The Tavistock and Portman NHS
NHS Foundation Trust

Information Governance Policy

Version:	4
Bodies consulted:	Caldicott Guardian, IM&T Directors
Approved by:	MT
Date Approved:	27/10/2015
Lead Manager:	Governance Manager
Responsible Director:	SIRO
Date issued:	October 2015
Review date:	September 2019

Contents

Information Governance Policy

1 Introduction

The Trust recognises the vital contribution that reliable information makes to the clinical management of individual patients and the efficient management of services and resources and recognises the key role it plays in Trust governance, service planning and performance management.

The Trust recognises that it is of paramount importance to ensure that information is efficiently managed, and that appropriate policies, procedures and management accountability provide a strong governance framework for information management, that enhance the use of information whilst taking all reasonable steps to minimise the risks of misuse and/or loss of information.

2 Purpose

The Information Governance Policy sets out the how the Trust will ensure that information is used effectively, efficiently, securely and legally.

3 Scope

This policy and associated procedures covers the use and management of information in all formats, including the security, availability, collection, processing, storage, communication and disposal of information.

The policy applies to all employees and contractors working for, or supplying services to, or for, the Trust.

An overview of IG is set out in the Information Governance Framework, see appendix 2.

4 Definitions

Term	Definition
IG Toolkit	The Information Governance Toolkit is a tool with which organisations can assess their compliance with standards set by the Health and Social Care Information Centre (HSCIC).
Secure File Transfer Protocol	A safe solution for transferring large amounts of data electronically. The data is sent down a secure, encrypted pipe to a secure destination.
Encryption	Encryption is the coding or scrambling of information so that it can only be decoded and read by someone who has the correct decoding key.

5 Policy Statements

6.1 Definition

Information Governance is to do with the way organisations 'process' or handle information. It covers personal information, relating to patients/service users and employees, and corporate information, eg financial and accounting records.

Information Governance provides a way for employees to deal consistently with the many different rules about how information is handled, including those set out in:

- The Data Protection Act 1998.
- The common law duty of confidentiality.
- The Confidentiality NHS Code of Practice.
- The NHS Care Record Guarantee for England.
- The Social Care Record Guarantee for England.
- HSCIC's IG toolkit
- The Information Security NHS Code of Practice.
- The Records Management NHS Code of Practice.
- The Freedom of Information Act 2000.

6.2 The IG Toolkit

The Information Governance Toolkit is a performance tool produced by the HSCIC. It draws together the legal rules and central guidance set out above and presents them in one place as a set of information governance requirements. The Trust is assessed on its compliance in the following areas:-

- management structures and responsibilities (e.g. assigning responsibility for carrying out the IG assessment, providing staff training, etc.);
- confidentiality and data protection; and
- information security.

Final submission assessment scores reported by organisations are used by the Care Quality Commission.

6.3 Trust Principles

The Trust recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The Trust fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about patients and staff as well as business-related sensitive information. The Trust also recognises the need to share patient information with other health organisations and other agencies in a controlled manner consistent with the interests of the patient and, in some circumstances, the public interest.

The Trust recognises that accurate, timely and relevant information is essential to deliver the highest quality health care. It is the responsibility of all staff: clinicians, managers, directors, and those with particular responsibility for clinical quality and informatics to ensure and promote the quality of care.

6.3.1 Openness

- Non-confidential information on the Trust and its services should be available to the public through a variety of media
- The Trust will establish and maintain policies to ensure compliance with the Freedom of Information Act
- Patients have right of access to information relating to their own health care, their options for treatment and their rights as patients
- The Trust will have clear procedures and arrangements for liaison with the press and broadcasting media
- The Trust will have clear procedures and arrangements for handling queries from patients and the public
- The Trust will be candid about IG data breaches

6.3.2 Legal Compliance

- The Trust regards all personal confidential information relating to patients as sensitive
- The Trust regards all personal confidential information relating to staff as sensitive, except where national policy on accountability and openness requires otherwise, or where required for fraud investigation and exempt from the Data Protection Act.
- The Trust will establish and maintain policies to ensure compliance with the Data Protection Act, Human Rights Act and the common law of confidentiality
- The Trust will establish and maintain policies for the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation (e.g. Health and Social Care Act, Crime and Disorder Act, Protection of Children Act, common law)

6.3.3 Information Security

- The Trust will establish and maintain policies for the effective and secure management of its information assets and resources
- The Trust will promote effective confidentiality and security practice to its staff through policies, procedures and training
- The Trust will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.
- No person may have access to any personal identifiable information unless they have completed IG training and passed any mandatory assessment each and every year

6.3.4 Information Quality Assurance

- The Trust will establish and maintain policies and procedures for information quality assurance (including data quality) and the effective management of records
- The Trust will undertake or commission annual assessments and audits of its information quality and records management arrangements
- Managers are expected to take ownership of, and seek to improve, the quality of information within their services
- Wherever possible, information quality should be assured at the point of collection
- Data standards will be set through clear and consistent definition of data items, in accordance with national standards.

- The Trust will promote information quality and effective records management through policies, procedures/user manuals and training.

6.3.5 Resources

Directors are responsible for implementation in their directorate; IG is seen as integral and all IG activity is 'business-as-usual' so resources are not usually specifically identified at this level. Line managers are responsible for ensuring that their staff comply with each of the Trust's policies and procedures.

The budget for IG work at corporate level shall be held by the Governance Manager.

6 Duties and responsibilities

These roles are at board level or the most senior leadership level. Whilst managers and directors are accountable to the Board of Directors, the Caldicott Guardian is distinct as it is an advisory role.

5.1 Chief Executive

The CE has ultimate responsibility for all elements of governance, be it clinical, information, or corporate. The CE has delegated the task of overseeing Information Governance to the Senior Information Risk Owner (SIRO).

5.2 Senior Information Risk Owner (SIRO)

The Trust's Senior Information Risk Owner (SIRO) is an executive director appointed by the Board of Directors (BD). The SIRO reports to the BD through the Corporate Governance and Risk work stream.

5.3 Governance Manager

The Governance Manager must ensure that this procedure and any supporting documentation are accurate and relevant to the Trust. The manager is also responsible for implementing these policies and procedures, including training, promoting awareness and providing

advice and guidance as and when required. More detail can be found in appendix 3.

5.4 The Caldicott Guardian

The Caldicott Guardian is the Trust's adviser with respect to the use of patient information. The post holder assists in the formulation of policies relating to the confidentiality of patient documentation and provides expert training and advice to clinical and non-clinical staff.

5.5 The Director of Information Management and Technology

The director manages the informatics and information communication technology teams.

5.6 All staff

All staff employed by the Trust are responsible for ensuring that they comply with the Trust's policy and procedures.

7 Procedures

The respective procedures relating to IG are set out in appendix 2.

8 Training Requirements

All staff will receive awareness training via the Trust INSET days and corporate/clinical induction, and targeted training will be used where specific issues are identified.

Tailored training is given annually to each member of staff through the IG training toolkit. Specialist training shall be provided for those people in specialist roles as part of their PDP.

9 Process for monitoring compliance with this policy

This will be as set out in the IG Framework (see appendix 2)

10 References

See appendix B

11 Associated documents[1]

[1] For the current version of Trust procedures, please refer to the intranet.

12 Appendix 1: Equality Impact Assessment

1. Does this policy, function or service development impact on patients, staff and/or the public?

YES (*go to Section 5*.)

2. Is there reason to believe that the policy, function or service development could have an adverse impact on a particular group or groups?

NO

3. Based on the initial screening process, now rate the level of impact on equality groups of the policy, function or service development:

Negative impact

Low…….
(i.e. minimal risk of having, or does not have negative impact on equality)

Positive impact:

Low……
(i.e. not likely to promote, or does not promote, equality of opportunity)

Date completed 6.1.11

Jonathan McKee, Information Governance Manager

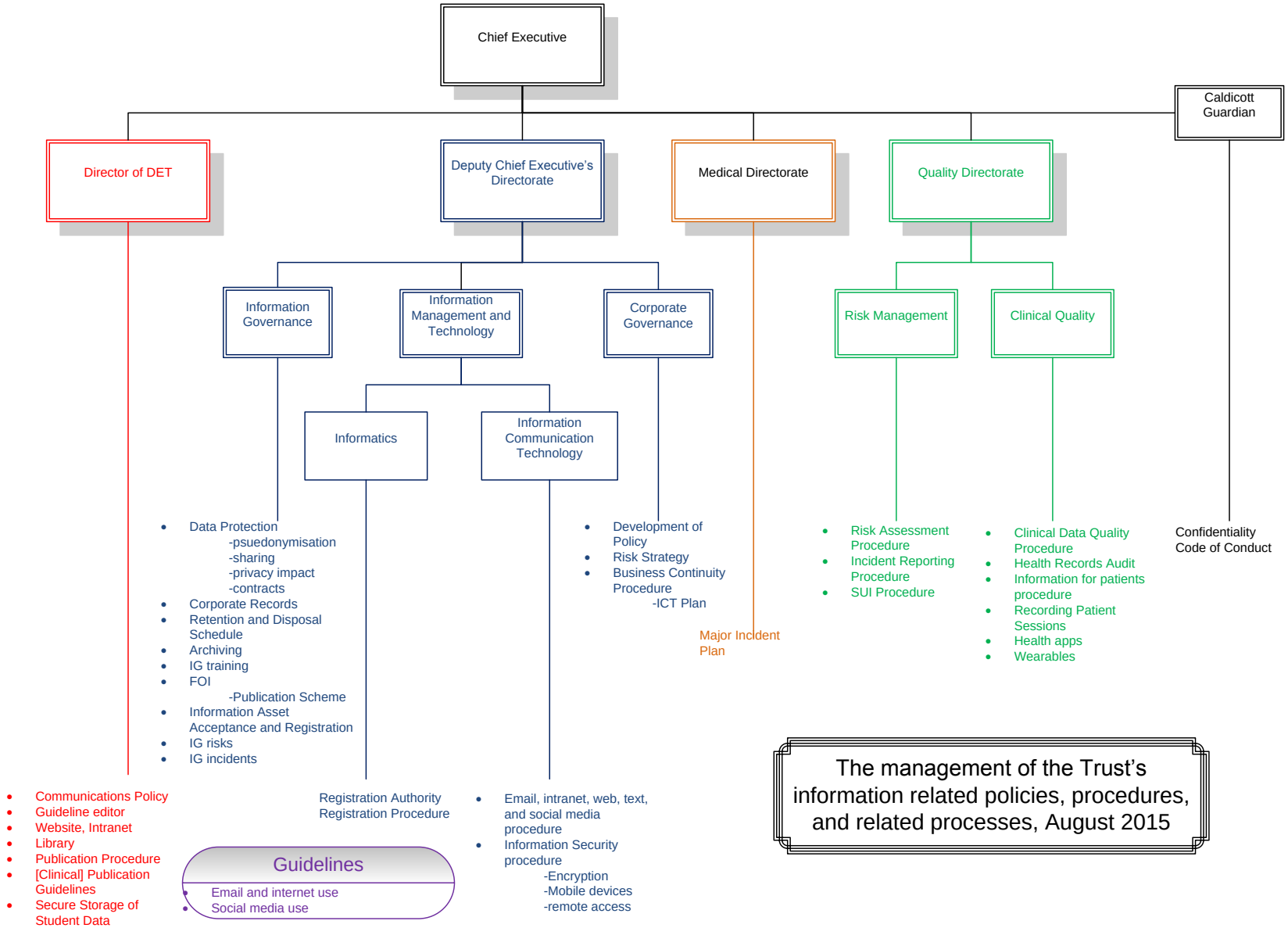
13 Appendix 2: Information Governance Framework

Introduction

This framework sets out the Trust's overview of IG, some of that captured here can be found in more substantive for in the respective policy or procedure.

Policies and procedures

The policies related to IG are written according to the Trust's approach to procedural documents as set out in the Development and Management of policy and procedural Documents procedure. The IG policy sets out the Trust's intent and refers to procedures to set out how this will be achieved; the main elements, and their sub-constituents, are:


Chief Executive
Caldicott Guardian
Director of DET
Deputy Chief Executive's Directorate
Medical Directorate
Quality Directorate
Information Governance
Information Management and Technology
Corporate Governance
Risk Management
Clinical Quality
Informatics
Information Communication Technology
Data Protection
-psuedonymisation
-sharing
-privacy impact
-contracts
Corporate Records
Retention and Disposal Schedule
Archiving
IG training
FOI
-Publication Scheme
Information Asset Acceptance and Registration
IG risks
IG incidents
Development of Policy
Risk Strategy
Business Continuity Procedure
-ICT Plan
Major Incident Plan
Risk Assessment Procedure
Incident Reporting Procedure
SUI Procedure
Clinical Data Quality Procedure
Health Records Audit
Information for patients procedure
Recording Patient Sessions
Health apps
Wearables
Confidentiality Code of Conduct
Communications Policy
Guideline editor
Website, Intranet
Library
Publication Procedure
[Clinical] Publication Guidelines
Secure Storage of Student Data
Registration Authority Registration Procedure
Guidelines
Email and internet use
Social media use
Email, intranet, web, text, and social media procedure
Information Security procedure
-Encryption
-Mobile devices
-remote access
The management of the Trust's information related policies, procedures, and related processes, August 2015

Roles

Senior Information Risk Owner

- ***The main duties of the Senior Information Risk Owner (SIRO) are to:-***

    - Oversee the development of an Information Risk Policy and a Strategy for implementing this policy, compliant with NHS IG policy, standards and methods.
    - Take ownership of the assessment processes for information risk, including prioritisation of risks and review of the annual information risk assessment to support and inform the IG toolkit declarations and the Statement of Internal Control.
    - Ensure that the Board and the Accountable Officer are kept up to date and briefed on all information risk issues affecting the organisation and its business partners.
    - Review and agree actions in respect of identified information risks.
    - Ensure that the Organisation's approach to information risk is effective in terms of resource, commitment and execution, being appropriately communicated to all staff.
    - Provide a focal point for the escalation, resolution and/or discussion of information risk issues.
    - Ensure that an effective infrastructure is in place to support the role by developing a simple Information Assurance governance structure, with clear lines of Information Asset ownership and reporting with well-defined roles and responsibilities.
    - Ensure that identified information threats and vulnerabilities are followed up for risk mitigation, and that perceived or actual information incidents are managed in accordance with NHS IG requirements
    - Ensure that there are effective mechanisms in place for reporting and managing Serious Untoward Incidents (SUIs) relating to the information of the organisation. These mechanisms should accommodate technical, operational or procedural improvements arising from lessons learned.
    - Direct the work of the Information Governance lead.
    - Work with the Information Governance lead and the Caldicott Guardian to provide leadership for the Information Asset Owners (IAOs) of the Organisation through effective networking structures, sharing of relevant experience, provision of training and creation of information risk reporting structures.

Caldicott Guardian

The Guardian plays a key role in ensuring that NHS, Councils with Social Services Responsibilities and partner organisations satisfy the highest practical standards for handling patient identifiable information.
Acting as the 'conscience' of an organisation, the 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 Information Governance requirements and issues at Board or management team level and, where appropriate, at a range of levels within the organisation's overall governance framework.

This role is particularly important in relation to the implementation of the National Programme for IT and the development of Electronic Social Care Records and Common Assessment Frameworks.

Information Governance Lead

The Governance Manager has been appointed as the overall Information Governance Lead to co-ordinate the IG work programme. Under the arrangements the IG lead is accountable for ensuring effective management, accountability, compliance and assurance for all aspects of IG; key tasks include:

a) developing and maintaining the currency of comprehensive and appropriate documentation that demonstrates commitment to and ownership of IG responsibilities, eg an overarching high level strategy document supported by corporate and/or directorate policies and procedures

b) ensuring that there is top level awareness and support for IG resourcing and implementation of improvements;

c) providing direction in formulating, establishing and promoting IG policies;

d) establishing working groups, if necessary, to co-ordinate the activities of staff given IG responsibilities and progress initiatives;

e) ensuring annual assessments and audits of IG policies and arrangements are carried out, documented and reported;

f) ensuring that the annual assessment and improvement plans are prepared for approval by the senior level of management, eg the Board or senior management team in a timely manner. For example, for NHS Trusts sign off may be scheduled in advance of the end of financial year submission on the 31 March each year.

g) ensuring that the approach to information handling is communicated to all staff and made available to the public;

h) ensuring that appropriate training is made available to staff and completed as necessary to support their duties and for NHS organisations this will need to be in line with requirements of the Informatics Planning component of the NHS Operating Framework for 2010/11;

i) liaising with other committees, working groups and programme boards in order to promote and integrate IG standards;

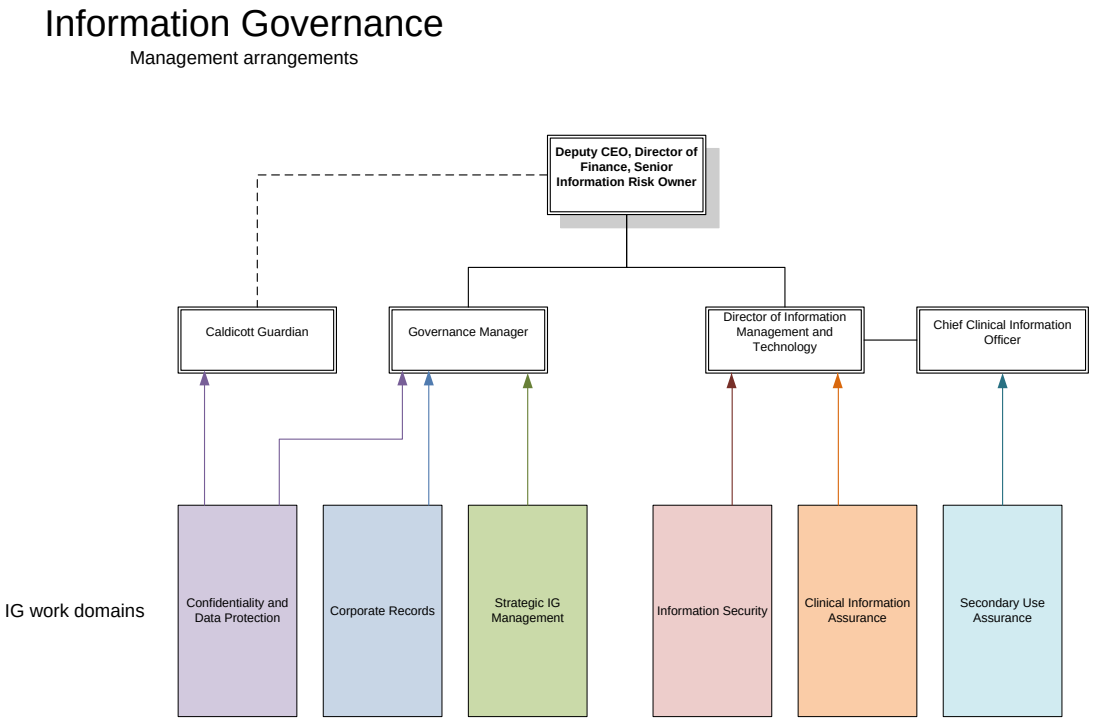
j) monitoring information handling activities to ensure compliance with law and guidance;

k) providing a focal point for the resolution and/or discussion of IG issues.

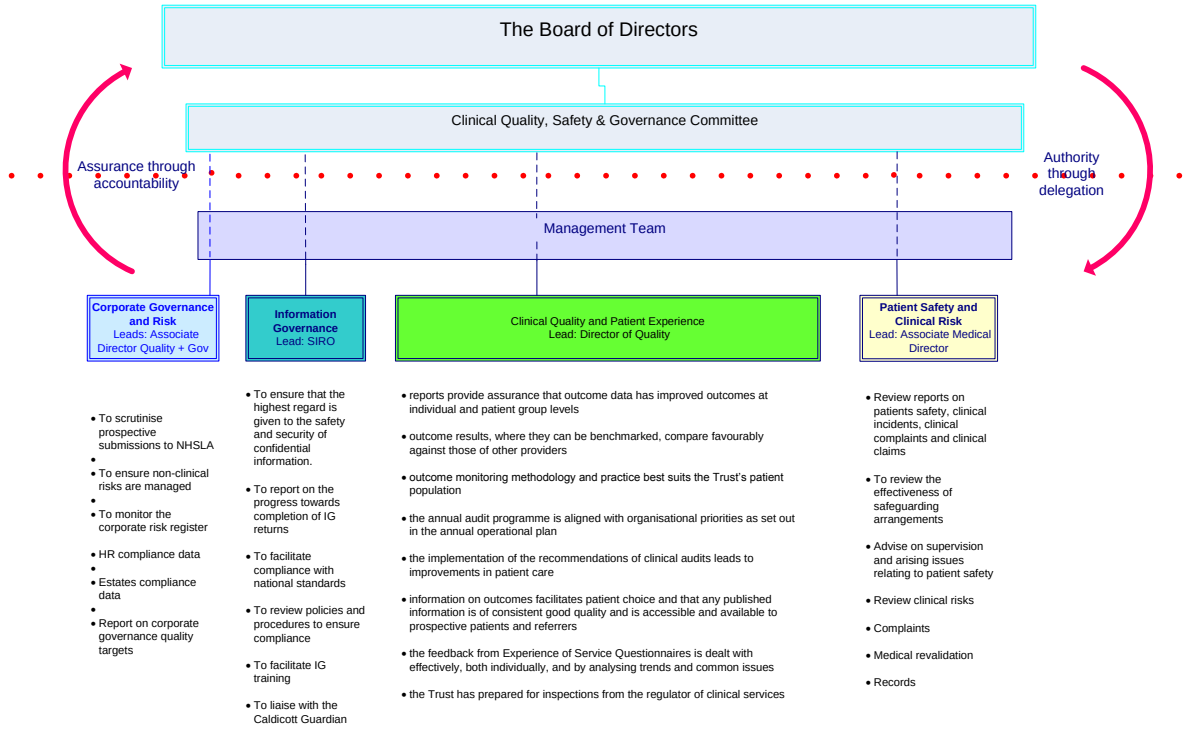
Information Governance Oversight

The Clinical Quality, Safety, and Governance Committee receives assurance that the Information Governance Work Stream is satisfied with the evidence (or action plans where evidence is not yet available) that demonstrates that the Trust is compliant with the requisite standards; that is, any legal, contractual, or regulatory requirements.

The main assessment of compliance will be through the HSCIC's IG toolkit and work towards completing it will be led by the IG manager and reported to the IG work stream on a quarterly basis.



Reporting Quality, Safety, and Risk to Board of Directors



See the Trust's *Guide to Governance* further details.

Training

This will be based on the HSCIC web based application, supplemented with specialist training where necessary. See the intranet for further information on training.

Incident Management

This will be undertaken according to the Trust's procedures on incidents (see intranet for current version).