Swansea Bay University Health Board (SBU) Information Governance (IG) Framework 2020-2022

This document may be made available in alternative formats and other languages, on request, as is reasonably practicable to do so.

Document Author:	**Head of Information Governance**
Approved by:	**Audit Committee**
Approval Date:	
Review Date:	**December 2022**
Document No:	**[this will be allocated by the document custodian i.e. Corporate Administration or COIN Team]**

Contents

Page

1. INTRODUCTION

Information Governance (IG) is a series of best practice guidelines and principles of law to be followed by NHS organisations and their employees in relation to the handling of information; it applies to sensitive and personal data of both employees and patients and corporate information. It is the framework within which accountability, standards, policies and procedures are developed and implemented, to ensure all information created, obtained or received by the Health Board is held and used appropriately.

Information is a vital asset for the Health Board, supporting day to day clinical and business operations and the effective management of services and resources. The Health Board requires accurate, timely and relevant information to enable it to deliver the highest quality health care and to operate effectively as an organisation. It is the responsibility of all staff to ensure that information is complete and up to date and that it is used proactively to support the business of the organisation. Having accurate relevant information available at the time and place where it is needed is critical in all areas of the Health Board's activities and plays a key part in corporate and clinical governance, strategic risk, service planning and performance management.

2. PURPOSE

This Framework covers the period 2020-2022 and builds upon on the first IG Strategic Direction and Framework 2017-2020. It includes the continuing development, implementation and embedding of a robust IG framework needed for the effective management and protection of the Health Board's information assets. It outlines the organisation's IG vision over the next 3 years and acknowledges the ongoing closer working relationship with the Local Authorities.

The IG arrangements underpin the Health Board's Strategic Aims and Enabling Objectives, ensuring that the information needed to support and deliver their implementation is available, accurate and clear. In addition, IG has been noted as an essential enabler within Digital Service's 2020 Framework.

The IG Framework's purpose below sets out to ensure the following primary aims of effective IG are achieved:

- Information will be organised, monitored and maintained in accordance with legal and regulatory frameworks and will be kept confidential where appropriate
- The integrity of information will be assured, monitored and maintained, to ensure that it is of expected quality and reliable for use for the purposes that it is collected and used for
- Information required for operational purposes will be kept secure and available to and accessed by those who need it
- Relevant patient information will be shared with health and social care organisations to support direct patient care

- All staff will have access to appropriate training and education to ensure they understand their responsibilities for managing information and abiding by the law
- All patients' and staff's rights with regards to their personal data will be upheld complying with data protection legislation
- The Risk Management procedure will be implemented to ensure ownership of and accountability for the Health Board's information assets and the mitigation of associated risks.

3. RESPONSIBILITIES

The summary below sets out the roles and responsibilities and accountabilities relating to the management of IG – see also Appendix 1.

3.1 The Board

The ultimate responsibility for IG in the NHS rests with the Board of each organisation, who should note that:

- IG is an important part of the Health Board's overall governance arrangements and, as such, needs to be considered when the Accountable Officer prepares the Health Board's Annual Governance Statement. In particular, information on personal data related incidents that have been formally reported to the Information Commissioner's Office (ICO) and personal data related incidents including serious incidents involving data loss or confidentiality breaches should be disclosed. Details of how the risks to information are managed and controlled should also be included
- It is good practice to have an Executive level Senior Information Risk Owner (SIRO) in each organisation and an Information Asset Owner (IAO)/Administrator (IAA) should be designated for each separate database or other major information asset
- An annual SIRO Report is made publically available
- Appropriate IG training is mandatory for all users of personal data and for all those in key roles
- It is a requirement of data protection legislation to uphold the rights of all staff and patients with regards to their personal data
- The results of the annual IG assessment, Caldicott Principles into Practice and/or the IG Toolkit, are made available to the public
- Organisations must provide assurance that they are meeting key IG requirements and must have robust improvement plans to address any shortfalls against other requirements.

3.2 The Chief Executive

The Chief Executive is the Accountable Officer of the Health Board and has overall accountability and responsibility for IG. He/she is required to provide assurance, through the Annual Governance Statement, that all risks to the organisation, including those relating to information, are effectively managed and mitigated.

3.3 The SIRO

The Executive Director of Corporate Governance is the SIRO and has a key understanding of how the strategic goals of the Health Board may be impacted by information risk. They are the Board member leading on IG. The SIRO provides an essential role in ensuring that identified information security risks are followed up and incidents managed. The Deputy SIRO is the Chief Information Officer.

3.4 The Caldicott Guardian

The Caldicott Guardian plays a key role in ensuring that the Health Board satisfies the highest practical standards for handling patient personal data. Within the Health Board the nominated Caldicott Guardian role is fulfilled by the Medical Director. Acting as the conscience of the Health Board, the Caldicott Guardian actively supports work to enable information sharing where it is appropriate to share, and advises on options for lawful and ethical processing of information. The Caldicott Guardian also has a strategic role which involves representing and championing confidentiality and information sharing requirements and issues at senior management level. The Caldicott Guardian has responsibility for approving the annual Caldicott Principles into Practice (C-PiP) self assessment or, going forward, the IG Toolkit. The role of Deputy Caldicott Guardian is held by the Deputy Medical Director.

3.5 Information Governance Group (IGG)

The purpose of the IGG is to provide the Audit Committee with evidence based and timely advice to assist it in discharging its functions and meeting its responsibilities with regard to:

- Information quality and integrity
- Information safety and security
- Appropriate access and use of information to support its provision of high quality healthcare and staff management.

The IGG will provide assurance to the Audit Committee in relation to the Health Board's arrangements for creating, collecting, storing, safeguarding, disseminating, sharing, using and disposing of information in accordance with:

- Its Terms of Reference
- Legislative responsibilities, e.g. the Data Protection Act 2018, the General Data Protection Regulation 2018 (this may change post full Brexit completion) and the Freedom of Information Act 2000
- Any relevant requirements and standards determined for the NHS in Wales.

The IGG will meet quarterly and offers the framework across SBU to achieve IG compliance within all areas.

3.6 IGG Leads

The nominated Leads that represent their Service Delivery Group (SDG)/Corporate Department on the IGG will be supported and trained by the Head of IG and IG Team so that they become responsible in their area for:

- Local IG Champion to promote and improve IG compliance and standards
- Disseminating IG information
- Signposting to and promoting of mandatory IG training
- Signposting to appropriate IG and Information Security advice
- Identifying Information Assets, their Owners and Administrators, and supporting the mapping of information flows and production of data sharing agreements
- Completing the IG Toolkit (or equivalent)
- Supporting IG and Information Security audits, and providing evidence to IGG of equivalent audits if they are already occurring by some other means
- Identifying and recording IG risks, producing action plans to address these and reporting back to IGG on progress made
- Providing an IGG Lead Update Report to the IG Partnership Group (IGPG) quarterly
- Nominating suitable representatives to sit on IGG Subgroups and Task and Finish groups.

3.7 Information Governance Partnership Group (IGPG)

The purpose of the Information Governance Partnership Group (IGPG) is to strengthen partnership working between the IG team and Information Governance Group (IGG) Leads and representatives. At IGPG meetings the IG team offers practical and operational support to the IGG Leads on all aspects of IG, providing learning and practical knowledge on agreed IG topics. The IGPG provides opportunities for operational discussions and to share lessons learned with the IG team and other IGG Leads. The IGPG supports the IGG in driving the broad IG agenda across the organisation by developing and implementing effective and consistent approaches and encouraging good practice on all aspects of IG.

3.8 Data Quality Group

The Data Quality Group supports the work of the IGG as one of its Subgroups. It aims to provide them with assurance that the organisation is making appropriate progress in developing systems, policies and processes to ensure that the Health Board is compliant in discharging its responsibilities relating to Data Quality.

3.9 IG Lead

The Deputy Chief Information Officer is the IG Lead and co-ordinates the IG Work Plan (see Appendix 4). The key responsibilities include developing and maintaining the Health Board's IG Framework and relevant policies ensuring top level awareness and support for IG resourcing and implementation of improvements.

3.10 The Head of IG and the IG Team

The Head of IG is responsible for overseeing the IG systems and processes within the Health Board and carrying out operational duties for the IG Lead. The Head of IG is the Data Protection Officer and designated contact with the ICO. As part of this role they will ensure that the Health Board's annual Data Protection Registration is maintained and kept up to date. The Team will provide expert advice, guidance and training on IG issues and deliver the IG Work Plan.

3.11 Digital Services Directorate

The IG Lead, Head of IG and the IG Team all reside within the Digital Services Directorate which is led by the Organisation's Director of Digital.

3.12 Service Delivery Group Directors and Service Managers

Service Delivery Group Directors and Service Managers have responsibility for the protection of personal data and for identifying and managing any associated risk. They are responsible for enforcing measures to protect information, including personal data as part of normal/everyday activity, setting and driving forward a culture that properly values, protects and uses data both in planning and delivery of Health Board services. They are responsible for ensuring that their staff follow the IG Incident and Near Miss Procedure. They are responsible for ensuring excellent data quality and to support their IAOs in auditing this and addressing any issues. They are responsible for ensuring actions required as a result of an IG Audit are carried out in a timely manner. They are responsible for ensuring Data Protection Impact Assessments (DPIAs) are completed whenever required.

3.13 All Employees, Contractors, Volunteers and Students

All employees, contractors, volunteers and students working for or supplying services to the Health Board who have access to personal data are responsible for ensuring that any personal data which they hold are kept securely, are not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party. This is supported by an appropriate confidentiality clause within their contract of employment or other contract with the Health Board. Any IG incidents and near misses should be reported on the organisation's Datix incident reporting system. Staff must be familiar with the Health Board's associated IG policies and procedures and comply with these. Staff must maintain their compliance with the mandatory IG training package, at the start of their employment and every 2 years thereafter.

3.14 NHS Wales Informatics Service (NWIS)

NHS Wales Informatics Service has a dedicated team to deal with strategic and operational IG issues that affect the NHS in Wales. Their work includes coordinating national IG meeting groups, providing advice and support on a number of IG issues including information sharing protocols in accordance with the Wales Accord for Sharing Personal Information (WASPI) framework etc.. The national IG framework and strategy is currently in development.

3.15 Third Party Contractors

Appropriate contracts, Data Processing Agreements and confidentiality agreements shall be in place with third parties where potential or actual access to the Health Board's confidential information assets is identified.

3.16 Information Commissioner's Office (ICO)

The ICO is the UK's independent body set up to uphold information rights in the public interest. Their role includes regulating key pieces of legislation including the Data Protection Act 2018 and Freedom of Information Act 2000. Part of their role is to improve the information rights practices of organisations by gathering and dealing with concerns raised by members of the public. In cases where a clear and serious breach of the legislation has taken place, they may take enforcement action and in the most serious cases, can serve a monetary penalty of up to 4% of annual turnover. SBU will work closely with the ICO to improve our standards, and this includes fully co-operating with their assessments and recommendations following reported IG breaches and ICO audits, and using those recommendations to inform our IG Framework, Policies and Work Plan.

3.17 Information Asset Owners (IAOs)

The IAO will be identified as the person who has operational ownership of an information asset. This is usually someone at Head of Department or other senior managerial position, dependent on the structure of the department. A person will be identified as an IAO primarily due to them being responsible for purchasing the asset or requiring it for their service. Systems may be provided to users across the Health Board but it is the different types of information held that are those owned by a designated manager. An IAO has responsibility for providing assurance to the Service Delivery Group Directors, IGG Leads and the SIRO that information is effectively managed within their SDG/Department. The IAO will also undertake the role of Data Custodian, as required by the Data Protection Act 2018.

The IAO will document, understand and monitor:

- What information assets are held, and for what purpose
- How information is created, amended or added to over time
- Who has access to the information and why
- Understand and address the risk to the asset, providing assurance to the SIRO.

Key responsibilities include:

1. Identifying and documenting the scope and importance of all information assets they own. This includes identifying all information necessary in order to respond to incidents or recover from a disaster affecting the information asset
2. Taking ownership of their local asset control, risk assessment and management processes for the information assets they own. This includes the identification, review and prioritisation of perceived risks and oversight of actions agreed to mitigate those risks

3. Providing a focal point for the resolution and/or discussion of risk issues affecting their information assets
4. Ensuring that staff and other relevant people are aware of, and comply with, expected information governance and Data Protection working practices for the effective use of information assets
5. Ensuring that the Organisation's requirements for information incident identification, reporting, management and response apply to the information assets they own; including ensuring completion of Data Flow Mapping exercises when required
6. Supervising and delegating tasks to the Information Asset Administrator
7. Completing annual audits of their information assets with the support of the Information Governance Department.

3.18 Information Asset Administrators (IAAs)

The IAOs will determine a person or persons who will be responsible for the day to day management of an application. Information Asset Administrators (IAAs) will be responsible for the data integrity of applications, user access including auditing of access, ensuring that there are appropriate operational procedures that include backup, business continuity planning. The IAAs will liaise with system suppliers to ensure that the asset is maintained so as to be fit for purpose. They may delegate certain tasks to third parties (e.g. to Digital Services) but will have responsibility for ensuring delegated responsibilities are carried out.

4. IG ASSURANCE

4.1 IG Assurance Framework

The IG Assurance Framework (Appendix 2**)** is the mechanism by which

- IG policies and standards are set
- Regulators can check an organisation's compliance
- The organisation can be performance managed.

The organisation's IG structure is illustrated in Appendix 3.

4.2 Legal compliance and other key drivers

The work of the IG Department is based on the IG Work Plan. This plan highlights areas requiring improvement identified through a number of means including:

- Compliance with current key legislation e.g. General Data Protection Regulation 2018, Data Protection Act 2018 and Freedom of Information Act 2000
- Compliance with national standards e.g. NHS Codes of Practice, IG Toolkit
- Internal and external audits
- IG incident and near miss management
- IG risk management
- ICO guidance and recommendations

- IG Toolkit annual submission

4.3 Health and Care Standard 3.4

This standard applies to IG and Communications Technology. It is in place to ensure health services' information enables the delivery, management, planning and monitoring of high quality, safe services. SBU will have systems in place, including information and communication technology, to ensure the effective collection, sharing and reporting of high quality data and information within a sound IG framework.

In order to meet the standard, SBU will:

- Develop safe and secure information systems in accordance with legislation and within a robust governance framework
- Have processes to operate and manage information and data effectively, to maintain business continuity and to support and facilitate patient care and delivery
- Have data and information that is accurate, valid, reliable, timely, relevant, comprehensible and complete
- Use information to review, assess and improve services
- Share information with relevant partners using protocols when necessary to provide good care for people.

4.4 IG Toolkit

The IG Toolkit has been developed by NWIS for organisations to use as their primary mechanism for benchmarking compliance across secondary care in Wales. It is a self audit tool that is publically reported and utilised to inform the IG Work Plan.

4.5 IG Work Plan

The Work Plan (Appendix 4) is based on the drivers stated in sections 4.2, 4.3 and 4.4, along with those actions remaining from the GDPR specific work plan in place during the last Strategic Direction timeframe and discussions held across the NHS in Wales. It has evolved over time to include all areas of IG requiring improvement which have been identified. It provides the focus for the IGG who can review priorities based on the associated risks.

5. IG DIRECTION

Through implementing this IG Framework the Health Board will:

5.1 Audit and Monitoring

Undertake regular reviews, assessments and audits of how information is recorded, held, accessed, used and shared. This includes third party supplier audits and review of existing contracts and other relevant documentation. The outcomes will be used to identify good practice and opportunities for improvement. Benchmarking

against other Health Boards in Wales and England will be used to inform our continual strive for the best achievable IG compliance across SBU.

5.2 Policies, Procedures and Guidelines

Ensure that all practice, policies and procedures relating to the handling and holding of personal and Health Board corporate information are legal and conform to best and/or recommended practice and that a review process is in place to monitor their effectiveness so improvements or deterioration in information handling standards can be recognised and addressed. Any All-Wales IG policies will be adhered to.

5.3 Training and Awareness

Work to instil a culture that recognises the importance of IG, and improves IG compliance in the Health Board through increasing awareness and providing IG mandatory training every 2 years as per the Core Skills Framework. This will be offered via video or via e-learning. All students, volunteers and staff, whether permanent, temporary or contracted, should be aware of their own individual responsibilities for the maintenance of confidentiality, data protection, information security management and information quality. The IGG Leads will monitor training compliance in their areas, and individual line managers are responsible for ensuring compliance of their staff and monitoring this via the PADR process. IG training compliance by SDG/Corporate Dept will be reported to IGG quarterly.

5.4 Information for Service Users/The Public/Staff

Review and maintain an IG communications strategy to ensure that staff, patients and the public are adequately informed about confidentiality and the way their information is used and shared, their rights as data subjects, in particular how they may access their personal data and how they may exercise those rights. Effective Tier 2 and Tier 3 privacy notices will continue to be developed and maintained across the Health Board for both staff and patient personal data. Effective procedures will ensure that detailed questions raised by patients can be answered and their right of choice can be exercised and respected. Ensure that non confidential information about the Health Board and its services is readily and easily available through a variety of media, in line with the Health Board's Publication Scheme. Review and expand the IG Intranet pages to continue to support staff, and publish regular bulletins to refresh and/or inform staff on their responsibilities.

5.5 Data Protection Impact Assessments (DPIAs)

Utilise appropriate technical and organisational measures to implement the data protection principles and safeguard individuals' rights: This is data protection by design and by default. SBU ensures that data protection is embedded from the outset into the organisation's processing activities and business practices, from the design stage right through the lifecycle. This is enabled by the completion, IG approval and ongoing review of DPIAs for all new flows of personal data where they may be a risk to the rights and freedoms of data subjects. This ensures that the organisation complies with data protection legislation's fundamental principles and requirements, and forms part of the focus on accountability.

5.6 Information Confidentiality

Ensure that patient and staff confidentiality is maintained in accordance with the Confidentiality Code of Practice for Health and Social Care in Wales and legal requirements under the Data Protection Act 2018, European Convention of Human Rights (Article 8) (Human Rights Act 1998) and common law.

5.7 Data Quality

Ensure managers take ownership of, and seek to improve the quality of information within their services and that information quality is assured at the point of collection. Quality will be maintained through accurate recording and through clear and consistent definition of data items in accordance with national standards.

5.8 Information Asset Register (IAR)

Build upon the IAR to continue to catalogue all structured Health Board information held, whether paper, electronic or some other form. IAOs identified are answerable to the SIRO and responsible for the named asset(s). IAAs identified are answerable to the relevant IAO and responsible for the day-to-day management of the named asset(s). All assets must be managed in a secure and confidential way, adhering to relevant legislation and best practice. Information sharing will be monitored via the IAR. The IAO will be responsible for annually auditing the security and compliance of their respective asset(s) utilising guidance documentation produced by the IG Department. Reports on the IAR are received by IGG quarterly, and an overview is included in the annual SIRO Report.

5.9 Information Sharing

Ensure that, where appropriate and subject to confidentiality constraints, information is securely and legally shared with other NHS, social care, partner organisations and contractors in order to support patient care. This should be managed in accordance with the WASPI framework and will include the use of Information Sharing Protocols, Data Disclosure Agreements, Intra NHS Sharing Agreements and Data Processing Agreements.

5.10 IG Risk Management

Continue to develop and utilise clear lines of accountability for information risk management that lead directly to the Senior Leadership Team. The SIRO, IGG Leads, IAOs and IAAs will be accountable for the management and mitigation of information risks and will provide assurance to that effect for the Annual Report and Statement of Internal Control. Information risk will be managed via IGG and the Health Board Risk Management Policy.

5.11 Breach Management

All IG incidents and near misses will be reported via Datix and managed using the IG Incident and Near Miss Procedure. All reported instances of actual or potential breaches of information security and confidentiality will be investigated and the ICO informed when necessary. Actions Taken and Lessons Learnt will be managed via IGPG and highlight reports taken to the IGG to improve compliance and to notify of particular areas of risk.

5.12 Cyber Security

The Cyber Security Team has been formed in 2020 following the appointment of a Cyber Security Manager and two additional Cyber Security Specialists, to work with the existing IT Security Manager. The formation of this team has provided an opportunity to improve cyber security and move to a proactive rather than reactive approach. The work plan to date has focused on the implementation of a number of local and national tools to provide insights into the security risks across the health board, and proactively investigate and mitigate against those risks. Awareness of Cyber Security across the workforce is being achieved through the availability of training material and the targeted training.

Figure 1 below illustrates the relationship between IG and Cyber Security:

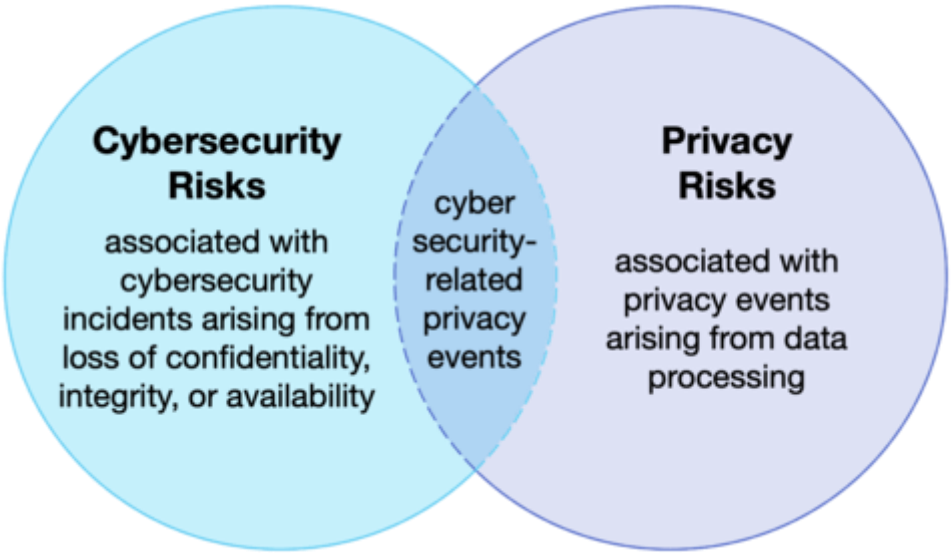


Figure 1 - NIST Cyber and Privacy Framework

The Health Board is classified as an Operator of Essential Services under the Networking and Information Systems Regulation (NIS), which sets out regulatory requirements and expectations for Cyber Security. Welsh Government will be the authority on upholding these regulatory requirements, and work is underway in preparedness for this in the Cyber Security Team. Just like GDPR, failure to comply with this regulation, or experiencing a breach through lack of compliance, can result in multi-million pound fines.

A Cyber Security Framework draft will be developed within the first half of 2021, and will directly address the objectives required to meet NIS compliance. The outcome of

ongoing Infrastructure Review and M365 Compliance will influence strategy. This work is happening in parallel to, and in collaboration with, other Health Boards in Wales to establish the scope and criteria for compliance with Welsh Government.

5.13 Joint/Collaborative Working

Continue to develop close working relationships with other Welsh Health Boards, WAST, Swansea University, the local Authorities and 3rd sector organisations in respect of IG. Collaborate over key areas of IG and adopt a joint approach to tackling areas identified within the IG Work Plan where possible. Continue to support the NWIS digital programme and other national/local initiatives as appropriate eg. WCCIS and PKB. Explore links with Primary Care to ensure the appropriate governance and assurance is developed. Work with Research and Development to ensure best practice with regards to IG and confidentiality.

5.14 Governance

Maintain a clear reporting structure and ensure through management action and training that all staff understand IG requirements. Develop information systems and reporting processes which support effective performance management and monitoring. IGG Leads are responsible for ensuring that IG is embedded into their SDG/Corporate Department governance structure and that IG compliance is upheld in their areas.

5.15 Records and Information Management

Ensure effective processes are in place to manage records and information. Effective management of records will ensure that information is available and held securely in identified repositories. This will support the delivery of patient care, enable the Health Board to respond promptly to access to information requests and support openness and transparency where appropriate.

5.16 IG Key Performance Indicators (KPIs)

Report IG KPIs quarterly to the IGG. These will include:

- IG incidents reported to the ICO
- IG breach trends noted on Datix
- IG breaches noted on National Intelligent Integrated Auditing Solution (NIIAS))
- Subject Access Request compliance
- Mandatory training uptake figures
- Freedom of Information Requests (reported by Board Secretary)
- IG Audit summaries
- Data Quality Standards

5.17 IG Performance Reporting and Evaluation

Measure the Health Board's IG performance though:

- Quarterly IG Work Plan Progress Reports taken to the IGG
- Review of all internal and external audits and associated Management Response(s)
- Annual IG Toolkit score
- IG KPIs taken to IGG quarterly
- Register of DPIAs taken to IGG quarterly
- Register of data sharing agreements taken to IGG quarterly
- IG self-assessment report from each IAO
- IGG Lead reports taken to IGG quarterly
- Annual Governance statement contribution

The IGG will be responsible for challenging IG performance and ensuring actions are taken to address shortfalls. The SIRO will report on IG performance to the Audit Committee and Senior Leadership team quarterly via the IGG Chair's Assurance report and annually via the SIRO Report.

6. IG FRAMEWORK IMPLEMENTATION

The IGG will monitor implementation of this IG Framework during the next 3 years. This will be achieved through the quarterly review of the IG Work Plan and ongoing support of the necessary resources given to the IG Department.

The IGG will review this IG Framework in 2022 or earlier in response to any significant changes to mandatory requirements including data protection legislation, guidance or as a result of significant IG risks or breaches.

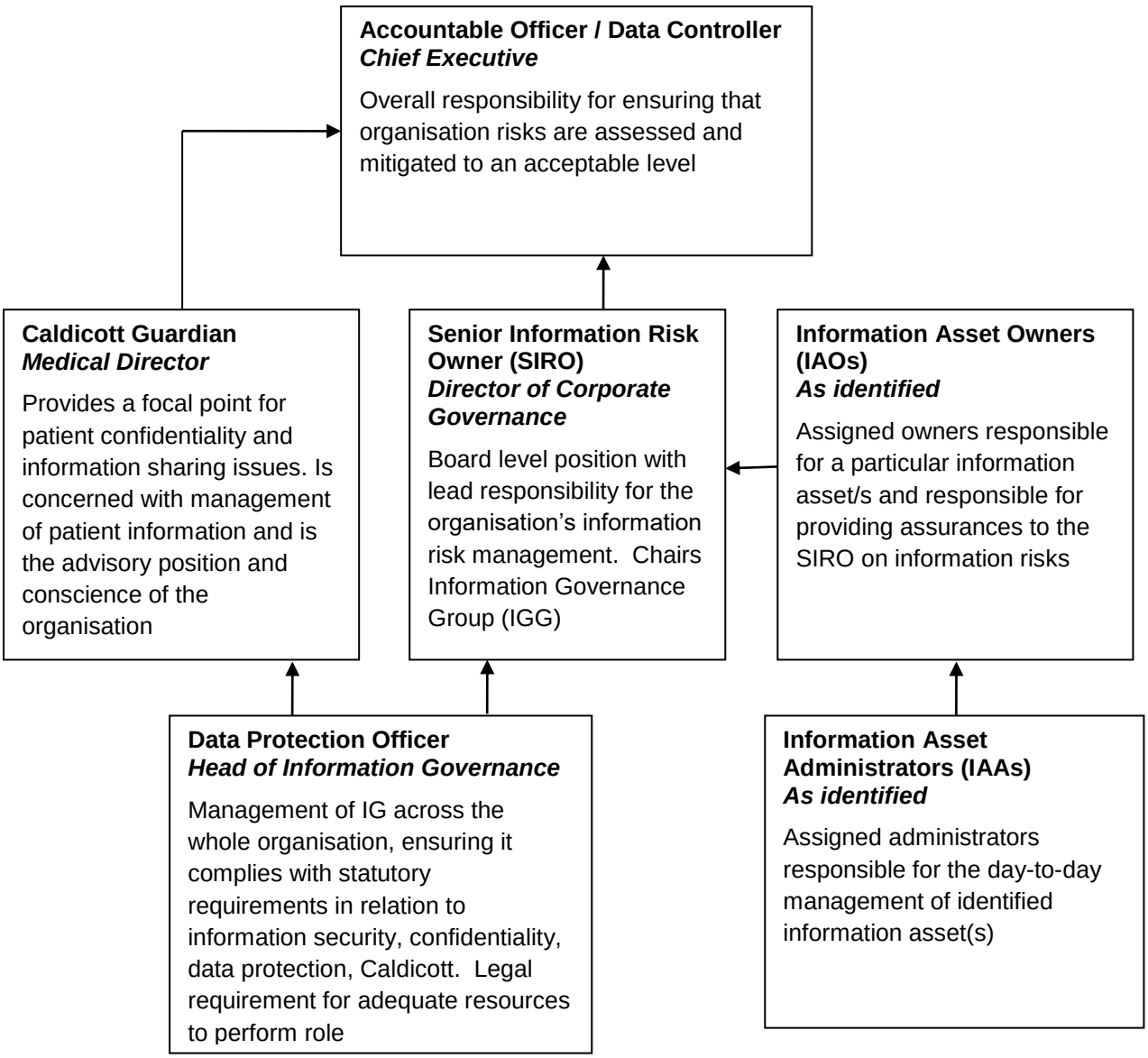
7. CONCLUSION

Implementation of this IG Framework will ensure that the Health Board and its staff handle and manage information in a consistent way. This will ensure:

- Compliance with the law and professional standards
- All information risks within the Health Board are effectively managed
- Improvements in information handling and sharing activities
- Reduction in number of IG incidents and complaints
- The Health Board has the highest standards with regards to safeguarding all personal data
- Increased service user and Regulator confidence in the NHS, the Health Board and its staff
- Implementation of Welsh Government advice and guidance
- Clarification of staff roles and responsibilities
- Contractual arrangements with other organisations are fit for purpose with regards to data protection legislation compliance
- Greater IG mandatory training compliance
- Year on year improvement.

Appendix 1

INFORMATION GOVERNANCE ROLES AND ACCOUNTABILITY CHAIN



Appendix 2

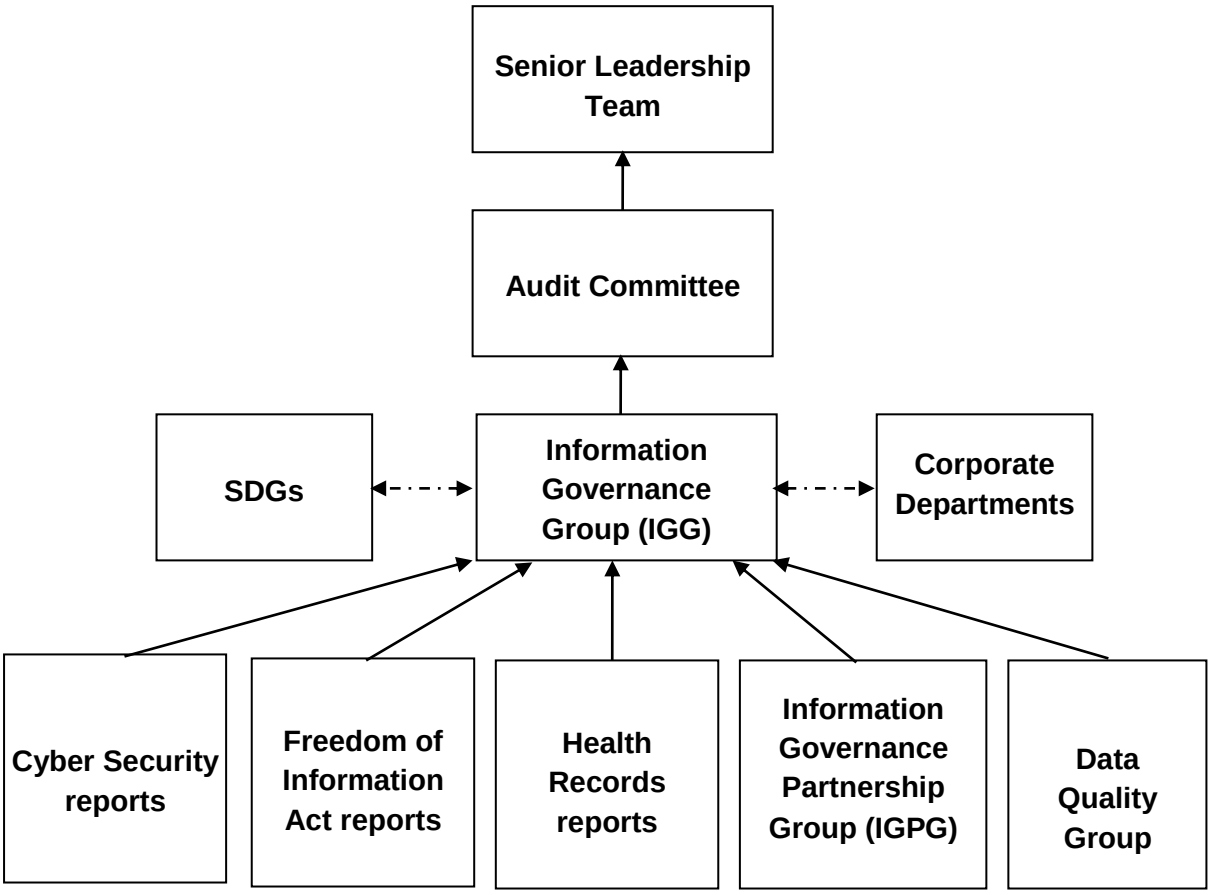
INFORMATION GOVERNANCE ASSURANCE FRAMEWORK

This IG Framework has been based upon the legal and other drivers as detailed below:

IG Theme	IG Assurance Requirement	Assurance Source
Governance	Strategy and Policy	IG Framework Implementation Plan Position report against status of IG Policies
	Quality of data and information	Performance reporting to the Board
	Complaints, incidents and learning	IG Incidents and complaints summary and associated learning
	Risks	IG Risks held on local registers, including audit recommendations
	Departmental audits	Overview of audits planned and outstanding recommendations
Statutory Obligations	Freedom of Information Act 2000	FOIA Annual Report Key Performance Indicators FOIA Policy and Procedures
	Data Protection Act 2018	SIRO Report Key Performance Indicators IGG Reports IG Policy and Procedures Information Security Policy
	Access to Health Records Act 1990	Health Records Policies and Procedures Key Performance Indicators
National Standards	IG Toolkit	Self assessment and summary report
	Welsh Code of Confidentiality	IG Policy Mandatory training uptake
	Records management standards	Health Records Policy Mandatory training uptake Incident reporting
	Information Security Standards	Information Security Policy Mandatory training uptake Incident reporting IG Annual Report ISO27001/2
Organisational Performance	Workforce training	Mandatory training uptake
	Performance Indicators	KPI reports to IGG

Appendix 3

INFORMATION GOVERNANCE STRUCTURE WITHIN SBU



KEY

Responsible to

IGG Lead responsible for

Appendix 4

INFORMATION GOVERNANCE WORK PLAN 2020-2022

This is available on request from the Information Governance Department by emailing sbu.confidentialityissues@wales.nhs.uk