# Information Governance Framework

**Policy Number:** 238  
**Supersedes:** V 5.0  
**Classification:** Corporate

<table>
<thead>
<tr>
<th>Version No</th>
<th>Date of EqIA</th>
<th>Approved by</th>
<th>Date of Approval</th>
<th>Date made Active</th>
<th>Review Date</th>
</tr>
</thead>
</table>

**Brief Summary of Document:** The Information Governance Framework sets out the standards to be applied across the Health Board for managing information governance including the organisational arrangements, roles, responsibilities and policies.

**Scope:** This framework applies to all Health Board staff and the following groups of people who work for or on behalf of the Health Board: committee chairs and members and remunerated expert advisors, agency workers, locums and contractors, secondees, students, volunteers and placement staff.

**To be read in conjunction with:**  
172 - Confidentiality Policy  
225 - Data Protection Policy  
224 - Information Classification Policy  
275 - Secure Transfer of Personal Information Policy  
183 - Information Security Policy  
279 - Third Party Supplier Security Policy

**Owning Committee**  
Information Governance Sub-committee (IGSC)

**Executive Director:** Karen Miles  
**Job Title:** Director of Planning, Performance and Commissioning
## Reviews and updates

<table>
<thead>
<tr>
<th>Version no:</th>
<th>Summary of Amendments:</th>
<th>Date Approved:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>New Policy</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Minor Revision</td>
<td>Feb 2012</td>
</tr>
<tr>
<td>3</td>
<td>Framework Review</td>
<td>23.04.13</td>
</tr>
<tr>
<td>4</td>
<td>Framework Review</td>
<td>23.09.14</td>
</tr>
<tr>
<td>5</td>
<td>Framework Review</td>
<td>23.02.16</td>
</tr>
<tr>
<td>6</td>
<td>Full review including changes to the revised Data Protection Act /General Data Protection Regulations 2016 or any subsequent legislation to the same effect</td>
<td>26.6.2018</td>
</tr>
</tbody>
</table>

## Glossary of terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIRO</td>
<td>Senior Information Risk Owner</td>
</tr>
<tr>
<td>DPO</td>
<td>Data Protection Officer</td>
</tr>
<tr>
<td>DPIA</td>
<td>Data Protection Impact Assessments</td>
</tr>
<tr>
<td>NIIAS</td>
<td>National Integrated Intelligent Audit System</td>
</tr>
<tr>
<td>IGSC</td>
<td>Information Governance Sub Committee</td>
</tr>
<tr>
<td>IAO/GDPR</td>
<td>Information Asset Owners/General Data Protection Regulations</td>
</tr>
<tr>
<td>EPR</td>
<td>Electronic patient record</td>
</tr>
<tr>
<td>CP-P</td>
<td>Caldicott Principles into Practice</td>
</tr>
</tbody>
</table>

## Keywords

Information governance, data protection, SIRO, risk,
1. Introduction ......................................................................................................................... 4
2. Policy Statement .................................................................................................................. 4
3. Scope .................................................................................................................................. 4
4. Aim .................................................................................................................................... 4
5. Objectives ........................................................................................................................... 4
6. Roles and responsibilities ................................................................................................... 5
   6.1. Chief Executive ............................................................................................................. 5
   6.2. Senior Information Risk Owner (SIRO) ........................................................................ 5
   6.3. Deputy SIRO ............................................................................................................... 5
   6.4. Caldicott Guardian ...................................................................................................... 5
   6.5. Deputy Caldicott Guardian .......................................................................................... 5
   6.6. Data Protection Officer (DPO) ..................................................................................... 6
   6.7. Information Asset Owners .......................................................................................... 6
   6.8. Information Asset Administrators .............................................................................. 6
   6.9. The Information Governance Team ............................................................................. 6
   6.10. Access to Health Records Team .................................................................................. 7
   6.11. Corporate Office ...................................................................................................... 7
   6.12. Managers .................................................................................................................... 7
   6.13. Staff ............................................................................................................................. 7
7. Information asset and information risk management .......................................................... 8
8. Governance structure .......................................................................................................... 9
9. Information governance policies and procedures ............................................................... 11
10. Information governance training and awareness ............................................................. 12
11. Information governance incident management .............................................................. 13
11.1 Incident reporting process ............................................................................................. 14
11.2 Reporting structures ..................................................................................................... 14
12. Managing third party access to information .................................................................... 15
13. IT, cyber security and business continuity ...................................................................... 15
14. Monitoring and review ...................................................................................................... 15
15. Appendix 1 – Responsibility for the management of Information Assets within Hywel Dda University Health Board ................................................................................. 17
1. Introduction
The Information Governance Framework sets out the standards to be applied across the Health Board for managing information governance including the organisational arrangements, roles, responsibilities and policies.

Information governance covers the framework of law and best practice to ensure information is managed in a confidential, secure and consistent way. Particular focus is placed on the management of personal data and other confidential information to ensure it is handled legally, securely and efficiently to provide the best possible service to our patients.

2. Policy Statement
The Health Board is committed to managing its information securely, legally and effectively in order to provide the best possible services to our patients. This framework provides clear guidance to staff around how information should be managed and outlines the accountability structures, governance processes, documented policies and procedures, staff training and resources required to undertake this task.

Good information governance ensures that the Health Board is able to provide the right service, at the right time for the right people in an inclusive, open and accountable way that upholds the rights of individuals.

3. Scope
This framework applies to all Health Board staff and the following groups of people who work for or on behalf of the Health Board: committee chairs and members and remunerated expert advisors, agency workers, locums and contractors, secondees, students, volunteers and placement staff.

It applies to management and governance of all information across the Health Board with a particular emphasis on personal and confidential information. It applies to information held in both electronic and paper format and their associated systems.

4. Aim
The aim of the Information Governance Framework is to ensure that there is a clear structure in place for managing information governance across the Health Board and this is communicated to our staff and stakeholders. It will ensure that the Health Board is managing all information in an effective and efficient way and is meeting its legal and ethical requirements, including to safeguard the confidentiality and privacy of patients, staff and service users.

5. Objectives
- The Health Board is making the best use of the information it holds to provide the best possible service and care to patients.
- The Health Board is protecting personal information to ensure that the confidentiality and privacy rights of individuals are upheld.
- The Health Board is meeting its legal and statutory duties including in relation to the Data Protection Act /General Data Protection Regulations 2016 or any subsequent legislation to the same effect, the Freedom of Information Act, the Human Rights Act and in upholding the common law duty of confidentiality.
- There is a strong senior oversight of information governance within the Health Board with a clear reporting structure to the Board.

Please check that this is the most up to date version of this written control document
HYWEL DDA UNIVERSITY HEALTH BOARD

- All Health Board staff understand the required standards for managing information and are clear about their individual responsibilities in this area.
- There are adequate policies, procedures and processes in place to meet the aims of the Information Governance Framework and these are applies consistently across the organisation.
- There is a clear structure for managing information risk across the organisation.

6. Roles and responsibilities

6.1. Chief Executive
The Chief Executive has overall responsibility for information governance and provides assurance through the Annual Governance Statement that risks relating to information are effectively managed.

6.2. Senior Information Risk Owner (SIRO)
The Director of Planning, Performance and Commissioning is the Health Board’s SIRO and is the Executive representative to the board for Information Governance.

The SIRO:
- Leads and fosters a culture of good information governance across the Health Board.
- Ensures information governance compliance with legislation and Health Board policies.
- Has overall responsibility for managing information risk including information and cyber security.
- Chairs the Information Governance Sub-committee.

6.3. Deputy SIRO
The Assistant Director of Informatics acts as the Health Board’s Deputy SIRO. The Deputy SIRO assists the SIRO in undertaking the responsibilities outlined above and acts as the deputy chair of the Information Governance Sub-committee.

6.4. Caldicott Guardian
The Medical Director & Director of Clinical Strategy acts as the Caldicott Guardian for the Health Board. The Caldicott Guardian is responsible for protecting the confidentiality of patient and service user information and enabling appropriate information sharing to promote high quality care.

The Caldicott Guardian:
- Leads and fosters a culture of good information governance across the Health Board with a focus on managing patient information.
- Upholds the standards around the safe and ethical use of patient information.
- Ensures that the Health Board is meeting its statutory requirements in relation to the management of patient information.
- Acts as the ‘conscience’ of the organisation and actively supports work to enable appropriate information sharing and, advises staff on the options for lawful and ethical use of information.

6.5. Deputy Caldicott Guardian
The Associate Medical Director of Professional Standards acts as the Deputy Caldicott Guardian for the Health Board. The Deputy Caldicott Guardian assists the Caldicott Guardian in undertaking the roles and responsibilities listed above and, attends the Information Governance Sub-committee and sub groups to provide appropriate advice and support.
6.6. Data Protection Officer (DPO)

The DPO facilitates the Health Board’s compliance with its legal and ethical obligations in relation to the management of personal information by providing expert advice to the organisation around its duties and responsibilities. The individual who will undertake the role of the DPO is currently being reviewed by the organisation.

The DPO:
- Advises the organisation of its requirements in relation to the Data Protection Act / General Data Protection Regulations 2016 or any subsequent legislation to the same effect and other EU member state data protection provisions.
- Monitors the organisation’s compliance with meeting the above and the organisation’s policies and procedures including the assignment of responsibilities and training of staff and related audits.
- Collects information to identify what processing the organisation is undertaking.
- Provides advice in relation to Data Protection Impact Assessments (DPIA) (Privacy Impact Assessments) and monitors their performance.
- Cooperates with the ICO and acts as the contact point including ensuring that the ICO is consulted in the event that a DPIA shows there is a high risk in a processing activity being undertaken (or proposed to be undertaken).
- Has regard for and provides advice around risks associated with the processing of personal data.
- Provides advice, information and issues recommendations to the organisation or any organisation processing information on behalf of the Health Board.

6.7. Information Asset Owners

Each service area and major system that contains personal information is owned by a named Information Asset Owner. These individuals are accountable for the information held within their service area and understand how the information is held, used and shared. They work with the SIRO and the Information Governance Team to effectively manage information risk within their service area.

The Information Asset Owners promote a culture of good information governance within their service areas and disseminate information and key messages to their managers and staff.

6.8. Information Asset Administrators

Information Asset Administrators are named individuals within each service who assist the Information Asset Owners in the responsibilities outlined above.

6.9. The Information Governance Team

The Information Governance Team is responsible for providing expert advice and assistance to the organisation and for putting the requirements of the Information Governance Framework into practice. The Information Governance Team work with the SIRO, Caldicott Guardian, the DPO, Information Asset Owners/Administrators and key staff across the Health Board to put in place all of requirements needed to ensure good information governance is in place across the Health Board:
- Staff training and awareness.
- Undertaking Data Protection Impact Assessments.
HYWEL DDA UNIVERSITY HEALTH BOARD

- Managing the Information Security Incident procedure.
- Undertaking the Caldicott Principles into Practice Assessment and implementing the Action Plan.
- Developing and implementing the Data Protection, Confidentiality and other related policies.
- Developing appropriate information sharing agreements.
- Developing Data Processing Agreements and reviewing contract arrangements with third party organisations and suppliers.
- Managing the National Integrated Intelligent Audit System (NIIAS) to ensure appropriate access to patient records.
- Managing corporate subject access requests and advising the access to medical records and freedom of information teams.
- Developing the Health Board's information and cyber security compliance.

6.10. Access to Health Records Team
The Access to Health Records Team process requests for access to patient records in-line with the organisation’s legal requirements and provide specialist advice and guidance about how patient health records are managed by the Health Board.

6.11. Corporate Office
The Health Board's Corporate Office manages requests and provides specialist advice in relation to the Freedom of Information Act 2000 and maintains the Health Board’s publication scheme and disclosure log. The Corporate Office has responsibility for the management of corporate information in-line with the Health Board's policies and procedures.

6.12. Managers
Managers and supervisors have the following responsibilities:
- Ensuring information governance policies, procedures and guidance notes are read and understood by their staff.
- Ensure staff have completed their mandatory information governance training every two years via the ESR portal.
- Ensure staff understand their responsibilities in terms of patient confidentiality, in particular the fact that staff should never access a patient record or information unless it is required for a valid work purpose.
- Encourage the safe handling of information by their staff and report any concerns about practice to their Information Asset Owner or to the Information Governance Team.
- Report any information security incidents they are made aware of to the Information Governance Team immediately.
- Seek further guidance from the Information Governance Team in relation to any requests for information sharing that fall outside of providing direct patient care or an agreed information sharing process (unless in emergency situations).

6.13. Staff
All staff have the following responsibilities:
- Read and understand the Health Board’s information governance policies, procedures and guidance notes and contact their manager if they require any clarification, advice and guidance.
- Complete their mandatory information governance training every two years via the ESR portal.
7. Information asset and information risk management
An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and lifecycles.

An information asset is usually a set of information that can be identified as it is used for a specific purpose or function within the Health Board.

Some examples of information assets:

- Patient complaint files,
- Staff disciplinary files,
- Child safeguarding referrals,
- Patient identifiable data held for a specific clinical audit,
- A patient waiting list in the A&E department,
- A database of contacts,

The Health Board retains an information asset register for each service area. The asset register lists all personal information held and further details such as how it is stored, who it is shared with, the legal basis for processing and how long it is stored for.

In addition to the asset register, the Health Board holds a detailed asset risk audit for its major systems that hold patient information. The risk audit has detailed information about how the information stored within the system is processed.

The Health Board maintains an asset risk register which identifies any information risk against an information asset and the actions that have been agree to mitigate that risk.

Information Asset Owner are responsible for agreeing any actions to mitigate risk linked to their information assets and ensuring the actions are completed. Information Asset Owners can transfer any significant information risk onto their service risk registers.

Any significant information risk that affects the organisation is added to the information governance risk register and is monitored through the Information Governance Sub-committee.

The diagram below outlines the information asset risk management cycle operated by the Health Board.
8. Governance structure
The Health Board has a clear governance structure to provide assurance to the Board that the organisation is complying with its statutory requirements and guidance and best practice in relation to information governance practice.
The Information Governance Sub Committee (IGSC) is responsible for ensuring the Health Board is compliant with information governance legislation and information handling requirements and good practice standards. The committee oversees and influences the development of Information Governance and Security across the Health Board and with third party suppliers and contractors.

The committee oversees the following key areas:

- 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
- Risk Management and Incident Management
- Data Protection Impact Assessments
- Patient records

The Information Governance Sub-committee (IGSC) provides assurance to the Board via the Business Planning and Performance Assurance Committee which it reports to on a bi-monthly basis. The IGSC receives regular assurance reports from its sub groups that detail the work undertaken and reporting significant risks.

The following sub-groups report to the Information Governance Sub-committee and oversee the day to day work in relation to key policy areas:

- **Information Asset Owners/General Data Protection Regulations (IAO/GDPR) Group** – to take forward the GDPR work plan, establish Information Asset Owners across the organisation and to develop an information asset register. NB: Data Quality has been added as a standing agenda item to this sub-group.
- **Information Governance Incident Group** – to ensure there is robust governance and assurance around how the organisation is managing and reporting on information security incidents.
- **National Integrated Intelligent Audit System (NIIAS) Project Group** – to take forward the roll out of the NIIAS system across the organisation and ensure that staff are adhering to patient confidentiality and system access requirements.
- **Health Records Group** – to discuss and resolve risk and issues affecting the health record and its users and to provide clear leadership in the promotion of effective health records management. To support the development of a Health Board wide integrated records management system, including storage, security arrangements and the move towards an electronic patient record (EPR), providing expert advice and guidance.

From 2018 the following work plans will be overseen by the IGSC and form the basis of its assurance framework:

- Caldicott Principles into Practice (C-PIP) Action Plan.
- The GDPR/IAO Implementation Action Plan.
- IG Training and Awareness Action Plan
9. Information governance policies and procedures
The IGSC has responsibility for recommending policies and procedures relating to information governance to the Business Planning & Performance Assurance Committee for approval on behalf of the Board.

The following policies and procedures are in place as part of the information governance framework.

<table>
<thead>
<tr>
<th>Policy name</th>
<th>Approval/last review date</th>
<th>Next review date</th>
<th>Policy owner</th>
<th>Owning committee/approving committee</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acceptable use of IT Policy</td>
<td>Jan 2013</td>
<td>Currently under review</td>
<td>Head of ICT</td>
<td>IGSC/BPPAC</td>
</tr>
<tr>
<td>CCTV Policy</td>
<td>April 2013</td>
<td>Currently under review</td>
<td>Risk/Health and Safety Manager</td>
<td>IGSC/BPPAC</td>
</tr>
<tr>
<td>Confidentiality Policy</td>
<td>April 2015</td>
<td>April 2018</td>
<td>Head of IG</td>
<td>IGSC/BPPAC</td>
</tr>
<tr>
<td>Consumer Device Policy (Smartphone/Tablets)</td>
<td>April 2015</td>
<td>April 2018</td>
<td>Head of ICT</td>
<td>IGSC/BPPAC</td>
</tr>
<tr>
<td>Corporate Records Management Policy</td>
<td>June 2013</td>
<td>Currently under review</td>
<td>Corporate Services</td>
<td>IGSC/BPPAC</td>
</tr>
<tr>
<td>Corporate Records Management Strategy</td>
<td>June 2013</td>
<td>Currently under review</td>
<td>Corporate Services</td>
<td>IGSC/BPPAC</td>
</tr>
<tr>
<td>Data Protection Policy</td>
<td>May 2016</td>
<td>May 2018</td>
<td>Head of IG</td>
<td>IGSC/BPPAC</td>
</tr>
<tr>
<td>Display Screen Equipment Procedure</td>
<td>June 2016</td>
<td>June 2019</td>
<td>Head of ICT</td>
<td>IGSC/BPPAC</td>
</tr>
<tr>
<td>Disposal of Information/IT Assets Policy</td>
<td>Jan 2013</td>
<td>Currently under review</td>
<td>Head of ICT</td>
<td>IGSC/BPPAC</td>
</tr>
<tr>
<td>All Wales E-mail Use Policy</td>
<td>Feb 2017</td>
<td>Feb 2019</td>
<td>Head of ICT</td>
<td>IGSC/BPPAC</td>
</tr>
<tr>
<td>Freedom of Information Policy</td>
<td>July 2013</td>
<td>Currently under review</td>
<td>Head of Corporate Office</td>
<td>IGSC/BPPAC</td>
</tr>
<tr>
<td>Health Records Management Policy</td>
<td>August 2015</td>
<td>August 2018</td>
<td>Health Records Manager</td>
<td>IGSC/BPPAC</td>
</tr>
<tr>
<td>Health Records Management Strategy</td>
<td>August 2015</td>
<td>August 2018</td>
<td>Health Records</td>
<td>IGSC/BPPAC</td>
</tr>
<tr>
<td>Policy name</td>
<td>Approval/last review date</td>
<td>Next review date</td>
<td>Policy owner</td>
<td>Owning committee/approving committee</td>
</tr>
<tr>
<td>------------------------------------------------------</td>
<td>---------------------------</td>
<td>------------------</td>
<td>---------------------------------------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>Information Classification Policy</td>
<td>August 2017</td>
<td>August 2020</td>
<td>Head of IG</td>
<td>IGSC/BPPAC</td>
</tr>
<tr>
<td>Information Governance Incident Procedure</td>
<td>January 2018</td>
<td>January 2020</td>
<td>Head of IG</td>
<td>IGSC/BPPAC</td>
</tr>
<tr>
<td>Information Quality Assurance Strategy</td>
<td>Dec 2011</td>
<td>Currently under review</td>
<td>Head of Information Services</td>
<td>IGSC/BPPAC</td>
</tr>
<tr>
<td>Information Security Policy</td>
<td>June 2015</td>
<td>June 2018</td>
<td>Head of IG</td>
<td>IGSC/BPPAC</td>
</tr>
<tr>
<td>All Wales Internet Usage Policy</td>
<td>Feb 2017</td>
<td>Feb 2019</td>
<td>Head of ICT</td>
<td>IGSC/BPPAC</td>
</tr>
<tr>
<td>Informatics Procurement and Requests Procedure</td>
<td>Feb 2017</td>
<td>Feb 2020</td>
<td>Head of ICT</td>
<td>IGSC/BPPAC</td>
</tr>
<tr>
<td>Mobile Working Policy</td>
<td>March 2016</td>
<td>March 2019</td>
<td>Head of ICT</td>
<td>IGSC/BPPAC</td>
</tr>
<tr>
<td>Network Security Policy</td>
<td>March 2016</td>
<td>March 2019</td>
<td>Head of ICT</td>
<td>IGSC/BPPAC</td>
</tr>
<tr>
<td>Retention and Destruction of Records Policy (including Health Records)</td>
<td>August 2015</td>
<td>August 2018</td>
<td>Health Records Manager</td>
<td>IGSC/BPPAC</td>
</tr>
<tr>
<td>Reuse of Public Sector Information Procedure</td>
<td>Dec 2014</td>
<td>Dec 2017</td>
<td>Corporate Services</td>
<td>IGSC/BPPAC</td>
</tr>
<tr>
<td>Secure Transfer of Personal Information Policy</td>
<td>Aug 2017</td>
<td>Aug 2020</td>
<td>Head of IG</td>
<td>IGSC/BPPAC</td>
</tr>
<tr>
<td>Third Party Supplier Security Policy</td>
<td>Jan 2018</td>
<td>Jan 2020</td>
<td>Head of IG</td>
<td>IGSC/BPPAC</td>
</tr>
<tr>
<td>User Account Management Policy</td>
<td>Feb 2016</td>
<td>Feb 2019</td>
<td>Head of ICT</td>
<td>IGSC/BPPAC</td>
</tr>
</tbody>
</table>

All policies are available to staff via the Health Board’s policies and procedures information governance intranet page: Information Governance Policies and Procedures

10. Information governance training and awareness

10.1 Current approach to information governance training

The Health Board is currently adopting the following approach to staff information governance training:

- The Health Board offers a mandatory e-learning information governance module that must be completed by all staff every two years.
- The Information Governance Team undertakes mandatory classroom based training for any staff that have accessed their own record or a family member’s record without a valid work reason for doing so.
- The Information Governance Team undertakes mandatory classroom based training for any teams where there has been an information security incident or near miss.
- Managers and staff can request additional training from the information governance team if they have identified a need within their service area.
The Information Governance Team undertake classroom based information governance training for key staff groups on a regular basis e.g. nursing staff, clinical staff etc.

The Information Governance Team undertake regular training for newly qualified nurses prior to them commencing with the Health Board.

10.2 Current approach to awareness raising
The Information Governance Team undertake a number of awareness raising activities which are planned through an annual communications plan. Some examples of activities are provided below:

- Producing and disseminating information leaflets, posters and FAQs.
- Running Information Governance drop-in sessions.
- Running a Data Protection/Information Governance Awareness Week.
- Using global e-mails, pop-ups, newsletters and messaging to provide information to staff.
- Information Governance Officers regularly visit hospital sites.

10.3 Monitoring of training compliance
Information Governance mandatory training compliance is reported on and monitored through the IGSC on a bi-monthly basis.

10.4 Information Governance Training and Awareness Strategy
The Health Board will be developing an Information Governance Training and Awareness which will be implemented from April 2018. This strategy will be accompanied by a dedicated action plan to develop a strategic approach to improving information governance training and awareness within the current resources available. The strategy will look at the following key areas:

- Improving the completion rate for mandatory information governance training.
- Undertaking a training needs analysis to ensure that resources are concentrated in the right areas.
- Developing an on-line resource of easy read guides for managers and staff that cover key information governance areas.
- Improving the information provided to new staff at induction.
- Identifying areas where training is already taking place with key staff groups and putting information governance onto the agenda.

11. Information governance incident management
The Health Board has a 602 Information Governance Incident Procedure that provides clear guidance to staff about what to do if they become aware of an information security incident. All incidents must be reported to the Information Governance Team immediately through the standard reporting form.
11.1 Incident reporting process
The following process is followed for the management of all information security incidents:

**Emergency Management**
- Assessing the risk and scoring the incident.
- Containing the breach and retrieving any information/protecting confidentiality.
- Informing affected individuals/relevant organisations.

**Formal Information Governance (IG) Investigation**
- Nominate the IG investigating officer.
- Link with Workforce and manager. Workforce will decide if a separate investigation in line with the disciplinary policy is required.
- Link with other relevant departments e.g. Patient Support and Legal Services.
- Oversee investigation report with identified findings, lessons learnt and SMART action points.
- Report outcome to Information Governance Incident Group.

**Formal Report and Closure**
- Monitor action points until completion.
- Close incident once all actions completed with agreement from the Information Governance Incident Group.

11.2 Reporting structures
The Information Governance Incident Group functions as the primary reporting and decision making group in relation to all information security incidents. The Group will meet on a monthly basis and be chaired by either the SIRO or Deputy SIRO.

The Information Governance Incident Group reports to the following:
- The Information Governance Sub-committee on a bi-monthly basis.
- The Executive Team when it is agreed they need to be made aware of a particular information security incident, process or decision. This will be agreed by the SIRO or at the Information Governance Incident Group meetings.
- To the In Committee Board on a quarterly basis.
12. Managing third party access to information
12.1 Third party supplier agreements and contracts
The Health Board has a 279 - Third Party Supplier Security Policy which outlines the process that must be followed before information is shared as part of any agreement or contract with an outside organisation.

The policy is linked to the Health Board’s procurement process and ensures that full assurance is provided to the Health Board that a third party supplier has the appropriate security and technical measures in place to protect the Health Board’s personal information.

The Health Board ensures that any contract or agreement entered into with a third party supplier has the appropriate contract or data processing agreement in place that outlines the information governance requirements prior to any information being shared.

12.2 Information sharing with other organisations
Information sharing is managed in accordance with the Health Board’s data sharing protocols to ensure information sharing is managed in line with the organisation’s legal duties and is carried out in a safe and secure way.

Information is shared on a strictly ‘need to know’ basis with only the minimum amount of information required being shared.

The Health Board is planning to develop an Information Sharing Policy and Procedure as part of the Information Governance Team’s 2018/19 work plan to ensure that all staff are clear about their responsibilities in this area.

13. IT, cyber security and business continuity
The Health Board apply a comprehensive set of controls to the internal network to ensure resilience and disaster recovery in the event of a temporary or total loss of the network and/or key IT systems.

Business continuity plans are in place for key electronic systems and a programme of development is being implemented through the Information Asset Owners Group.

The Health Board is currently working towards Cyber Essentials and ISO 27001 compliance and a fully resourced action plan will be available from 2018 onwards following a mapping and gapping exercise that is currently being undertaken.

14. Monitoring and review
The key areas of information governance and their related action plans are monitored through regular reporting to the Information Governance Sub-committee. These action plans form the basis of the annual work plan for the Information Governance Team.

Regular audits are undertaken by the shared services audit team with actions identified and agreed by the service lead. Progress against these actions are monitored through the Information Governance Sub-committee and, any areas of the information governance framework that are considered to be of limited assurance and below are reported to the Audit and Risk Assurance Committee which reports directly to the Board.
Welsh Audit Office carry out an annual audit of the Health Board’s information governance practice and, recommended actions are built into the Information Governance Team’s work plan and are reported through the Information Governance Sub-committee.

The Information Governance Framework is reviewed every two years through the Information Governance Sub-committee.
15. Appendix 1 – Responsibility for the management of Information Assets within Hywel Dda University Health Board

**Senior Information Risk Owner (SIRO) and Deputy SIRO**
(Managing information risk)

**Caldicott Guardian and Deputy Caldicott Guardian**
(Legal and ethical use of patient information)

**Information Asset Owners (IAOs)**
(Ensuring the use of patient and other personal information within their designated service area is identified, documented and securely handled in line with the agreed Health Board policies and procedures).

**Information Asset Administrator (IAA)**
(Support IAO in their role and act as information governance link within service area).

**Data Protection Officer and Information Governance Team**
(Provide professional support, advice and guidance to all these individuals. Ensure policies and procedures are up to date and meet statutory requirements).

**Information Asset**
Identified electronic/filing/storage system that holds a named common set of records e.g. patient record, employee record, complaint files.