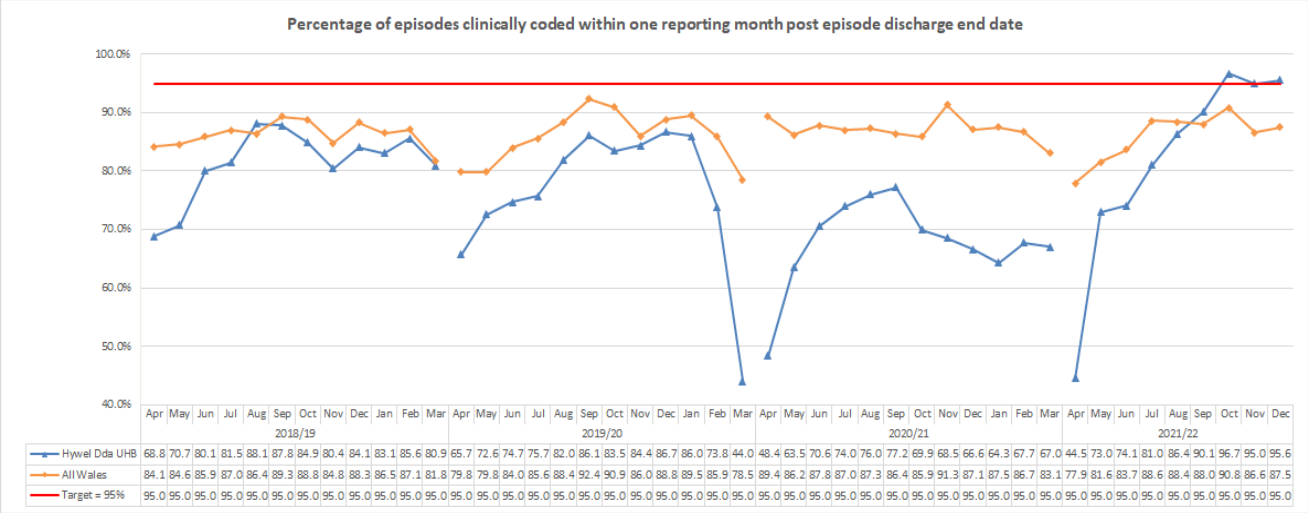
Enw y Grŵp/Is-Bwyllgor: Name of Group:	**Information Governance Sub-Committee (IGSC)**
Cadeirydd y Grŵp/Is-Bwyllgor: Chair of Group:	**Huw Thomas, Director of Finance**
Cyfnod Adrodd: Reporting Period:	**1st April 2022**

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

Clinical Coding Update

The Sub-Committee noted that Hywel Dda University Health Board (HDdUHB) clinical coding activity continued to improve for December 2021 and surpassed the 95% target with 95.6%. Over the past 4 months, the Health Board has been above the All-Wales average for the first time in a number of years and performance is continuing to improve. HDdUHB has ranked third of the 7 Welsh Health Boards for December 2021 performance, with only Powys Teaching Health Board and Velindre Trust also achieving the 95% target for December 2021 activity.

The Sub-Committee noted the current clinical coding performance being above the Welsh average and that the clinical coding team are ahead of the planned trajectory.



The Sub-Committee approved the approach for the Clinical Coding team to continue with current month on month processes to strive for 95% compliance for each calendar month and **not** to concentrate on backlog for 2021/22 during April and May of 2022/23, to enable the team to maintain momentum and progress to date.

Information Governance Documents

- **Corporate Records Management Policy:** The Sub-Committee noted the comments received and approved the Corporate Records Management Policy, attached at Appendix 1, for onward submission to the Sustainable Resources Committee for final approval.

Information Governance Toolkit

The Sub-Committee received an update on the submission of the Information Governance Toolkit. The submission was based upon the information received from specific departments of

the Health Board in the last quarter of 2021/22, including a snapshot of the department's documents and processes, the training undertaken by specific individuals, guidance for staff, documents used to inform patients/clients of the Health Board's processes, and patients/clients' rights in respect of the Health Board's processes. The Sub-Committee noted the updates and agreed that the final toolkit can be approved by Chair's Action prior to the final submission in April 2022.

Information Asset Registers
The Sub-Committee was requested to approve 5 Information Asset Registers (IARs), following assurance by the Information Asset Owners Group (IAOG) and the Services' Lead Directors:

- Estates
- Digital Services – Projects and Transformation
- Strategic Development
- Research and Development
- Tritech

Information Governance Workplan 2022/23
The Sub-Committee received the Information Governance Workplan for 2022/23. The Sub-Committee noted the workplan and requested that updates are presented on a quarterly basis.

HDdUHB's Privacy Notice – Review
The Sub-Committee received an update to the Privacy Notices to comply with the Data Protection Legislation.

Welsh Control Standard for Electronic Health and Care Records
The Sub-Committee received an update from Digital Health and Care Wales on the Welsh Control Standard for electronic health and care records. All Health Boards and NHS Trusts in Wales are required to sign up to the Welsh Control Standard to use national systems. Other organisations, such as primary care contractors who require access to national systems, must also sign up to the Welsh Control Standard.

Information Commissioner Office (ICO) Notifications
Since April 2021, there have been 13 occurrences when a notification to the ICO has been required. The following table highlights the current notifications:

	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Total
Open	1	0	0	1	1	1	1	1	1	0	0	0	7
Closed	2	0	2	1	0	0	0	0	0	1	0	0	6
Total	3	0	2	2	1	1	1	1	1	1	0	0	13

Information Governance Compliance Update
The Sub-Committee received an update on work undertaken by the Information Asset Owners and Information Governance team regarding General Data Protection Regulation (GDPR) compliance within the Health Board. The Sub-Committee was requested to approve the movement of the following 3 elements of the Information Asset Owners Action Plan from Amber to Green;

- Starters, Movers and Leavers Policy – in light of the work undertaken by the Digital Team to progress with the automation of the Starters, Movers and Leavers policy

- Information Governance Risks - Information Governance risks are identified as part of the mapping process and added to the risk tracker and IG Risk Register where appropriate., The Sub-Committee are informed by way of an Information Asset Register (IAR) Risk Report.
- Cyber Security - Progress is monitored by the Sub-Committee via a standard agenda item on Network and Information Systems Regulations (NIS-R).

Cyber Security and Network and Information Systems (NIS) Directive Update
A separate report has been prepared for presentation to the Sustainable Resources Committee to provide an update on progress of Cyber Security.

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

- Due to the inability of several health boards to submit the Information Governance Toolkit within the required deadline, the Sub-Committee agreed that sign-off of the Information Governance Toolkit via Chair's Action prior to the next Sub-Committee meeting.
- Approval of the Corporate Records Management Policy (attached at Appendix 1).

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

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

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

Adrodd yn y Dyfodol:
Future Reporting:

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

Dyddiad y Cyfarfod Nesaf:
Date of Next Meeting:

7th June 2022

Corporate Records Management Policy

FOR SRC APPROVAL

Policy Number:	347	Classification		Corporate
Supersedes	All former Corporate Records Management Policies and Corporate Records Management Strategy			
LOCSSIP reference:		NATSSIPS Standards	List standard (NATSSIPS Standards)	

Version No	Date of EqIA:	Approved by:	Date of Approval:	Date made Active:	Review Date:
V2		Sustainable Resource Committee			3 years

Brief 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:	193 – Retention and Destruction of Records Policy (Including Health Records) 224 – Information Classification Policy 191 – Health Records Management Strategy 192 – Health Records Management Policy 291 – Personnel Employee Record Management Policy 224 – Information Classification Policy 836 – All Wales Information Governance Policy 238 – Information Governance Framework

	172 – Confidentiality Policy 837 – All Wales Information Security Policy 186 – Business Continuity Planning Policy 173 – Freedom of Information Act Policy
Patient information:	N/A

Owning Committee	Information Governance Sub-Committee Director of Finance 01.04.2022

Executive Director:	Huw Thomas	Job Title	Director of Finance

Reviews and updates		
Version no:	Summary of Amendments:	Date Approved:
0.1	Submitted to Information Governance Sub-Committee for approval	14 June 2013
1.0	Submitted to Integrated Governance Committee for approval	25 June 2013
	Extension whilst review takes place to BP&PAC	23/8/2016 19/12/2017
2.0	Policy Reviewed	

Glossary of terms

Term	Definition
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 Health Board holds and how long they will be retained before disposal. It can also be used to set out what needs to happen to records at various different stages of their lifecycle to ensure that they are stored efficiently.
Critical Records	are records without which the Health Board could not effectively function or be reconstructed in the event of a disaster. These include records the Health Board 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.

Keywords	Records Management, Corporate Records

CONTENTS

1. 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.

2. 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.

3. 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.

4. Aim

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

5. Objectives

5.1 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.

5.2 The policy will ensure the following:

5.2.1 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.

5.2.2 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.

5.2.3 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

5.2.4 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.

5.2.5 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.

5.2.6 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.

5.2.7 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.

5.2.8 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.

6. Implementation of the policy

6.1 Record Creation

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

6.1.1 Ownership

All records created by employees of the Health Board in the course of their work remain the absolute property of HDUHB unless otherwise specifically agreed.

6.1.2 Evidential significance

Adequate records of all activities will be maintained to account fully and transparently for all actions and decisions of HDUHB.

6.1.3 Accuracy and authenticity

The Health Board shall ensure records are complete and accurate and that the information they contain is reliable and its authenticity can be guaranteed

6.1.4 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.

6.1.5 Legislative compliance

All the records created by the Health Board 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.

6.2 Records Retention and records disposal

HDUHB will store records to maximize 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 Health Board's retention schedule. 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.

6.2.1 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.

6.2.2 Arrangement of records

Information will be arranged 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.

6.2.3 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 Health Board will develop a corporate classification scheme for the storage of records, and to facilitate the application of access control and retention schedules.

6.2.4 Access Control

The security of the Health Board's records is essential. The security controls in place to safeguard the records of HDUHB are detailed in the All Wales Information Security Policy.

6.3 Records Storage

6.3.1 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 Health Board's approved storage providers, with access to the records provided on demand.

6.3.2 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.

6.3.3 Disposal and transfer

Services must have in place clearly defined and accountable arrangements for the appraisal and selection of records for disposal and transfer, and for documenting this work. Specific requirements for keeping and disposing of all records regardless

of medium are contained within the Health Board's Retention Schedule. All records should be managed in accordance with this schedule. 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. Mechanisms for the regular transfer of records selected for permanent preservation should be in place and agreed with Health Board's Corporate Archivist. 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.

7. Use of Records

7.1 Using physical records

Physical records are the responsibility of the user, who should have regard to 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.

7.2 Use of the Internal and Off-site Storage

All storage areas need to be assessed and IG Service should be contacted for advice.

7.3 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.

7.4 Critical Records

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

7.5 Business Continuity and Recovery

If records are damaged the service area must undertake a risk assessment to decide whether restoration would be beneficial. Advice should be sought from the IG Service or Business Continuity Service.

7.6 Risk Management

Records form part of the corporate assets of the Health Board, 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 Health Board's risk management framework and included on each service's risk register for local management and escalated through their management structure where appropriate.

7.7 Partnership Working

Information sharing protocols will be drawn up with partners to reflect agreement in data sharing. The Health Board 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.

7.7.1 Partnership working where HDUHB is the lead partner:
Core records will be retained and managed by HDUHB under retention schedules agreed by the Health Board. HDUHB's Corporate Records Management Policy will apply

7.7.2 Partnership working where another organisation is the lead partner:
Core records will be retained by the other organisation. The Health Board will identify and manage records relating to its role in the partnership under retention schedules agreed by the Health Board.

7.7.3 Partnership working where no single organisation is the lead partner:
The Health Board will ensure that an agreement is in place with one partner for the management of core records

8. Responsibilities

Chief Executive – The Chief Executive takes overall responsibility for the Health Board's information governance performance and is required to ensure that:

- the Health Board can demonstrate accountability against the requirements within the Data Protection Act;
- decision-making is in line with the Health Board's 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 Digital Director who will be accountable for the Health Board's 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 Digital Director 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 Health Board's culture. The SIRO is the Chair of the Information Governance Sub-Committee.

Caldicott Guardian - The Medical Director has been nominated as the Health Board's 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 Health Board adopts information governance best practice and

standards. This role will report to the Digital Director and will be supported by the Information Governance Team who will also work in collaboration with the Information Asset Owners.

Chief Information Officer - The Chief Information Officer 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 Health Board's 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 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.

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.

Corporate Archivist - The Corporate Archivist is responsible for the transfer of records to the Health Board's 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 Health Board 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 Health Boards confidential information assets is identified

9. Monitoring

Monitoring of this policy will be the joint responsibility of the Digital Director 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 Health Board's 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.

10. Resources

The Information Governance Team should have sufficient resource in order to ensure the Health Board remains complaint against its legislative requirements and timescales.

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

11. Training

11.1 All staff within HDUHB, are mandated to undertake Information Governance training. This training must be renewed every two years.

11.2 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.

11.3 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.

12. Audit

12.1 The Health Board 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.

12.2 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.

13. 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 (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