NHS

The Royal Bournemouth and Christchurch Hospitals

NHS Foundation Trust

Information Governance Strategy

Approval Committee	Version	Approval Date	Review Date	Document Author
Board of Directors	6	June 2019	June 2020	Information Governance Manager

Table of Contents

1. Introduction

Information Governance provides a framework to bring together all the legal rules, guidance and best practice that apply to the handling of information, supporting:

- high quality care;
- compliance with the law;
- implementation of central advice and guidance, and;
- year on year improvement.

Information Governance provides a consistent way for the Trust and its employees to deal with the many different standards and legal rules that apply to information handling, including:

- data protection and confidentiality
- information sharing for care and for non-care purposes
- information security and information risk management
- information quality
- records management for both clinical and corporate information

The Trust believes that accurate, timely and relevant information, protected as required and appropriate, is essential as a component of the highest quality healthcare. As such, it is the responsibility of all clinicians and managers to promote the quality and care of information used in decision-making processes throughout the Trust.

2. Purpose and Scope

The purpose of this document is to set out the internal management structures and responsibilities and provide an overview of the policies and procedures to ensure the safe handling of all information in the Trust in accordance with the law, regulation, best practice and national guidance and minimising information risk within the Trust. Information Governance is the responsibility of every member of staff. The Information Governance Strategy is designed to set out the responsibilities of key staff, and provide all staff with information regarding the structures that are in place to achieve compliance.

The document should not be considered in isolation as it forms part of the Trust's Integrated Governance approach to the management and monitoring of corporate and clinical governance, risk management and clinical effectiveness.

The scope of Information Governance is wide ranging and includes electronic and paper records relating to patients and service users and employees as well as corporate information. The goal is to embed best practice in the Trust so that sensitive and safe handling of all information is considered as part of normal business.

3. Key Roles

The lead for Information Governance within the Trust is the Director of Informatics, who is also the **Senior Information Risk Owner** (**SIRO**).

The SIRO is responsible for coordinating the development and maintenance of information risk management policies, procedures and standards for the Trust in the context of the Trust's overall risk management framework, and updating the Board regularly on information risk issues. The Director of Informatics has line management responsibility for the Information Governance Manager.

The Trust's **Caldicott Guardian** is the Medical Director. The Caldicott Guardian is the most senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing.

As a public authority, the Trust is required by data protection legislation to appoint a **Data Protection Officer** (**DPO**). This is an essential role in facilitating 'accountability', and the organisations' ability to demonstrate compliance with the General Data Protection Regulation (GDPR). This role is assumed by the Information Governance Manager.

4. Key Policies

The Trust has the following Information Governance-related policies:

- Data Protection Policy
- Freedom of Information Policy
- Confidentiality and Disclosure Policy
- Safe Haven Policy
- Information Risk Management Policy & Procedures
- Corporate Records Management and Information Lifecycle Policy
- Health Records Strategy
- Health Records Retention and Disposal Policy
- IT Security Policy
- Risk Management Strategy & Risk Assessment Toolkit
- LERN Policy (incl. Serious Incidents)
- Essential Core Skills Training Policy

Copies of the policies are available on the Trust's intranet and separate guidance on confidentiality and data protection is provided to all staff, governors and volunteers through Essential Core Skills training.

Policies are ratified by the appropriate committees and groups as detailed on the front page of each document, a full list of which is included in the Trust's Document Control Policy.

Policies relating to health records management and subject access requests will be ratified by the Health Records User Group and reviewed by the Information Governance Committee. IT related security policies will be ratified by the Information Governance Committee.

The Healthcare Assurance Committee is responsible for reviewing and approving the Risk Management Strategy & Risk Assessment Toolkit which is ratified by the Board of Directors.

The Quality and Risk Committee is responsible for reviewing and approving the Serious Incident Policy and the LERN (Learning Event Reporting Notification) Policy (incl. Serious Incidents).

The Essential Core Skills Training Group is responsible for reviewing the Essential Core Skills Training Policy which is ratified by the Workforce Strategy Group.

The Information Governance Committee is responsible for reviewing and approving the other policies which are ratified by the Board of Directors or the Audit Committee as required.

5. Governance Framework

The Information Governance Committee is the key governance body with overall responsibility for delivering the Information Governance agenda across the Trust. The Information Governance Committee reports to the Audit Committee, which in turn is a sub-committee of the Board of Directors.

The Trust is audited on the basis of compliance with the laws and standards specified in Appendix A. Compliance is monitored internally through clinical audit, the results of which are reported through the Quality and Risk Committee and Healthcare Assurance Committee, and internal audit which is reported through the Audit Committee. In addition the Data Security and Protection Toolkit is completed each year and the results are forwarded to the local Clinical Commissioning Groups, NHS Improvement and the Care Quality Commission, all of which have powers to intervene in the running of the Trust in the event of failings in its healthcare standards.

Compliance with the Data Security and Protection Toolkit is used as one of the measures reported in the Quality Report and Annual Governance Statement in the Annual Report and Accounts. This assures compliance with the Care Quality Commission's standards relating to Information Governance.

6. Resources

The Information Governance Manager is responsible for:

- ensuring compliance with legislation and standards for Information Governance and reporting performance to the Information Governance Committee;
- keeping new legislation and standards under review and ensuring appropriate amendments to policies and procedures are introduced;
- developing and reviewing the Information Governance action plan and reporting progress, risks and outcomes to the Information Governance Committee;
- reporting issues and risks relating to confidentiality to the Information Governance Committee;
- developing and maintaining relevant policies, standards, procedures and guidance;
- reviewing operational Information Governance issues that arise;
- providing a co-ordinating role for Information Governance within the Trust;
- communicating and raising awareness of Information Governance across the Trust.

The **SIRO** is also supported by **Information Asset Owners** (**IAOs**) who have been appointed by their respective departments/directorates, and who shall ensure that information risk assessments are performed at least once each year on all information assets (IT systems/databases which contain personal data) where they have been assigned ‘ownership’, following guidance from the SIRO on assessment method, format and content. This process should reflect the policy and procedures for risk assessment adopted by the Trust more generally. IAOs shall submit the risk assessment results and associated mitigation plans to the SIRO for review at meetings of the Information Governance Committee.

IAOs are also responsible for:

- ensuring that commercial contracts with third parties relating to their assets contain the relevant Information Governance clauses;
- ensuring that their assets support appropriate access controls;
- putting in place business continuity arrangements as required to support the continuation of services in the event of the asset being unavailable;
- providing the Information Governance Manager with details of any transfers of personal data into and outside of the Trust from within their work areas, including those that are overseas;
- understanding the legal basis under which data within their department is processed, and keeping this up to date on the Information Asset Register, and;
- disseminating best Information Governance practice throughout their department/work areas.

A full role profile for IAOs is available within the Information Risk Management Policy.

The lead for **IT Security** (including policy development) is the IT Security Manager.

The lead for **Data Quality** (including policy development) is the Head of Information.

The lead for **Health Records** management and subject access policy development is the Health Records Manager.

The lead for the Trust’s **Registration Authority** (**RA**) function is the Director of Informatics. Responsibilities for the management and implementation of the RA function including documenting a local RA policy have been allocated to the IT Applications Manager, who acts as the RA Manager.

The Trust has also nominated a **Clinical Safety Officer** who is responsible for the control of clinical risk associated with a new IT system roll out or change to an IT system to support compliance with ISB 0160.

All staff contracts contain clauses relating to data protection and confidentiality. These clauses alert staff to how their data will be used and their data protection rights and the consequences of breaching confidentiality in terms of disciplinary action and professional registration. Breaches of confidentiality are specifically referred to in the Trust’s Disciplinary Policy and Procedure as an example of gross misconduct.

There is also a Code of Conduct for Staff which acts as a guide to all members on the required behaviours, responsibilities and actions expected of employees of the Trust. This has been is produced in line with guidance issued by the Department of Health.

7. Training and Guidance

All staff, volunteers and governors receive Information Governance training as part of initial induction and annually thereafter. The Information Governance training programme covers staff at all levels, both clinical and non-clinical, and is detailed in full in the Information Governance Training Plan, which is reviewed annually for its effectiveness.

In addition, IAOs are given specific training by the Information Governance Manager, SIRO and other subject matter experts to ensure that they understand their duties and can complete their IAO tasks effectively.

8. Incident Management

Information Governance incidents should reported and managed in accordance with the Trust's LERN Policy (including Serious Incidents). The Quality and Risk Department will inform the Information Governance Manager of all adverse incidents which relate to Information Governance so that the Information Governance Manager may provide input and support to staff dealing with these incidents and monitor these as required. The reporting process for incidents which are suspected to be serious incidents is set out in Appendix D. Serious incidents are assessed using the NHS Digital Guide to the Notification of Data Security and Protection Incidents and reported to the relevant authorities through the Data Security and Protection Toolkit in accordance with Trust policies supported by additional guidance used by the Information Governance Manager.

APPENDIX A
Legislative and Regulatory Framework

The Information Governance Strategy brings together all the requirements, standards and best practice that apply to handling information. The areas that are covered are to be kept under review as changes are made to legislation and guidance.

Legislation and common law

This includes:

- Access to Health Records Act 1990
- Access to Medical Reports Act 1988
- Common law duty of confidentiality
- Computer Misuse Act 1990
- Data Protection Act 2018
- General Data Protection Regulation (GDPR) 2016
- Environmental Information Regulations (EIR) 2004
- Freedom of Information (FOI) Act 2000
- Health and Social Care Act 2012
- Human Rights Act 1998 (Article 8)
- National Health Service Act 2006
- Privacy and Electronic Communications (EC Directive) Regulations 2003
- Protection of Freedoms Act 2012
- Re-use of Public Sector Information Regulations 2005

Standards and Guidance

The standards are defined by a number of national bodies and include:

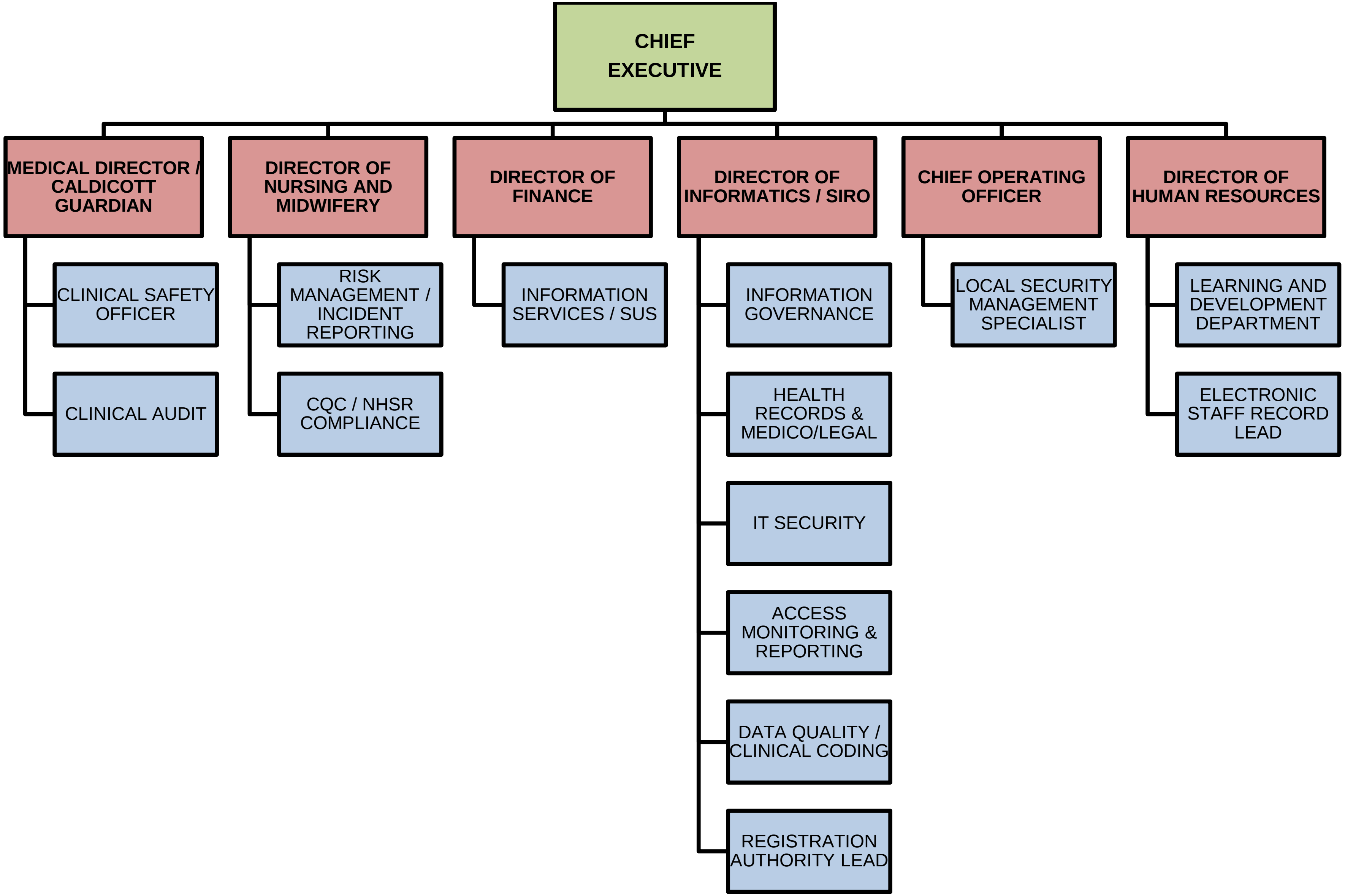
- Health Service Circular: HSC 1999/012 (requirement for NHS organisations to have a Caldicott Guardian)
- The Caldicott Principles
- The Caldicott Guardian Manual 2010
- Care Quality Commission Fundamental Standards Regulation 17: Good Governance
- NHS Data Security and Protection Toolkit
- NHSLA standards for Acute Trusts
- BS ISO/IEC 17799:2005; BS ISO/IEC 27001:2005; BS7799-2:2005 – Management Information Security compliance
- Information Security Management: NHS Code of Practice (April 2007)
- Confidentiality: NHS Code of Practice (November 2003)
- Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems (ISB 0160 2013)
- HSCIC: A guide to confidentiality in health and social care (September 2013)
- Information Governance Alliance Records Management Code of Practice for Health and Social Care (July 2016)
- Information: To Share or not to Share – The Information Governance Review (“Caldicott 2”) (March 2013)
- National Data Guardian for Health and Care Review of Data Security, Consent and Opt-Outs (“Caldicott 3”) (June 2016)
- Guide to the Notification of Data Security and Protection Incidents (September 2018)

Professional Codes and Rules

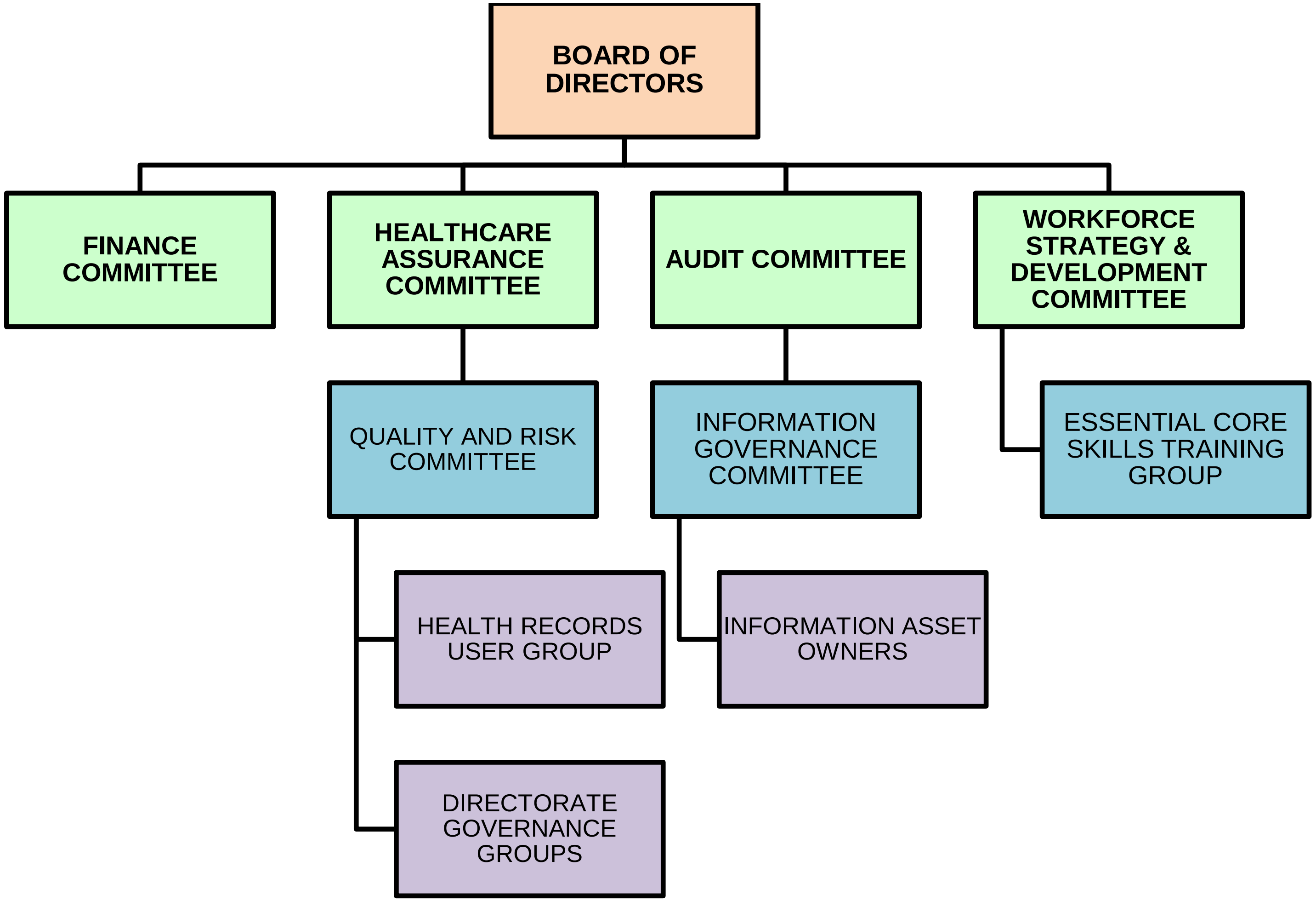
Professional bodies have also set out standards for relevant professionals and associated guidance which includes:

- General Medical Council, Good Medical Practice (2013)
- General Medical Council, Confidentiality for Doctors (2017)
- Nursing & Midwifery Council, The code: Standards of conduct, performance and ethics for nurses and midwives produced by the– paragraphs 42-47 (May 2008)
- Nursing & Midwifery Council, Record keeping: Guidance for nurses and midwives (July 2009)
- General Pharmaceutical Council, Standards of conduct, ethics and performance – principle 3 (July 2012)
- Health & Care Professions Council, Standards of conduct, performance and ethics – principle 2 (2012)
- Chartered Society of Physiotherapy Rules of Professional Conduct (2nd edition) – Rule 3 (January 2002)
- British Medical Association, Confidentiality and Disclosure of Health Information Toolkit
- Royal College of Physicians, Generic Medical Records Keeping Standards (June 2015)

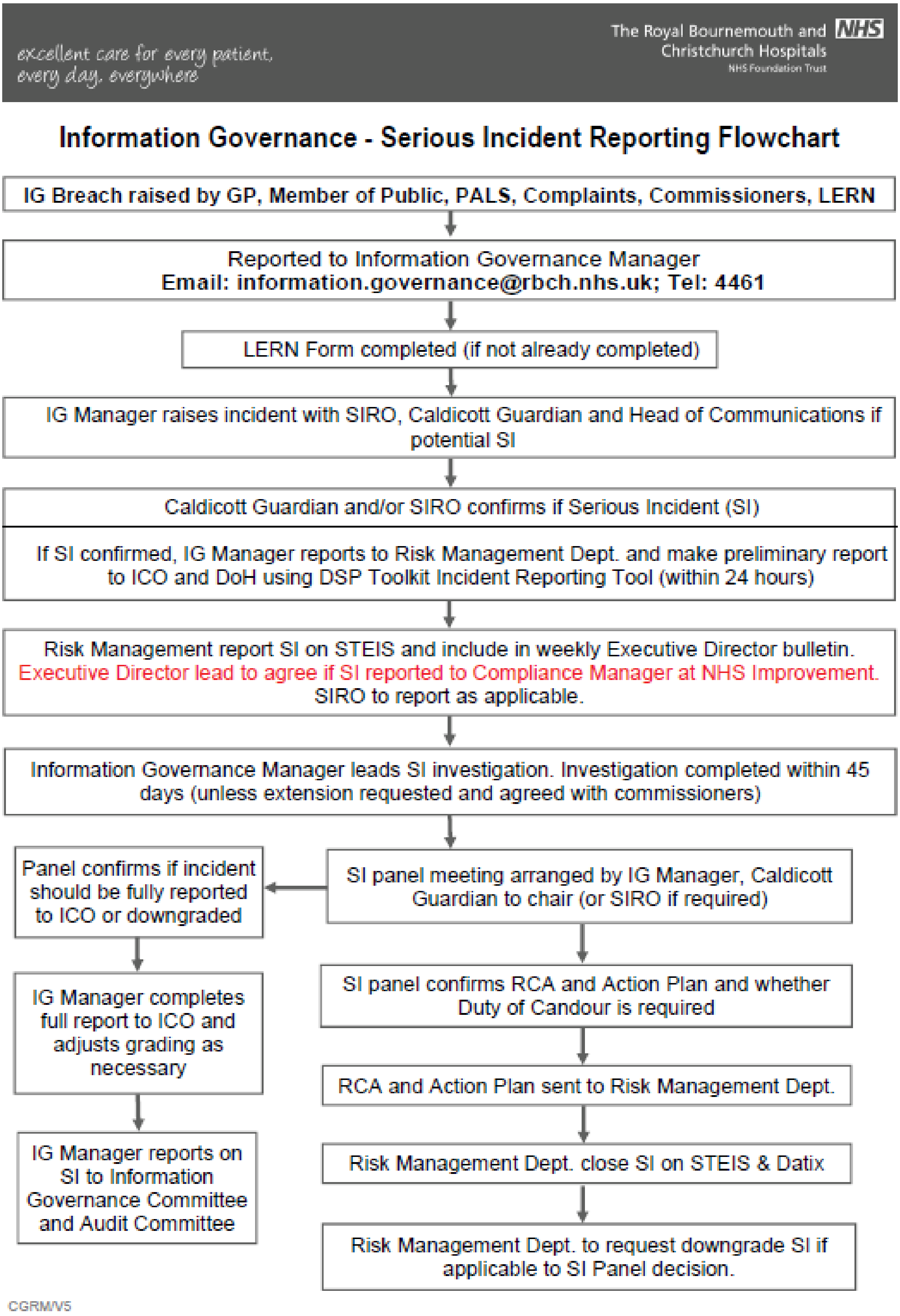
APPENDIX B
Overarching Information Governance Structure


CHIEF EXECUTIVE
MEDICAL DIRECTOR / CALDICOTT GUARDIAN
CLINICAL SAFETY OFFICER
CLINICAL AUDIT
DIRECTOR OF NURSING AND MIDWIFERY
RISK MANAGEMENT / INCIDENT REPORTING
CQC / NHSR COMPLIANCE
DIRECTOR OF FINANCE
INFORMATION SERVICES / SUS
DIRECTOR OF INFORMATICS / SIRO
INFORMATION GOVERNANCE
HEALTH RECORDS & MEDICO/LEGAL
IT SECURITY
ACCESS MONITORING & REPORTING
DATA QUALITY / CLINICAL CODING
REGISTRATION AUTHORITY LEAD
CHIEF OPERATING OFFICER
LOCAL SECURITY MANAGEMENT SPECIALIST
DIRECTOR OF HUMAN RESOURCES
LEARNING AND DEVELOPMENT DEPARTMENT
ELECTRONIC STAFF RECORD LEAD

APPENDIX C
Committee Structure


BOARD OF DIRECTORS
FINANCE COMMITTEE
HEALTHCARE ASSURANCE COMMITTEE
AUDIT COMMITTEE
WORKFORCE STRATEGY & DEVELOPMENT COMMITTEE
QUALITY AND RISK COMMITTEE
INFORMATION GOVERNANCE COMMITTEE
ESSENTIAL CORE SKILLS TRAINING GROUP
HEALTH RECORDS USER GROUP
INFORMATION ASSET OWNERS
DIRECTORATE GOVERNANCE GROUPS

APPENDIX D
Information Governance Serious Incident Reporting Flowchart



excellent care for every patient, every day, everywhere

The Royal Bournemouth and Christchurch Hospitals NHS Foundation Trust

Information Governance - Serious Incident Reporting Flowchart

IG Breach raised by GP, Member of Public, PALS, Complaints, Commissioners, LERN

Reported to Information Governance Manager
Email: information.governance@rbch.nhs.uk; Tel: 4461

LERN Form completed (if not already completed)

IG Manager raises incident with SIRO, Caldicott Guardian and Head of Communications if potential SI

Caldicott Guardian and/or SIRO confirms if Serious Incident (SI)

If SI confirmed, IG Manager reports to Risk Management Dept. and make preliminary report to ICO and DoH using DSP Toolkit Incident Reporting Tool (within 24 hours)

Risk Management report SI on STEIS and include in weekly Executive Director bulletin. Executive Director lead to agree if SI reported to Compliance Manager at NHS Improvement. SIRO to report as applicable.

Information Governance Manager leads SI investigation. Investigation completed within 45 days (unless extension requested and agreed with commissioners)

SI panel meeting arranged by IG Manager, Caldicott Guardian to chair (or SIRO if required)

Panel confirms if incident should be fully reported to ICO or downgraded

IG Manager completes full report to ICO and adjusts grading as necessary

IG Manager reports on SI to Information Governance Committee and Audit Committee

SI panel confirms RCA and Action Plan and whether Duty of Candour is required

RCA and Action Plan sent to Risk Management Dept.

Risk Management Dept. close SI on STEIS & Datix

Risk Management Dept. to request downgrade SI if applicable to SI Panel decision.

CGRM/V5