Somerset Partnership NHS
NHS Foundation Trust

INFORMATION GOVERNANCE POLICY

Version:	5
Date issued:	**August 2017**
Review date:	**June 2018**
Relevant Staff Group/s:	All staff who have access to any Personal Confidential Data (PCD).

This document is available in other formats, including easy read summary versions and other languages upon request. Should you require this please contact the Equality and Diversity Lead on 01278 432000

DOCUMENT CONTROL

Reference	**Version**	**Status**	**Author**
PA/Aug15/IGP	5	Final	Information Governance and Records Manager

Amendments

- Annual review of the policy to include latest changes to Health and Social Care Information Centre, Department of Health and NHS England guidance and any change to UK legislation.
- Change to structure in Appendix A
- Although 3 year review date review will occur annually for any changes to guidance or UK Law.
- Policy extended to September 2017
- Due review: policy updated to comply with the revised policy template, updated titles and groups following the revised Governance Structure and correct Caldicott Guardian.

Document objectives: This policy provides the overarching focus for Information Governance for the Partnership Trust in line with the Information Governance Toolkit.

Approving body	Caldicott and Information Governance Group	Date: June 2017
Equality Impact Assessment	Impact Part 1	Date: August 2017
Ratification Body	Senior Management Team	Date: August 2017
Date of issue	**August 2017**	
Review date	**June 2018**	
Contact for review	Information Governance and Records Manager	
Lead Director	Director of Strategy and Corporate Affairs	

CONTRIBUTION LIST Key individuals involved in developing the document

Designation or Group
Information Governance Manager
Director of Strategy and Corporate Affairs
Caldicott and Information Governance Group
Claims and Litigation Manager
EIA / Head of Corporate Business
Senior Management Team

CONTENTS

1. INTRODUCTION

1.1 "Information Governance" informs the processes required to ensure all information held by the Trust adheres to approved levels of confidentiality, security, accountability, standards, policies and procedures.

1.2 The NHS Information Governance Toolkit requires all NHS Trusts to develop and maintain information governance standards. As the Toolkit evolves, the Partnership Trust must ensure that it adheres to increasingly stringent criteria. The toolkit initially was IT focussed but now encapsulates records management, confidentiality, record keeping and many other areas.

1.3 This policy is supported by and should be read in conjunction with the following information related documents:

- Confidentiality and Data Protection Policy
- Freedom of Information Policy
- Information Security Policy
- Record Keeping and Records Management Policy

2. PURPOSE & SCOPE

2.1 Information Governance covers all information held by the Trust regardless of format.

2.2 Information is categorised as sensitive and confidential if it contains personal details of staff, service users and families. Non-confidential information would, for example, be approved policies placed on the Trust's website.

2.3 The Trust must comply with NHS Records Management: Code of Practice legislation which regulates the creation, holding, transfer and destruction of such information.

2.4 Information held by the Partnership Trust may be owned or required from external organisations, for it to undertake its legitimate business.

2.5 Access to accurate and timely information is invaluable to any organisation however, maintaining appropriate levels of confidentiality and security is also essential.

2.6 It is therefore vital that the organisation has in place strong and developed management accountability through policies, procedures and structures which provide a robust governance framework for Information Management.

2.7 Partnership Trust operational strategies, policies and guidance exist to underpin the fundamental building blocks of Information Governance. These will be reviewed in line with the evolution of the Information Governance toolkit criteria.

2.8 Where significant changes are required practice guidance will be issued immediately and appropriate policies reviewed to incorporate any new requirements.

3. DUTIES AND RESPONSIBLITIES

3.1 **All staff** have a responsibility to ensure that information is recorded accurately and in a timely manner and that information is only shared with those who need to know and is transmitted securely.

3.2 This responsibility is both a professional one (required by the appropriate professional governing body), and a contractual one, with confidentiality incorporated into the terms and conditions of all contracts of employment and contracts for services. Ongoing training and awareness will be provided to all staff teams. Awareness for new staff is provided through the Trust's induction process.

3.3 **All managers** are required to ensure that policies are understood, with issues being discussed in supervision or team meetings. Where areas of poor understanding exist, training needs analysis should be carried out and contact made with the Information Governance and Records Manager so further support and training can be provided. Managers will take responsibility for ensuring that the Information Governance Policy is implemented within their area of responsibility.

3.4 Where temporary or contract staff are employed it is the responsibility of the line manager employing those individuals to ensure compliance with and understanding of Information Governance, IM&T Security and that signing of the Code of Confidentiality takes place prior to commencement of work.

3.5 The **Caldicott and Information Governance (IG) Group** will meet on a quarterly basis and will be responsible for the oversight of:

- annual formal verification and sign off of compliance with the Information Governance Toolkit (IGT)
- approving and monitoring an Information Governance work programme annually informed from the NHS Information Governance Toolkit.
- health records management for the Trust.
- the development, approval and implementation of all associated policies and processes and ongoing monitoring of compliance related to Information Governance.
- review this Policy at least every three years or sooner if required due to changes in either local procedure and/or national guidance.
- areas or concern and new significant risks which will be escalated to the Quality and Performance Committee within the quarterly reporting schedule

3.6 **Trust Board:** The Trust Board has overall responsibility for ensuring robust operational management systems and governance are in place in order for the Trust to be able to comply with the Data Protection Act 1998 and the general law on matters of confidentiality.

3.7 **Chief Executive**: The Chief Executive has the ultimate responsibility for compliance with Information Governance under the asepses of the Information Governance Toolkit for the Trust and as such the Chief Executive shall:

- appoint a Data Protection Officer
- appoint a Caldicott Guardian
- appoint a Senior Information Risk Owner

3.8 **Data Protection Officer: The Director of Strategy and Corporate Affairs** is the Lead Director for Data Protection who will ensure that the Trust complies with the Data Protection Act 1998, maintain the Trust's Data Protection registration with the Information Commissioner's Officer and lead on the data protection work programme, in collaboration with the Caldicott Guardian.

3.9 **Caldicott Guardian: Consultant Psychiatrist** is the Caldicott Guardian who will lead on all aspects of Caldicott work across the Trust including confidentiality of patient information as required by the Caldicott principles and role of the NHS Caldicott Guardian.

3.10 **Senior Information Risk Owner: The Director of Finance and Business Development** is the Senior Information Risk Owner and is responsible for ensuring Information Security is compliant to the requirements of the Information Governance Toolkit.

3.11. **Chief Operating Officer**: will ensure Senior Managers are aware of the requirements of this policy.

3.12 **Data Protection Lead Manager:** The Head of Risk will be the lead manager on Data Protection, supported by the Information Governance and Records Manager and the Information Governance Administrator: who between the three of them, together with the Caldicott Guardian, undertake the Caldicott Function role. The role will be the lead on Subject Access Requests under the Data Protection Act 1998.

3.13 **Information Governance and Records Manager**: This role will lead on the co-ordination of the Trust's compliance with the Information Governance Toolkit and will assist the lead on the processing and response to Subject Access requests under the Data Protection Act 1998.

3.14 **Head of Information:** This role will lead on all aspects of the NHS Connecting for Health Information Governance Toolkit: information technology solutions assisted by the Information Systems Technical Manger and key Information Team staff.

3.15 **Information Security Manager:** This role will include the lead on all aspects of information security under the Senior Information Risk Officer (SIRO).

3.16 **Information Delivery Manager**: will monitor the data quality with regard to the Trust's EPR (Electronic Patient Records – RiO system).

4. DEFINITIONS

4.1 **IGT – Information Governance Tool kit** – Self assessment tool provided by the NHS Information Centre which provides all NHS organisations with a set of standards appropriate to their area.

5. INFORMATION GOVERNANCE

5.1 This document sets out the Policy the Trust will use to ensure compliance with the information governance toolkit initiatives which are categorised under the following headings:-

- Information Governance Management
- Confidentiality and Data Protection Assurance
- Information Security Assurance
- Clinical Information Assurance
- Secondary User Assurance
- Corporate Information assurance

5.2 The following are overviews of the initiatives and are not exhaustive lists.

Information Governance Management
This informs the Trust's requirements for accountability by the Trust Board and delegated sub-groups. It informs specific individuals e.g. Caldicott Guardian and Directors, Senior Managers and lead staff, e.g. information security expert/data protection manager.

Confidentiality and Data Protection Assurance
This informs the Partnership Trust of the NHS Confidentiality Code requirements and maps the flow of sensitive and personal information. It also states the requirements to ensure computer technology is robust, fit for purpose and secure.

5.3 The assurance requires the Partnership Trust to ensure that:

- service users, carers and families are informed of what information is held about them and what rights they have to access it.
- any information held is only shared with people who have a legitimate relationship with the client and therefore have the right to access it.

Information Security Assurance

5.4 The Partnership Trust will ensure under this initiative that:

- information is held securely within filing systems, whether electronic or paper based.
- technological processes are used to ensure that when information is sent outside of the Partnership Trust and potentially the Trust's control. This is done using secure methods of transfer, using appropriate levels of protection wherever possible.

- all desktop computers and laptops are encrypted to ensure high risk devices are protected from accidental loss or theft (using the nationally procured encryption software).

Clinical Information Assurance

5.5 Under this initiative the Trust will ensure that:

- information is cross-referenced with external systems to verify that information held is of good quality and accurate.
- information recorded on all systems is updated by operational staff, ensuring its accuracy.
- staff are appropriately trained about their responsibility to ensure information is recorded accurately and in a timely fashion.

Secondary User Assurance

5.6 This initiative centres around NHS standard definitions, benchmarking, data quality reports and audits, ensuring compliance with national set standards ensuring our data is fit for purpose for use by other organisations via the Secondary User Service.

Corporate Information Assurance

5.7 This initiative set is broadly separated into Records Management and the Freedom of Information Act 2000.

6. REPORTING DATA BREACHES

6.1 Reporting any confidentiality breach will be through the Trust's DATIX electronic untoward incident reporting system.

6.2 All breaches of confidentiality will be collated by the Trust's Caldicott Guardian assisted by the Caldicott Function and will be presented to, and reviewed by, the Caldicott and Information Governance Group.

6.3 If there appears to have been a significant breach of confidentiality or the legislation then this should be immediately reported to the Data Protection Officer or the Caldicott Guardian so that reporting to the relevant regulatory body (Department of Health, Information Commissioner) through the new Information Governance SIRI reporting tool within the Information Governance Toolkit can take place.

6.4 The Information Governance Reporting structure is demonstrated within Appendix A of this policy.

7. TRAINING REQUIREMENTS

7.1 The Trust will ensure that all necessary staff are appropriately trained in line with the organisation's training needs analysis.

7.2 Additionally, staff who have specific responsibilities under the Information Governance Toolkit, will, as required, have training applicable to their needs, once a skills gap analysis has taken place.

7.3 Senior Managers will require training provided by the IG Toolkit or the NHS Health e-learning packages

7.4 All staff within the Trust will have basic Information Governance awareness as part of their induction training.

7.5 Information Asset Owners are trained via the Trust's specific training covering this activity.

8. MONITORING COMPLIANCE AND EFFECTIVENESS

8.1 The Trust will use the Department of Health's (NHS IC) Information Governance self-assessment toolkit to monitor ongoing compliance. The underlying principles are set out in the standards called the HORUS model. This sets out that information should be: -

- **H**eld securely and confidentially
- **O**btained fairly and efficiently
- **R**ecorded accurately and reliably
- **U**sed effectively and ethically
- **S**hared appropriately and lawfully

8.2 Monitoring arrangements for compliance and effectiveness

The Trust will utilise the Information Governance Toolkit and related national initiatives, e.g. CQC for ongoing monitoring against Information Governance standards.

8.3 Responsibilities for conducting the monitoring

The Caldicott and Information Governance Group will monitor overall compliance against standards. Assessment reports of compliance will be produced by the Information Governance and Records Manager and presented to the Caldicott and Information Governance Group Quarterly along with, where required, a compliance work plan.

8.4 Methodology to be used for monitoring

- Information Governance Toolkit
- Incident reporting
- Audits including internal and external auditors

9. REFERENCES, ACKNOWLEDGEMENTS AND ASSOCIATED DOCUMENTS

9.1 References

Information Governance Tool kit version 11

Relevant National Requirements

Department of Health – Information Governance

Data Protection Act 1998

Freedom of Information Act 2000

Access to Health Records Act 1990

NHS Records Management: Code of Practice 2005

9.2 Cross reference to other procedural document

Confidentiality and Data Protection Policy

Freedom of Information Policy

Information Security Policy

Learning Development and Mandatory Training Policy

Record Keeping and Records Management Policy

Risk Management Policy and Procedure

Staff Mandatory Training Matrix (Training Needs Analysis)

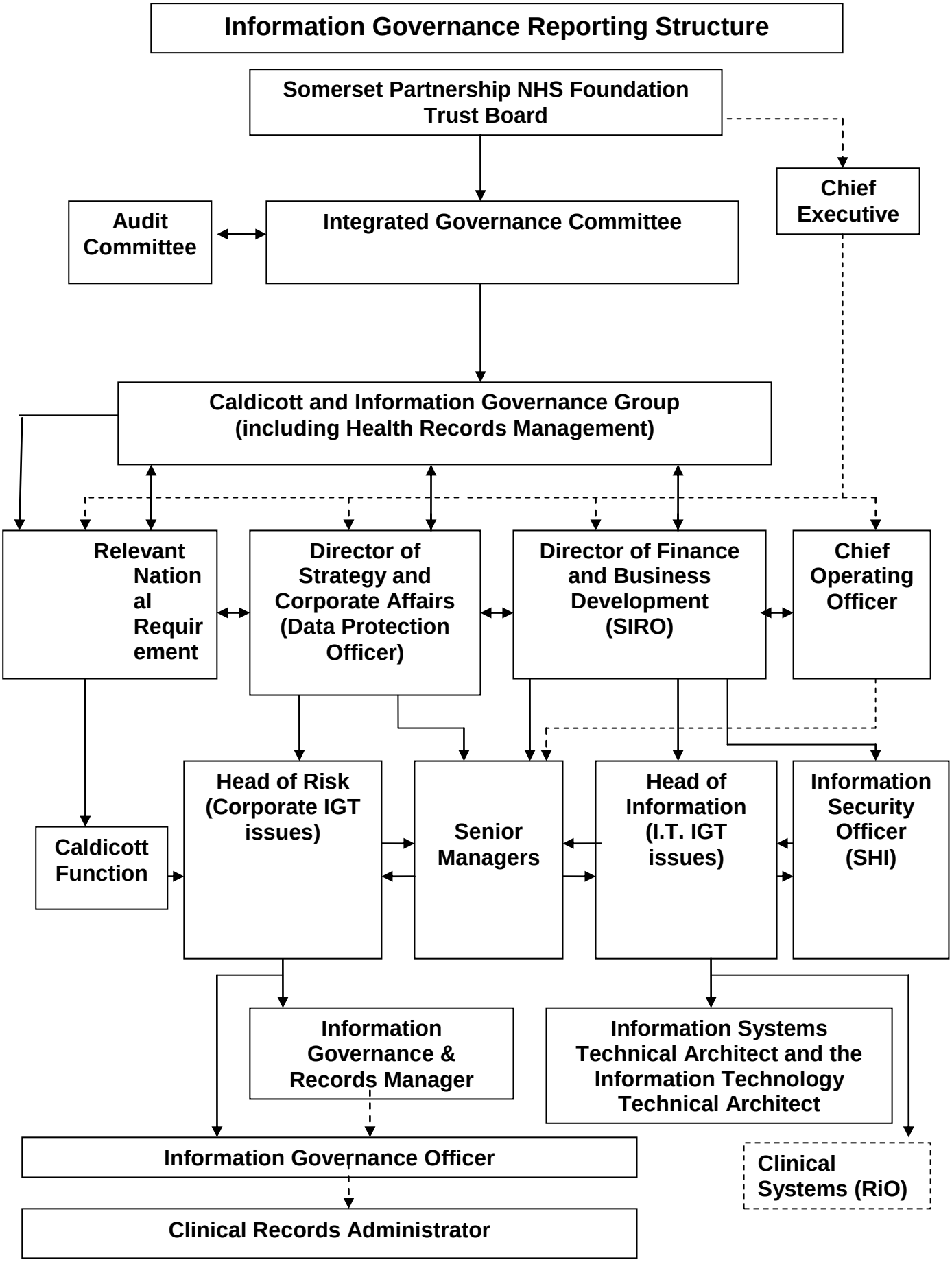
Untoward Event Reporting Policy and procedure

For the avoidance of any doubt the appendices in this policy are to constitute part of the body of this policy and shall be treated as such. This should include any relevant Clinical Audit Standards.

10. APPENDICES

10.1 For the avoidance of any doubt the appendices in this policy are to constitute part of the body of this policy and shall be treated as such.

Appendix A Information Governance Reporting Structure


Information Governance Reporting Structure
Somerset Partnership NHS Foundation Trust Board
Chief Executive
Audit Committee
Integrated Governance Committee
Caldicott and Information Governance Group (including Health Records Management)
Relevant National Requirement
Director of Strategy and Corporate Affairs (Data Protection Officer)
Director of Finance and Business Development (SIRO)
Chief Operating Officer
Caldicott Function
Head of Risk (Corporate IGT issues)
Senior Managers
Head of Information (I.T. IGT issues)
Information Security Officer (SHI)
Information Governance & Records Manager
Information Systems Technical Architect and the Information Technology Technical Architect
Information Governance Officer
Clinical Systems (RiO)
Clinical Records Administrator