INFORMATION GOVERNANCE ASSURANCE MANAGEMENT FRAMEWORK

Summary

This policy sets out an overarching framework for the strategic Information Governance agenda. In particular, this framework looks at the operational and management structures, roles, responsibilities, systems, policies and audit controls that the Trust intends to establish to ensure such issues are appropriately addressed throughout the organisation. This structured approach relies upon the identification of information assets and assigning ‘ownership’ of assets to senior accountable staff.

The Framework document includes standards set out to support the delivery of the NHS Operating Framework for the NHS, NHS Informatics Planning and the NHS Care Record Guarantee. These standards are reflected in the NHS Information Governance Toolkit.

CONTENTS

Section		**Page**
1	Introduction	2
2	General Principles	2
3	The Information Governance Toolkit	3
4	The NHS Connecting for Health Information Governance Statement of Compliance	3
5	Essential Standards of Quality and Safety	4
6	Information Governance Training	4
7	Confidentiality Code of Conduct	5
8	Communications Plan	5
9	Roles and responsibilities	5
10	Information Risk	7
11	Information Security Incident Management	7
12	Security of Information	8
13	Privacy Impact Assessments	8
14	Information Asset Register	8
15	Freedom of Information	9
16	Confidentiality of Patient Data	9
17	Records Management	10
18	Third Party Contracts	10
19	Consent to share information	11
20	Information Sharing Agreements	11
21	Transfers of Personal Information outside the UK	11
22	Information Quality Assurance	12
23	Information Governance Toolkit Requirements	12
Annex A	Information Risk – Roles and Responsibilities	15
Annex B	Key Responsibilities of the SIRO	16
Annex C	Key Responsibilities of IAO	17
Annex D	Key Responsibilities of IAA	19
Annex E	Information Risk Assessment Form	20
Annex F	IG Policy Framework	23

1. Introduction

Information Governance is the framework of law and best practice that regulates the manner in which information (including information relating to and identifying individuals) is managed, i.e. obtained, handled, used and disclosed.

The Information Governance Assurance Framework (the “Framework”) is a national framework of standards that bring together all statutory, mandatory and best practice requirements concerning information management. The standards are set out in the Information Governance Toolkit (IGT) as a road map enabling the Trust to plan and implement standards of practice and to measure and report compliance on an annual basis.

The Trust’s performance against these standards is mandated by and reported to the Department of Health and forms a part of the assurance processes associated with Care Quality Commission, Monitor and the NHS Litigation Authority (NHSLA) risk management standards.

Information is an important asset to the Trust whereby Information Governance is a key corporate-wide agenda that cannot be successful if it is seen in isolation, particularly in relation to the Integrated Governance agenda.

2. General principles

“Information Governance” is an umbrella term for a collection of distinct but overlapping disciplines. Information Governance is about the way in which the Trust handles its information, particularly personal data. The Trust relies on good quality information being available at the point of need in order to provide a high quality service. Staff rely on the quality of data they use to make decisions about patient care and treatment, and the way in which we use resources and run Trust business. It is important for staff to understand their own responsibility for recording information to a consistently high standard and for keeping it secure and confidential. Public confidence in our ability to handle their data responsibly and efficiently is based on a good reputation for keeping their data safe.

Reference to “information governance” in this policy shall also mean reference to the following areas:

- Access to information (Freedom of Information Act 2000 and Subject Access Requests)
- Confidentiality and Data Protection Act 1998
- Information security assurance
- Information quality assurance
- Records Management

Information Governance provides a consistent way for employees to deal with the many different information handling requirements. Listed below are the Legislation, Standards and Guidelines applicable to this Framework:

- Access to Health Records Act 1990
- BS ISO/IEC 17799:2005; BS ISO/IEC 27001:2005;
- BS7799-2:2005

- Data Protection Act 1998
- Confidentiality: NHS Code of Practice
- Freedom of Information Act 2000
- The Common Law Duty of Confidentiality
- The Caldicott Guardian Manual 2010
- The NHS Information Governance Toolkit
- Records Management: NHS Code of Practice
- Information Security Management: NHS Code of Practice
- NHS Operating Framework
- NHS Informatics Planning
- NHS Information Governance: Guidance on legal and professional obligations

3. The Information Governance Toolkit

The annual information governance assessment is measured via an assessment process of compliance against the standards set out in the NHS Information Governance Toolkit and assured by Internal Audit.

From 2010/11 onwards, the organisation is required to submit three Information governance performance reports to the Health and Social Care Information Centre (HSCIC), which can be tracked by Commissioners and other monitoring bodies. The reporting deadlines are as follows:

- Baseline assessment (31st July)
- Performance update (31st October)
- Final submission (31st March)

The final performance assessment is submitted to the HSCIC on the 31st March each year and shared with the Care Quality Commission, the Audit Commission, Monitor and the National Information Governance Board. The results are also published on the Connecting for Health website and made available to the general public.

4. The NHS Connecting for Health Information Governance Statement of Compliance

All organisations wishing to access and use NHS systems and services, including the N3 network, must meet the terms and conditions in the Information Governance Statement of Compliance (IGSoC). The IGSoC is the agreement between NHS CFH and Approved Service Recipients that sets the information governance policy and terms of conditions for use of NHS services.

The IGSoC contains a number of obligations which aim to preserve the integrity of these services, which requires:

- No patient identifiable data or other sensitive data is stored or processed offshore, where the location is deemed non-compliant with the NHS Offshore Policy
- The right of audit by HSCIC or nominated third parties
- Change Control Notification procedures and approval processes
- Organisations to achieve or be working towards ISO27001
- Organisations report security events and incidents

Since the NHS Operating Framework for 2010/11, organisations are required to achieve level 2 performance against all 45 requirements identified in the Information Governance Toolkit.

The Trust's information governance performance will be measured through the baseline, improvement and annual IG Toolkit reports and reported to the Information Governance Committee.

5. The Fundamental Standards

The Care Quality Commission inspects and assesses organisations against the fundamental standards using five key questions;

- are they safe?
- are they effective?
- are they caring?
- are they responsive to people's needs?
- are they well led?

The Care Quality Commission cross-check the Trust's Information Governance Toolkit submission as part of assurance that the Trust is meeting the fundamental standards.

The Trust must have effective governance and systems to check on the quality and safety of care. These must help the service improve and reduce any risks to patient's health, safety and welfare. For example the standards require the Trust to ensure that medical records are accurate, fit for purpose, held securely and remain confidential.

6. Information Governance Training

Fundamental to the success of delivering the Framework is developing an Information Governance culture within the Trust. Awareness and training needs to be provided to all Trust staff who utilise information in their day-to-day work to promote this culture.

All staff should receive annual basic information governance training appropriate to their role through the online NHS Information Governance Training Tool which is also now available via the Marsden E-Learning Hub. An icon is on every computer to access the E-Learning Hub so staff can undertake the training.

Information Governance Training is incorporated into the Trust's Mandatory Training programme. It is a **mandatory** requirement for all staff at the Royal Marsden without exception to undertake annual Information Governance training. This includes staff on temporary contracts of more than 3 months, secondments, agency staff, students and volunteers.

Different levels of training will be delivered:

- All staff to receive Information Governance awareness training as part of their corporate induction programme.

- Practitioner level for those engaged in, or intends to take on IG specialist roles e.g. SIRO (Senior Information Risk Owner) and Information Asset Owners to complete the module 'NHS Information Risk Management for SIROs and IAOs'.
- Caldicott Guardian completes external training if new in post or the online module 'The Caldicott Guardian in the NHS and Social Care' when it becomes available.

7. Confidentiality Code of Conduct

All 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. Failure to maintain confidentiality may lead to disciplinary action, including dismissal.

8. Communications Plan

The Trust will develop and maintain a communications plan to ensure that 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 when consent is required to use their data for non-healthcare purposes.

9. Information Risk Roles and Responsibilities (See Annex A)

The Trust Board

The Board is responsible for ensuring that the information governance functions are addressed.

The Chief Executive

The Chief Executive as the Accountable Officer for the Trust has overall accountability and responsibility for Information Governance in the Trust and is required to provide assurance through the Statement of Internal Control that all risks to the Trust, including those relating to information, are effectively managed and mitigated.

The Senior Information Risk Owner

The Chief Operating Officer at the Trust is the Senior Information Risk Owner ("the SIRO"). The SIRO has overall responsibility for managing information risk across the Trust and is the owner of the Trust's Information Asset Register. The SIRO is a member of the Executive Board Team and Trust Board and provides written advice to the Accounting Officer on the content of the Statement of Internal Control in regard to information risk. See **Annex B** for list of key responsibilities.

The SIRO is responsible to the Board for ensuring that all Information risks are recorded and mitigated where applicable. The SIRO is responsible for ensuring that all record management issues (including electronic media) are managed in accordance with this policy.

The SIRO will own the Trust's overall information risk assessment process, test its outcome, and ensure it is used. The SIRO will be responsible for how the Trust implements NHS Information Governance risk management in its own services and activities and those of its delivery partners, and how compliance will be monitored. The SIRO will ensure that information asset risk reviews are completed every quarter. Based on the information risk assessment the SIRO will evaluate what information risks there are to the Trust and its business partners through its delivery chain, and ensures that they are addressed, and that they inform investment decisions including the risk considerations of outsourcing.

The SIRO is supported by Information Asset Owners (the "IAOs"), the Trust's Caldicott Guardian and members of the Information Governance Committee, although ownership of Information Risk and the information risk assessment process remains with the SIRO.

Information Asset Owner

Information Asset Owners (IAOs) are directly accountable to the SIRO and must provide assurance that information risk is being managed effectively in respect of the information assets that they 'own'. IAOs will also lead and help foster with their respective Directorates a culture that values, protects and uses information.

IAOs must be a member of staff who is senior enough to make decisions concerning the asset at the highest level. At the Trust IAOs are members of the Executive Board who are involved in running the Trust. Their role is also to understand and assess risks to the information assets they 'own' and to provide assurance to the SIRO on the security and use of those assets. They will ensure that all threats, vulnerabilities and impacts are properly assessed and included in the Trust's Information Asset Register.

The owner can assign day to day responsibility for each information asset to an administrator or manager known as an Information Asset Administrator, which must be formalised in job descriptions.

The SIRO is responsible for the appointment and management (in terms of information assets) of the IAOs.

See **Annex C** for list of key responsibilities Information Asset Administrator

The IAOs (in consultation with the SIRO) are responsible for appointing Information Asset Administrators (IAAs). It is at the IAOs discretion how many IAAs are appointed to support them in their role. Information Asset Administrators are operational staff with day to day responsibility for managing risks to their information assets. They will support IAOs by ensuring that policies and procedures are followed, recognise actual or potential security incidents, consult their IAO on incident management, ensure that privacy impact assessments are completed and ensure that information asset registers are accurate and up to date.

See Annex D for list of key responsibilities.

Caldicott Guardian

The Chief Nurse is the Caldicott Guardian and the “conscience” of the Trust, providing a focal point for patient confidentiality and information sharing issues and advising on the options for lawful and ethical processing of information as required.

Information Governance Committee (IGC)

The IGC has responsibility for overseeing the implementation of this Framework document, the Information Governance Policy, the annual information governance toolkit assessment and the annual Information Governance improvement plan. This Committee also reviews and approves all IG-related policies and procedures.

The IGC reports to the Integrated Governance and Risk Management Committee (IGRM).

10. Information Risk

The Trust will establish clear lines of accountability for information risk management that lead directly to the Board through the SIRO and the appointment of Information Asset Owners’ (IAO) and Information Asset Administrators who will collectively be responsible for the maintenance of a Trust wide Information Asset Register.

The IAOs and SIRO will be accountable to the Accountable Officer, the Chief Executive for the management and mitigation of information risks and will provide assurance to that effect for the Annual Report and Statement of Internal Control.

The IAO will ensure that information risk assessments are performed at least once each quarter on all information assets where they have been assigned ‘ownership’ of. They will ensure that any significant risks are included in a quarterly assessment to the Trust’s SIRO.

At least once a year, each of the Trust’s IAOs will carry out a risk assessment to examine forthcoming potential changes in services, technology and threats.

See Information Management Risk Assessment Template at Annex E. Risks that score 9 and above will be entered onto the appropriate risk register as documented in the Trust Risk Management Policy.

The SIRO and Information Governance Committee will be made aware of all information risk assessments and approve identified risk mitigation plans.

On an annual basis the Trust’s IAOs will provide assurances to the Trust’s SIRO on the security and use of assets they ‘own’.

11. Information Security Incident Management

The Trust’s SIRO and Caldicott Guardian via the relevant IAO must be informed immediately of all information security incidents involving the unauthorised disclosure of patient information for consideration of any necessary actions.

A key function of the Information Governance Committee is to monitor and review untoward occurrences and incidents relating to Information Governance and to ensure that effective remedial and preventative action is taken. Reports of such incidents will be distributed to the Information Governance Committee for consideration.
Information incident reporting will be in line with both organisations overall incident reporting processes. Please refer to the Trust policy 'Accident/Incident & Patient Safety Incident Reporting Policy Including Serious Incidents'.

12. Security of Information

The Trust will protect personal data held in its information systems through compliance with the Department of Health Information Security Code of Practice an associated standard of ISO/IEC 27002:2005.

The Trust will ensure that personal data is protected by encryption in accordance with Department of Health directives. Please refer to the Information Management and Technology Security Policy.

13. Privacy Impact Assessments

The impact of any proposed changes to the Trust's processes and/or information assets need to be assessed in accordance with the Trust's Privacy Impact Assessment Policy, to ensure that the confidentiality, integrity and accessibility of personal information are maintained.

The Information Governance Committee should be consulted during the design phase of any new service, process or information asset so that the Committee can decide if a privacy impact assessment is required for a particular project or plan.

14. Information Asset Register

All assets should be clearly identified and the Information Asset Register.

It will be the responsibility of each IAO to identify what information assets are held within their area of responsibility, and to ensure this is documented in their Directorate's Information Asset Register which will form part of a Trust wide Register owned by the Trust's SIRO.

The Information Asset Register should include all information necessary in order to recover from a disaster, including type of asset, format, location, backup information, license information, and a business value. The register should not duplicate other inventories unnecessarily, but it should be ensured that the content is aligned. In addition, ownership should be agreed and documented for each of the assets. Based on the importance of the asset, its business value and its security classification, levels of protection commensurate with the importance of the assets should be identified as should details of risk assessor, risk assessment frequency, risk assessment rating and date of last risk assessment.

There are many types of assets, including:

- information: databases and data files, contracts and agreements, system documentation, research information, user manuals, training material, operational or support procedures, business continuity plans, fallback arrangements, audit trails, and archived information;
- software assets: application software, system software, development tools, and utilities;
- physical assets: computer equipment, communications equipment, removable media, and other equipment;
- services: computing and communications services, general utilities, e.g. heating, lighting, power, and air-conditioning;
- people, and their qualifications, skills, and experience;
- intangibles, such as reputation and image of the organisation.

All information and assets associated with information processing facilities should be owned by a designated part of the organisation, for example a Trust Directorate. **Priority must be given to information assets that comprise or contain personal information about patients or staff.**

The IAO should be responsible for ensuring that information and assets associated with information processing facilities are appropriately identified and classified; defining and periodically reviewing access restrictions, classifications, and business continuity arrangements taking into account applicable access control policies.

Routine tasks may be delegated, e.g. to a custodian looking after the asset on a daily basis (i.e. an information assets administrator (IAA), but the responsibility remains with the owner.

In complex information systems it may be useful to designate groups of assets, which act together to provide a particular function as ‘services’. In this case the service owner is responsible for the delivery of the service, including the functioning of the assets, which provide it.

15. Freedom of Information

The Trust will ensure compliance with the Freedom of Information Act 2000 and associated Lord Chancellor’s Codes of Practice under sections 45 and 46. This is set out in the Trust’s Freedom of Information Policy.

16. Confidentiality of Personal Data

The Trust, as the legal person and Data Controller for the proposes of the Data Protection Act will ensure that all personal data it holds is controlled and managed in accordance with the terms of the Data Protection Act 1998 principles, the Department of Health Confidentiality: NHS Code of Practice European Convention of Human Rights (Article 8) (Human Rights Act 1998) and common law. This is set out in the Trust’s Confidentiality and the Data Protection Act Policy, Records Management Strategy and Access to Health Records Policy.

17. Records Management

The Trust is committed to a systematic and planned approach to the Management of records within the organisation, from their creation to their ultimate disposal. The Trust will ensure that it controls the quality and quantity of the information that it generates, can maintain that information in an effective manner, and can dispose of the information efficiently when it is no longer required. The Trust will ensure that Health Records are managed in accordance with the Department of Health Records Management: NHS Code of Practice. This is set out in the Trust's Management of Medical Records – Policy and Procedure.

To ensure that the Trust maintains the highest standards in the quality of its clinical records an annual audit of clinical records will be undertaken.

18. Third Party Contracts

It is not unusual to have third parties gaining access to the Trusts information assets, e.g. computers, telephones, paper records etc. The third parties would include temporary agency staff, consultants, IT support staff, cleaning staff, catering staff and security guards. It is possible that as a result of access to information assets, third party staff may have significant access to patient or staff personal data. This situation therefore clearly has information governance risk implications such as data being used inappropriately.

Suitable clauses should be included when negotiating and completing contracts with third parties who have access to or process personal information on behalf of the Trust. All contractors or support organisations with access to the Trust's information assets should be clearly identified and appropriate information governance clauses included in their contracts. The terms and conditions of a contract must ensure that failure to deliver any aspect of information governance assurances will be at the third parties risk.

Attention should also be paid to the possible use of sub-contractors by the third party to provide services in order to undertake the contract.

The SIRO and IAOs must take all reasonable steps to ensure that that contractors and support organisations to whom personal information is disclosed comply with their contractual obligations to keep personal information secure and confidential.

Risk Assessments

Directorates and IAOs should ensure that a risk assessment has been carried out prior to any agreement being made with a third party to evaluate any potential threats to networks, systems and locations from third party operatives.

The ways in which third parties gain access, will help determine how extensive the risk assessment needs to be. For example, a risk assessment for cleaning contractors will be different to that carried out for a contractor connecting to the network. Temporary access will also see different considerations to long-term access. **An Information Risk Assessment template can be located at Annex E.**

Review of contracts

IAOs should ensure that all existing contracts are monitored and reviewed annually to ensure that IG controls are being adhered to and to resolve problems or unforeseen events.

A register of all third party contracts should be maintained by the Trust.

19. Consent to share information

It is generally accepted that consent to disclose or to use patient information can be implied where the purpose is directly concerned with the individuals care or with the quality assurance of that care.

Where the Trust wishes to use or disclose confidential personal information for a purpose unrelated to care, consent cannot be implied. In most cases, patients should be asked for their explicit consent for information to be shared with non-care organisations such as government departments, the police and voluntary services. There are exceptions where it is believed that the reasons for disclosure are so important (sometimes termed a public interest justification or defence) that they override the obligation of confidentiality (e.g. to prevent someone from being seriously harmed).

20. Information Sharing Agreements

Sharing information about an individual between partner agencies is vital to the provision of co-ordinated and seamless services. The need for shared information standards and robust information security to support the implementation of joint working arrangements is recognised.

Information sharing protocols can be a useful way of providing a transparent and level playing field for organisations that need to exchange information. They can provide assurance in respect of the standards that each party to an agreement will adopt. However, they do not in themselves provide a lawful basis for sharing confidential information. That can only result from effectively informing the person whose information it is about the possibility of sharing and the choices they have to limit sharing. If the individual says no to sharing, then confidential information may only be shared in exceptional circumstances.

Routine information sharing continues to require information sharing protocols in order to ensure that the ‘rules’ are clearly understood and that the requirements of law and guidance are being met. Information sharing protocols are not required where the sharing is for an ad hoc request for information.

21. Transfers of Personal Information outside the UK

The Data Protection Act governs transfers of personal information and requires that personal information is not transferred to countries outside of the European Economic Area unless that country has an adequate level of protection for the information and for the rights of individuals. The European Economic Area (EEA) is made up of the EU member states plus the European Free Trade Association (EFTA) countries of Iceland, Liechtenstein and Norway.

All transfers of personal data outside the EEA must be for a lawful and justified purpose and the Trust's Caldicott Guardian must be informed of such transfers. A log shall be maintained of such transfers.

Personal Information should only be transferred outside the EEA if the individual's consent, which should be explicit, has been obtained or following a risk assessment the Caldicott Guardian is satisfied that there is an adequate level of protection in place. In certain circumstances a contract containing standard EU approved clauses as providing adequate protection to transfer individuals' personal information may be necessary.

22. Information Quality Assurance

The quality of information acquired and used within the Trust is a key component to its effective use and management. As such, managers will be expected to take ownership of, and seek to improve, the quality of data collected and held within their services.

The Trust will promote data quality through the use of policies and procedures including the Medical Records Management Policies and Data Quality Policy, and associated statutory professional requirements to ensure that wherever possible, information quality will be assured at the point of collection.

23. Information Governance Toolkit Requirements

This Framework is intended to comply with the following Information Governance toolkit requirements:

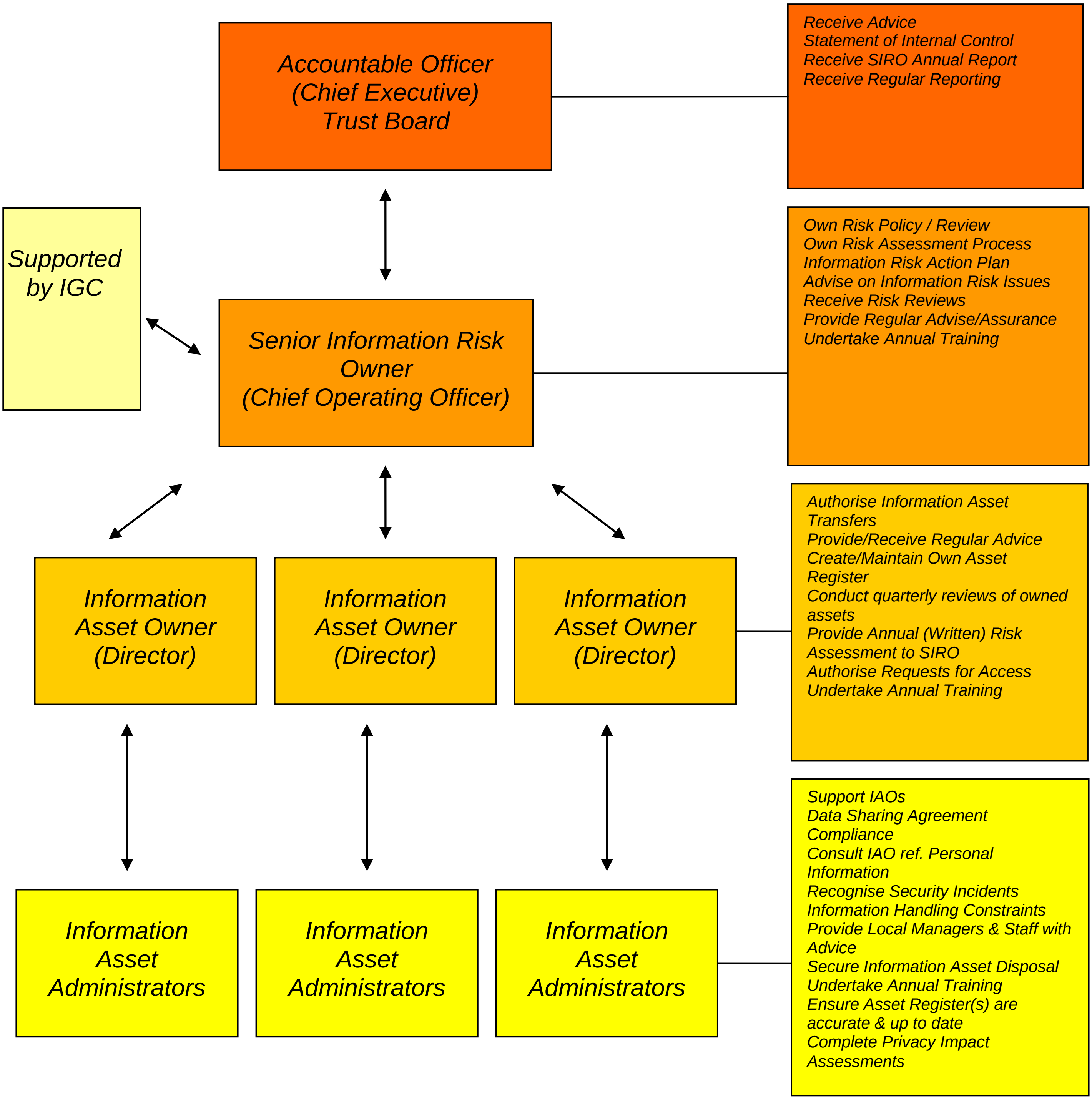
14-101	There is an adequate Information Governance Management Framework to support the current and evolving Information Governance agenda
14-105	There are approved and comprehensive Information Governance Policies with associated strategies and/or improvement plans
14-110	Formal contractual arrangements that include compliance with information governance requirements, are in place with all contractors and support organisations
14-111	Employment contracts which include compliance with information governance standards are in place for all individuals carrying out work on behalf of the organisation
14-112	Information Governance awareness and mandatory training procedures are in place and all staff are appropriately trained
14-140	Responsibility for Information Governance has been assigned to an appropriate member, or members, of staff
14-200	The Information Governance agenda is supported by adequate confidentiality and data protection skills, knowledge and experience which meet the organisation's assessed needs
14-201	The organisation ensures that arrangements are in place to support and promote information sharing for coordinated and integrated care, and staff are provided with clear guidance on sharing information for care in an effective, secure and safe manner
14-202	Confidential personal information is only shared and used in a lawful manner and objections to the disclosure or use of this information are appropriately respected

14-203	Patients, service users and the public understand how personal information is used and shared for both direct and non-direct care, and are fully informed of their rights in relation to such use
14-205	There are appropriate procedures for recognising and responding to individuals' requests for access to their personal data
14-206	Staff access to confidential personal information is monitored and audited. Where care records are held electronically, audit trail details about access to a record can be made available to the individual concerned on request
14-207	Where required, protocols governing the routine sharing of personal information have been agreed with other organisations
14-209	All person identifiable data processed outside of the UK complies with the Data Protection Act 1998 and Department of Health guidelines
14-210	All new processes, services, information systems, and other relevant information assets are developed and implemented in a secure and structured manner, and comply with IG security accreditation, information quality and confidentiality and data protection requirements
14-300	The Information Governance agenda is supported by adequate information security skills, knowledge and experience which meet the organisation's assessed needs
14-301	A formal information security risk assessment and management programme for key Information Assets has been documented, implemented and reviewed
14-302	There are documented information security incident / event reporting and management procedures that are accessible to all staff
14-303	There are established business processes and procedures that satisfy the organisation's obligations as a Registration Authority
14-304	Monitoring and enforcement processes are in place to ensure NHS national application Smartcard users comply with the terms and conditions of use
14-305	Operating and application information systems (under the organisation's control) support appropriate access control functionality and documented and managed access rights are in place for all users of these systems
14-307	An effectively supported Senior Information Risk Owner takes ownership of the organisation's information risk policy and information risk management strategy
14-308	All transfers of hardcopy and digital person identifiable and sensitive information have been identified, mapped and risk assessed; technical and organisational measures adequately secure these transfers
14-309	Business continuity plans are up to date and tested for all critical information assets (data processing facilities, communications services and data) and service - specific measures are in place
14-310	Procedures are in place to prevent information processing being interrupted or disrupted through equipment failure, environmental hazard or human error
14-311	Information Assets with computer components are capable of the rapid detection, isolation and removal of malicious code and unauthorised mobile code
14-313	Policy and procedures are in place to ensure that Information Communication Technology (ICT) networks operate securely

14-314	Policy and procedures ensure that mobile computing and teleworking are secure
14-323	All information assets that hold, or are, personal data are protected by appropriate organisational and technical measures
14-324	The confidentiality of service user information is protected through use of pseudonymisation and anonymisation techniques where appropriate
14-400	The Information Governance agenda is supported by adequate information quality and records management skills, knowledge and experience
14-401	There is consistent and comprehensive use of the NHS Number in line with National Patient Safety Agency requirements
14-402	Procedures are in place to ensure the accuracy of service user information on all systems and/or records that support the provision of care
14-404	A multi-professional audit of clinical records across all specialties has been undertaken
14-406	Procedures are in place for monitoring the availability of paper health/care records and tracing missing records
14-501	National data definitions, standards, values and data quality checks are incorporated within key systems and local documentation is updated as standards develop
14-502	External data quality reports are used for monitoring and improving data quality
14-504	Documented procedures are in place for using both local and national benchmarking to identify data quality issues and analyse trends in information over time, ensuring that large changes are investigated and explained
14-505	An audit of clinical coding, based on national standards, has been undertaken by a Clinical Classifications Service (CCS) approved clinical coding auditor within the last 12 months
14-506	A documented procedure and a regular audit cycle for accuracy checks on service user data is in place
14-507	The secondary uses data quality assurance checks have been completed
14-508	Clinical/care staff are involved in quality checking information derived from the recording of clinical/care activity
14-510	Training programmes for clinical coding staff entering coded clinical data are comprehensive and conform to national clinical coding standards
14-601	Documented and implemented procedures are in place for the effective management of corporate records
14-603	Documented and publicly available procedures are in place to ensure compliance with the Freedom of Information Act 2000
14-604	As part of the information lifecycle management strategy, an audit of corporate records has been undertaken

Annex A

Information Risk – Roles and Responsibilities


Accountable Officer
(Chief Executive)
Trust Board
Supported by IGC
Senior Information Risk Owner
(Chief Operating Officer)
Information Asset Owner (Director)
Information Asset Owner (Director)
Information Asset Owner (Director)
Information Asset Administrators
Information Asset Administrators
Information Asset Administrators

Receive Advice
Statement of Internal Control
Receive SIRO Annual Report
Receive Regular Reporting

Own Risk Policy / Review
Own Risk Assessment Process
Information Risk Action Plan
Advise on Information Risk Issues
Receive Risk Reviews
Provide Regular Advise/Assurance
Undertake Annual Training

Authorise Information Asset Transfers
Provide/Receive Regular Advice
Create/Maintain Own Asset Register
Conduct quarterly reviews of owned assets
Provide Annual (Written) Risk Assessment to SIRO
Authorise Requests for Access
Undertake Annual Training

Support IAOs
Data Sharing Agreement Compliance
Consult IAO ref. Personal Information
Recognise Security Incidents
Information Handling Constraints
Provide Local Managers & Staff with Advice
Secure Information Asset Disposal
Undertake Annual Training
Ensure Asset Register(s) are accurate & up to date
Complete Privacy Impact Assessments

Annex B

Key Responsibilities of the SIRO

- To oversee the development of an Information Risk Policy, and a Strategy for implementing the policy within the existing Information Governance Framework.

- To take ownership of the risk assessment process for information risk, including review of the annual information risk assessment to support and inform the Statement of Internal Control.

- To review and agree an action plan in respect of identified information risks.

- To ensure that the Trust's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff.

- To provide a focal point for the resolution and/or discussion of information risk issues.

- To ensure the Board is adequately briefed on information risk issues.

- To advise the Chief Executive and the Trust Board on information risk management strategies and provide periodic reports and briefings on Program progress.

Annex C

Key Responsibilities of the IAO

To understand and address risks to the information assets they 'own' and provide assurance to the SIRO on the security and use of these assets (understands the Organisation's plans to achieve and monitor the right NHS IG culture, across the Organisation and with its business partners and to take visible steps to support and participate in that plan (including completing own training).

IAO's will take appropriate actions to:

- Know what information the Asset holds, and understands the nature and justification of information flows to and from the asset (approves and minimises information transfers while achieving business purposes; approves arrangements so that information put onto portable or removable media like laptops is minimised and are effectively protected to NHS IG standards.
- Know who has access and why, and ensure their use is monitored and compliant with policy (checks that access provided is the minimum necessary to satisfy business objectives; receives records of checks on use and assures self that effective checking is conducted regularly).
- Ensure the confidentiality, integrity, and availability of all information that their system creates, receives, maintains, or transmits and protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
- Conduct Privacy Impact Assessments for all new projects in line with the Trust's Privacy Impact Assessment Policy.
- Participate in an Annual Information Risk Assessment.
- Understand and address risks to the asset, and provide assurance to the SIRO (makes the case where necessary for new investment or action to secure 'owned' assets; provides an annual written risk assessment to the SIRO for all assets 'owned' by them).
- Ensure that information risk assessments are reviewed **(See Annex E)** at least once every quarter on all information assets where they have been assigned 'ownership' and where:
  - New systems, applications, facilities etc. is introduced that may impact the assurance of Trust Information or Information Systems.
  - Before enhancements, upgrades, and conversions associated with critical systems or applications.
  - Ensure that risks 9 and above follow the Trust process for inclusion on the Trust's risk register.
- IAOs shall submit the risk assessment results and associated mitigation plans to the SIRO for review. Mitigation plans shall include specific actions with expected completion dates, as well as an account of residual risks.
- Compile their Information Asset Register.

- Ensure the asset is fully used for the benefit of the organisation and its patients, including responding to requests for access from others (considers whether better use of the information is possible or where information is no longer required; receives, logs and controls requests from others for access; ensures decisions on access are taken in accordance with NHS IG standards of good practice and the policy of the organisation.
- Approve and oversee the disposal mechanisms for information of the asset when no longer needed).

Annex D

Key Responsibilities of the IAA

Information Asset Administrators will provide support to their IAOs to ensure that policies and procedures are followed and to recognise potential or actual security incidents. They will consult their IAOs on incident management to ensure that information asset registers are accurate and maintained up to date.

Ensuring compliance with data sharing agreements within the local area and that information handling procedures are fit for purpose and are properly applied.

Under the direction of their IAO, they will ensure that personal information is not unlawfully exploited and they will, upon recognising new information handling requirements (e.g. a new type of information arises) that the relevant IAO is consulted over appropriate procedures. They will consult with the IAOs regarding any potential or actual security incidents.

Reporting to the relevant IAO on current state of local information handling and ensure that local information handling constraints (e.g. limits on who can have access to the assets) are applied, referring any difficulties to the relevant IAO. They will act as first port of call for local managers and staff seeking advice on the handling of information.

Under the direction of their IAO, they will ensure that information is securely destroyed when there is no further requirement for it.

Annex E

Information Risk Assessment Form

Information Asset Owner:	**Department/Section:**	**Date:**

Information Asset:

What is the threat? (Please describe the threat of something damaging the confidentiality, integrity or availability of information)

Examples of information asset threats may include:
Technical risks**: loss of essential service, technical failures, unauthorised access (inadequate password management), Data loss /corruption (disc error reports, lack of patching schedule)* ***Physical Risks: *Physical damage to asset, Unrestricted access to office, Security of laptops/removable media, Access to printouts,* ***Administrative Risks****; Inappropriate use of equipment (lack of policies), lack of user training, inaccurate management information*
Service Provision Risks: *Corruption /inaccuracy of patient record, Failure to update patient records*

What are the consequences?

Examples of consequences may include:
Financial: *Negligent use / loss of patient data (inadequate security) – up to £500,000 issued by the Information Commissioner, Fine for copyright infringement, Additional cost of re-inputting data* ***Reputation****: Loss of reputation arising from a loss of patient data* ***Staff****: Lowering of staff morale/reduced quality of service*

What would be the potential severity (Consequence) of such an incident? (Circle appropriate value)

How bad?	**Insignificant**	**Minor**	**Moderate**	**Major**	**Catastrophic**
Value	1	2	3	4	5

What is the likelihood an incident will occur given the key controls and assurances in place? *(circle appropriate value)*

	Rare Exceptional occurrence	*Unlikely* Could occur at some time but unusual	*Possible* Reasonable chance of occurring	*Likely* Likely to occur, not a surprise	*Almost Certain* Is expected to occur in most circumstances.
% chance	<1%	1%	2-10%	10-50%	More than 50%
Value Awarded	1	2	3	4	5

Existing Controls:

Risks with existing controls:			
Consequence	Likelihood	Risk Score	
x		**=**	
If risks not accepted complete action plan			
Actions to minimise risk	Responsibility	Timescale	Revised Risk Score
Overall Risk Value:	Consequence	Likelihood	Risk Rating
	x		=

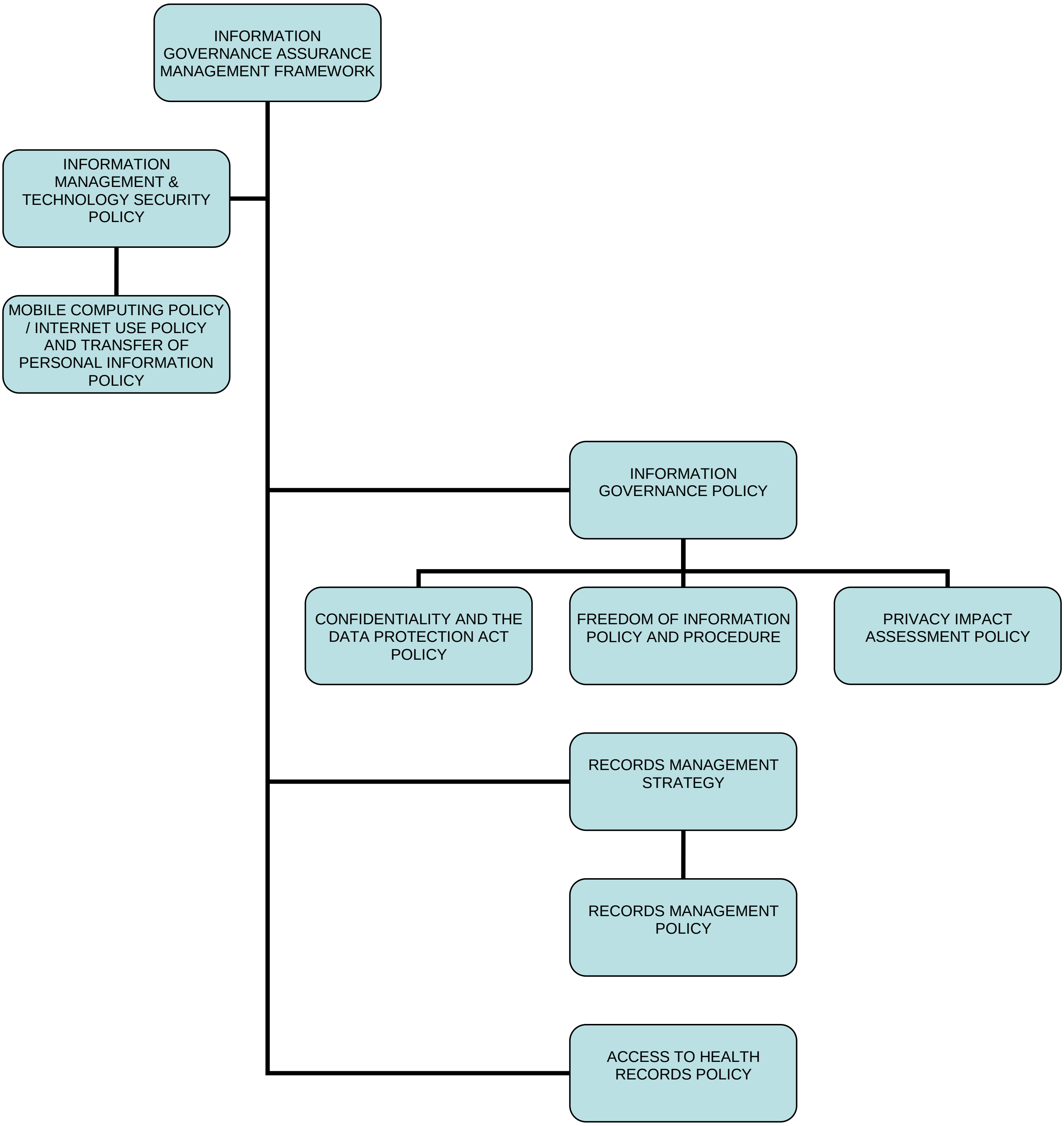
Evaluating Information Risk / Risk rating for Information Risk Assessments

A simple approach to quantifying risk is to define qualitative measures of consequences and likelihood such as the exemplars given below. This allows construction of a risk matrix which can be used as the basis of identifying acceptable and unacceptable risk. In order to prioritise actions, it is necessary to evaluate the level of risk presented by each of the identified hazards. This is done using a simple rating system (1-5). First, for each of the hazards/risks decide how likely it is to happen (Likelihood) and how serious the consequences are most likely to be (Severity) from the following guide, taking into account the measures already in place.

RISK LEVEL	ACTION AND TIME SCALE
INSIGNIFICANT **Risk value 1** Slight damage to property or equipment, Slight delay in service provision, An element of financial loss, Minor clinical incident – no immediate effect on patient safety or patient care, Potential breach of confidentiality where less than 5 people affected or risk assessed as low, e.g. files were encrypted.	No action is required to deal with trivial risks, and no documentary records need to be kept.
MINOR **Risk value 2** E.g. Slight damage to property or equipment, Slight delay in service provision, An element of financial loss, Minor clinical incident – no immediate effect on patient safety or patient care, Loss of availability to authorised users, Serious potential breach of confidentiality e.g. unencrypted clinical records lost. Up to 20 people affected.	No further preventive action is necessary, but consideration should be given to more cost-effective solutions, or improvements that impose no additional cost burden. Monitoring is required to ensure that the controls are maintained.

RISK LEVEL	ACTION AND TIME SCALE
MODERATE **Risk value 3** E.g. Significant but temporary damage to property or equipment, Failure in environmental systems (e.g. air conditioning) leaves systems unavailable, Financial loss, Temporary delay to service provision, Claim and complaint potential, Unauthorised Access to systems, Network access by unauthorised users, Serious breach of confidentiality e.g. up to 100 people affected from inadequately protected PC(s), laptop(s) and remote device(s).	Efforts should be made to reduce the risk, but the costs of prevention should be carefully measured and limited. Risk reduction measures should normally be implemented within three to six months, depending on the number of people exposed to the hazard. ***Stage 2 Assessment Required.*** Where the significant risk is associated with extremely harmful consequences, further risk assessment ***may*** be necessary to establish more precisely the likelihood of harm as a basis for determining the need for improved control measures. **Enter the Risk on to the Risk Register if the overall score is 12 and above.**
MAJOR **Risk value 4** E.g. Negative clinical outcome, Significant (permanent or long term) damage to property or equipment, Major financial loss, Long term delays in service provision, Litigation, Complaint, Media coverage, Malicious software (e.g. viruses), Serious breach of confidentiality with either particular sensitivity or up to 1000 people affected.	***Stage 2 Assessment Required.*** Work should not be *started or continued* until the risk has been reduced. Considerable resources may have to be allocated to reduce the risk. Where the risk involves work in progress, the problem should normally be remedied within one to three months, depending on the number of people exposed to hazard. **Enter the Risk on to the Risk Register if the overall score is 12 and above.**
CATASTROPHIC **Risk value 5** E.g. Major loss of public confidence, Permanent loss of service, equipment and property, Serious breach of confidentiality with potential for ID theft or over 1000 people affected.	***Stage 2 Assessment Required.*** Work should not be *started or continued* until the risk level has been reduced. Whilst the control measures selected should be cost-effective, legally there is an absolute duty to reduce the risk. This means that if it is not possible to reduce the risk even with unlimited resources, then the work must not be started. **Enter the Risk on to the Risk Register if the overall score is 12 and above.**

Annex F INFORMATION GOVERNANCE POLICY FRAMEWORK



INFORMATION GOVERNANCE ASSURANCE MANAGEMENT FRAMEWORK
INFORMATION MANAGEMENT & TECHNOLOGY SECURITY POLICY
MOBILE COMPUTING POLICY / INTERNET USE POLICY AND TRANSFER OF PERSONAL INFORMATION POLICY
INFORMATION GOVERNANCE POLICY
CONFIDENTIALITY AND THE DATA PROTECTION ACT POLICY
FREEDOM OF INFORMATION POLICY AND PROCEDURE
PRIVACY IMPACT ASSESSMENT POLICY
RECORDS MANAGEMENT STRATEGY
RECORDS MANAGEMENT POLICY
ACCESS TO HEALTH RECORDS POLICY

[End of Document - Do Not Delete]