the Sub-Committee's activities. This includes

written updates on activity, as well as the presentation of an Annual Report within 6 weeks of the financial year.

- 9.4.2 Bring to the Digital, Data and Innovation Committee's specific attention any significant matter under consideration by the Sub-Committee.

10. Secretarial Support

- 10.1 The Sub-Committee Secretary shall be determined by the Sub-Committee Lead.

11. Review Date

- 11.1 These terms of reference shall be reviewed on at least an annual basis by the Sub-Committee for approval by the Digital, Data and Innovation Committee.

Requirement	Ref No	Toolkit Req. No	CPIP/Standards/Audit	Objective / Recommendation	IG Toolkit Improvement Plan Recommendation	Management Action	Lead Officer	Target Date and RAG Rating	2025 - 2026				
									Progress / Comments				
									Q1 April - June	Q2 July - September	Q3 October - December	Q4 January - March	
	1	ACCOUNTABILITY		ACCOUNTABILITY									
NHS Wales Requirement (IG Toolkit) (HDUHB Requirement)	1.1	tbc	G4	IGSC Annual Report		Develop and publish the Information Governance Annual Report which should be approved by IGSC, and SRC	Lead HoIG - Support IG Team / Medical Records / Information Services / FOI Team / Cyber Security Team						
NHS Wales Requirement	1.2			Welsh IG Toolkit - 2025 - 2026		Implement the All Wales IG Toolkit in replacement of Caldicott Outturn report.	HoIG / IGMs Lead: HoIG, IGMs / Medical Records / Cyber Security Team / FOI Team / Health, Safety & Security Team / Information Services						Submission in Q4
NHS Wales Requirement	1.3			Welsh IG Toolkit - Improvement Plan for 2025 - 2026	Yes	Coordinating the IG Toolkit Improvement Plan and presenting it to IGSC on a regular basis	HoIG / IGMs						as above
NHS Wales Requirement	1.6			IG Toolkit for Managed GPs		*Implement the All Wales IG Toolkit *Creating Teams Site with IG Resources for Managed Practices *Provide bespoke training *Attend quarterly all Managed practice forum meetings [Nia check] *Meeting with practice managers (face to face)	HoIG / IGMs						Submission in Q4
NHS Wales Requirement	1.7			Managed GPs - Improvement Plan		Coordinating the IG Toolkit Improvement Plan for Managed Practices and presenting it to IGSC on a regular basis	IGMs						As above
NHS Wales Requirement	1.8		GDPR	IG Policies and Procedures	Yes IG Policies and procedures to be included in the quarterly IG Activity Report to IGSC, where review dates are closely monitored.	Review and update annual cycle of policies and procedures to ensure compliance with legislation.	HoIG / IGMs / ISM	In Progress		to be included in Q2 report			
NHS Wales Requirement	1.9		G9	Third Party Monitoring		Continue to monitor all partners and 3rd sector organisations who have access to Health Board information assets	IGMs Support - IG Officers	Ongoing	Ongoing monitoring of Third Party suppliers through IARs work, DPIAs, Third Party Suppliers questionnaires, etc.	Ongoing monitoring of Third Party suppliers through IARs work, DPIAs, Third Party Suppliers questionnaires, etc.	Ongoing monitoring of Third Party suppliers through IARs work, DPIAs, Third Party Suppliers questionnaires, etc.	Ongoing monitoring of Third Party suppliers through IARs work, DPIAs, Third Party Suppliers questionnaires, etc.	
NHS Wales Requirement	1.10		G9	Employees Contracts (volunteers / trainees / work placements / apprenticeship / bank staff / agency / locum etc)		Continue to implement confidentiality clauses for any new contracts that involve contact; access or sharing of confidential information	IGMs Support - IG Officers	Ongoing					

To Be Accelerated (IG Team could be more effective with completed training package)	2.2			Review and update IG Training Package	Yes	* Training Material to be updated, include Corporate Records Management in the sessions * IG Training Sessions to be recorded (Virtual Learning Video) * IG Training Sessions Prospectus to be updated on the Workforce Site (IG Training Level 1; IG Training Level 2 (Information Asset Owners and Information Asset Administrators) * Produce Training/awareness/IG Communication material for staff not having access to digital platforms.	HoIG / IGMs / IGOs					
To Be Accelerated (IG Team could be more effective with completed training package)	2.3			Development of IG Training Platform		Development of short IG Movies on specific topic (e.g. National IG Policies) and to be placed on the SharePoint Site	IGMs					
ICO Requirement	2.4			Provision of tailored IG Training to different Services		Training Sessions delivered: * Information Asset Owners Training * Subject Access Requests Training to Access to Health Records Team and Complaints Service. * IG Training for Medical Secretaries	IGMs		Junior Doctors	Junior Doctors/ Consultants	Medical Secretaries Pembrokeshire Collage Students	Social Workers (WNCR) - New Starters and Refresher Complaints Team Managed Practices Pharmacies (BGH)
HUHB Requirement	2.5			Development of the IG Training Plan	Yes	The plan to be developed and reviewed annually *IG Training needs analysis (Questionnaire)	HoIG / IGMs				Training Plan reviewed	Training Plan approved
To Be Accelerated (IG Team could be more effective with completed intranet site, where guidance to staff is available)	2.6			Review and Update of IG Intranet Site for staff	Yes	* IG Intranet Site on HDUHB SharePoint, needs to be regularly checked and content reviewed * Links to IG Policies * Link to IG Training	IGMs / IGOs					review of content
To Be Accelerated (IG Team could be more effective with completed internet site, where guidance to patients is available)	2.7			Review and Update of IG Internet Site for patients and visitors		* IG External Website needs to be reviewed and updated if needed	IGMs / IGOs					
To Be Accelerated	2.8			Develop IG Communication Plan to ensure coordinated and consistent approach to dissemination of Information	Yes	Plan to include: * IG Newsletter * IG Guidance to be circulated through Global Email and HB's Bulletins * Planning Campaigns on National Data Protection/Privacy Day; Cyber Security Awareness Day, etc.	HoIG / IGMs		Linked with IG Training Plan	Linked with IG Training Plan	Linked with IG Training Plan	Linked with IG Training Plan

Statutory Requirement	2.9		IP2 GDPR	Privacy Notices		Review, update and make publicly available all fair processing information to ensure staff and patients are effectively informed with regards to the sharing of their data (full Review Yearly)	IGMs					
Statutory Requirement	2.10			Information Asset Registers - Platform for managing Registers		The identification of processing activities, recording them via the integrated asset register and data flow mapping tool on Teams that has been developed by IG Team remains an ongoing project. The Health Board should ensure that the IG Teams site is kept up to date.	IGMs					
Statutory Requirement	2.11			Information Asset Registers - Build with Services		Complete the project of creating IARs for all Services across HDUHB	IGMs	In Progress				
Statutory Requirement	2.12		IM1 & ICO A15	Information Asset Registers - Review	Yes	Continue to capture information flows and ensure that asset owners are adequately equipped to manage and review these flows (IARs need to be reviewed on a regular basis and IAOs and IAAs need to receive refresher training)	IGMs	Ongoing	Review plan submitted to IAOG/IGSC meeting	Review plan submitted to IAOG/IGSC meeting	Review plan submitted to IAOG/IGSC meeting	Review plan submitted to IAOG/IGSC meeting
Statutory Requirement	2.13			Information Asset Registers - Identify Data Flows from EEA		International Data Flows are being picked up through work with Information Asset Administrators.	IGMs	Ongoing				
HDUHB Requirement	2.14			Quarterly IG Activity reports		Quarterly Reports to be presented to IGSC	HoIG / IGO		Report Provided to IGSC	Report Provided to IGSC	Report Provided to IGSC	Report Provided to IGSC
ICO Requirement	2.15			Complying with ICO recommendations		Any actions arising from ICO recommendations or decision notices need to be reported to IGSC In-Committee Meetings.	IGMs		Report Provided to IGSC In Committee	Report Provided to IGSC In Committee	Report Provided to IGSC In Committee	Report Provided to IGSC In Committee
NHS Wales Requirement	2.16			Compliance with WASPI Framework		* Ensure relevant ISPs/DDAs are in place * Creation of Local Register	IGMs		ISPs Lead by HDUHB reviewed and up to date	ISPs Lead by HDUHB reviewed and up to date	ISPs Lead by HDUHB reviewed and up to date	ISPs Lead by HDUHB reviewed and up to date
NHS Wales Requirement	2.17			Maintenance of Caldicott Guardian Register		maintaining the register in line with internal guidance	IGMs		Report Provided to IGSC	Report Provided to IGSC	Report Provided to IGSC	Report Provided to IGSC
Statutory Requirement	2.18			IG Complaints and Investigation Process		* Develop process for dealing with IG complaints/investigations * Adding themes around staff's confidentiality through "Working in Confidence" Platform. IG Responder to be delegated. (these will be complaints raised anonymously in the beginning)	HoIG / IGMs	Closed				
Statutory Requirement	2.19			Personal Data Breaches	Yes	* Procedure to be reviewed * Adopting DATIX for management of Personal Data Breaches	HoIG / IGMs	In Progress				
Statutory Requirement	2.20			GDPR Compliance		* Ensure completion of project plan for implementation	HoIG / IGMs		Report Provided to IGSC	Report Provided to IGSC	Report Provided to IGSC	Report Provided to IGSC
Statutory Requirement	2.21			Development of IG Template Forms		* Individuals Right Request Form * Third Party Request Form * Subject Access Request Form Developing digital Forms.	HoIG / IGMs	Ongoing				
Statutory Requirement	2.22			Development of IG Template Agreements		* Data Processing Agreement (DPA) * Joint Data Controller Agreement (JDCA)	HoIG / IGMs	Closed				Review in 2026 - 2027

Statutory Requirement	2.23			Redaction of Health Records (including Mental Health)		*Assisting and providing advice to Access to Health records Team * Providing Guidance and Training	HoIG / IGMs	Ongoing				
NHS Wales Requirement	2.24			Adoption of the WASPI Information Sharing Gateway			HoIG / IGMs	Not Started	The system is being rolled out by DHCW, HDUHB awaiting local implementation.			
NHS Wales Requirement	2.25			Adoption of Information Sharing Code of Practice			HoIG / IGMs	Not Started	Awaiting the ICO directions			
3 INFORMATION SECURITY ASSURANCE												
HDUHB Requirement	3.1		GDPR M5 M7	Information Asset Owners - Systems	Yes	Ensure all entries on the Information Asset Registers have system owners and administrators who are regularly reviewing and updating their register entries.	IGM, ISM	Ongoing				
Statutory Requirement	3.2			Information Governance Audits	Yes inc. Cyber Security	Conduct site compliance audits to ensure Data Protection and UK GDPR compliance across the HB.	IGMs / IGOs					
NHS Wales Requirement	3.3			Management of Mail Marshal (Archived) Management of Data Loss Prevention Tool		* Release of email containing PII, which are being blocked by the system * Staff's Communications * Review & Monitor emails being sent to personal email addresses	ISM / IGMs / IGOs	Ongoing				
NHS Wales Requirement	3.4			Management of Secure File Share Portal Facility		* Promoting Secure Sending of PII * Policy Review	ISM / IGMs	Ongoing				
4 CLINICAL INFORMATION ASSURANCE												
Statutory Requirement	4.1			Individual Rights - enquiries from Patients and staff		Update procedures for Subject Access Requests and Access to health records requests to ensure compliance with the new right rights of a data subjects with regards to the right to restrict processing; rights of data portability; enhances right of erasure; rights to restrictions in processing for profiling	HoIG / IGMs / Health Records Manager	In Progress				
HDUHB Requirement	4.2			Review Storage for Health Records		Offsite Storage Providers and HDUHB's Premises are being reviewed	IGMs	In Progress	Ceredigion Site (outstanding)			
HDUHB Requirement	4.3			Multi Agency Access to Patients Records on WPAS, CarePartner, WCCIS and WNCR		Develop documented procedures and processes to ensure a multi-disciplinary approach to the regular auditing of clinical records (Link to	HoIG / IGMs	Ongoing				
Statutory Requirement	4.4			Monitoring Unauthorised Access to Patients Records		Continue with regular confidentiality audits (inc. NIIAS, WCP Break Glass) ensuring comprehensive audit trails are maintained and breaches are reported and dealt with appropriately	IGMs / IGOs		Report Provided to IGSC	Report Provided to IGSC	Report Provided to IGSC	Report Provided to IGSC
5 CORPORATE INFORMATION ASSURANCE												
HDUHB Requirement	5.1			Review & develop procedures, guidance and training packages to enable staff to work in a consistent way with regards to records management		* Roles of the IAO and IAA are captured and delivered as part of the IAO/IAA training package * Develop training and awareness package within IG training * Roll out a training schedule * Starters check list to be reviewed to include awareness around records management * Information Asset Register Procedure/Guidance/User Guides	HoIG / IGMs	Ongoing				Corporate Records Management Procedure Assured

HDUHB Requirement	5.2			Review storage arrangements for corporate archived information across the Health Board		<ul style="list-style-type: none"> * Identify current storage locations * Corporate Records Management Policy and Procedure to be developed and implemented * Conduct an audit of any records that are due to be transferred to PROs 	HoIG / IGMs		Report Provided to IGSC	Report Provided to IGSC	Report Provided to IGSC	Report Provided to IGSC
-------------------	-----	--	--	---	--	---	-------------	--	-------------------------	-------------------------	-------------------------	-------------------------