Torbay and Southern Devon Health and Care NHS Trust

Information Governance Policy

Date: February 2015

Partners in Care

Torbay Council

This is a controlled document. It should not be altered in any way without the express permission of the author or their representative.

On receipt of a new version, please destroy all previous versions.

Document Information

Date of Issue:	February 2015	Next Review Date:	February 2017
Version:	2	Last Review Date:	August 2012
Author:	Head of Information Governance, Helen Thorn		
Directorate:	Corporate Affairs		
Approval Route			
Approved By:		Date Approved:	
Management of Information Group		11 February 2015	
Links or overlaps with other strategies/policies:			
Information Governance Management Framework			
Information Governance Annual Report and Work Plan			
Information Lifecycle Strategy			
Information Management Policy and associated procedures			
Data Protection Policy			
Staff Code of Confidentiality			
Management of Information Policy			
Request for Information Procedure			

Amendment History

Issue	Status	Date	Reason for Change	Authorised
1	Final	August 2012	Creation of document	Helen Thorn
2	Final	11 February 2015	Review of documentation and refresh of links and contact details.	Management of Information Group

Contents

1. Introduction

1.1. Information Governance allows Torbay and Southern Devon Health and Care NHS Trust (Trust) and individual members of staff to ensure that information, including personal and sensitive information is handled legally, securely, efficiently and effectively, in order to deliver the best possible care.

1.2. Additionally it enables the Trust to put in place procedures and processes for their corporate information that support the efficient location and retrieval of corporate records where and when needed, in particular to meet requests for information and assist compliance with Corporate Governance standards.

1.3. Information Governance has the following fundamental aims:

- To support the provision of high quality care by promoting the effective and appropriate use of information;
- To encourage staff to work closely together, preventing duplication of effort and enabling more efficient use of resources;
- To develop support arrangements and provide staff with appropriate tools and support to enable them to discharge their responsibilities to consistently high standards;
- To enable organisations to understand their own performance and manage improvement in a systematic and effective way.

1.4. This Policy together with the following form the Information Governance Strategy for the Trust.

- The Information Governance Management Framework, Appendix 1;
- The Information Governance Toolkit self-assessment;
- The Annual Information Governance Report to the Board;
- The Information Governance Annual Work Plan;
- Terms of Reference and work plan for the Management of Information Group.

2. Policy Statement

2.1. This policy sets out how the Trust provides a robust Information Governance Management Framework to ensure the delivery of internal Information Governance assurance in accordance with national operating frameworks, legislation and the Information Governance Toolkit.

3. Responsibilities

3.1. **The Board** role is to define the Trust's policy in respect of Information Governance, taking into account legal and NHS requirements. The Board is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

They will receive the Information Governance Report and Work Plan on an annual basis. Regular reporting to the Board will be through the Corporate Governance Meeting and Integrated Governance Committee (see Appendix 1).

3.2. The **Chief Executive** has delegated responsibility for Information Governance to the Company Secretary. The Director of Finance is the Senior Information Risk Officer for the Trust.

3.3. **Senior Information Risk Officer (SIRO)** is

- familiar with and takes ownership of the Trust's information risk policy;
- acts as advocate for information risk on the Board.

3.4. **Caldicott Guardian**

- ensures that the Trust and its partner organisations satisfy the highest practical standards to handling personal information;
- acts as the "conscience" of the Trust;
- actively supports work to facilitate and enable information sharing, advising on options for lawful and ethical processing of information as required.

3.5. **Head of Information Governance** is responsible for:

- ensuring effective management, accountability, compliance and assurance for all aspects of Information Governance;
- developing and providing support to managers and staff to enable them to discharge their responsibilities to consistently high standards.

3.6. **Managers** are responsible for

- ensuring that the policy and its supporting standards and guidelines are built into local processes;
- ensuring on-going compliance within their teams;
- taking ownership of, and seeking to improve, the quality of information within their services;
- ensuring that all staff whether, permanent, contract, voluntary, student or temporary, undertake Information Governance Training on an annual basis.

3.7. **All Staff including contract, temporary, students, voluntary staff** are responsible for:

- understanding the Trust requirements for Information Governance;
- ensuring that they comply with them in day to day business;
- undertaking Information Governance training on an annual basis;
- ensuring and promoting the use of high quality information;

Staff should be aware that if they are found to have made an unauthorised disclosure they may face disciplinary action, which could lead to dismissal and legal action being taken against them.

3.8. **Management of Information Group** will

- meet on a regular basis;
- promote a holistic approach to Information Governance;
- influence integration and inclusion of information governance standards with other governance strategies, work programmes and projects, in particular IT;
- report to the Integrated Governance Committee.

4. Principles of Information Governance

The Trust believes that '*the right information, right person, right time'* is essential to deliver high quality integrated health and social care. There are four key interlinked strands to this Information Governance Policy:

- Openness
- Legal compliance
- Information security
- Quality assurance

4.1 Openness

- Non-confidential information on the organisation 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;
- The Trust will undertake annual assessments and audits of its policies and arrangements for openness;
- Patients/clients should have ready access to information relating to their own care, their options for care and treatment and their rights as patients/clients;
- The Trust will have clear procedures and arrangements for liaison with the press, broadcasting media and for handling queries from patients/clients and public.

4.2 Legal Compliance

- The Trust regards all identifiable personal information relating to individuals as confidential;
- The Trust will undertake or commission annual assessments and audits of its compliance with legal requirements;
- The Trust regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise;
- The Trust will establish and maintain policies to ensure compliance with the Data Protection Act, Freedom of Information 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/client information with other agencies, taking account of relevant legislation (e.g. Health and Social Care Act, Crime and Disorder Act, Children Act, etc.)

4.3 Information Security

- The Trust will establish and maintain policies for the effective and secure management of its information assets and resources;
- The Trust will undertake or commission annual assessments and audits of its information and IT security arrangements;
- 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.

4.4 Information Quality Assurance

- The Trust will establish and maintain policies and procedures for information quality assurance and the effective management of records;
- The Trust will undertake or commission annual assessments and audits of its information quality and records management arrangements;
- 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.

5. Incident Management

All Information Governance incidents including breaches of confidentiality, data loss will be managed through the Trust's Incident Reporting Procedure. The Information Governance Team will co-ordinate and feedback where appropriate on all investigations into Information Governance incidents.

6. Information Governance Risk

Incomplete or inaccessible information is a risk to the quality and safety of care for patients/service users. The Information Governance risks are monitored and reviewed as part of the Information Governance Toolkit, the Trust Risk Register and the Information Asset Register and are reported regularly to the Management of Information Governance group, Corporate Governance meeting and through the Information Governance Annual Report to the Board.

7. Training/Awareness

7.1 All staff must

- attend as part of their induction a training session on Information Governance; and
- undertake refresher information governance training either through a facilitated session or e-learning on an annual basis.

7.2. In addition the Information Governance Team will provide training at team meetings at the request of a line manager and support workshops, etc. to increase awareness of Information Governance issues.

7.3 The Information Governance Team will increase awareness to staff through training, iCare; staff bulletins, training bulletins, awareness campaigns, policies, procedures and guidelines in all areas of Information Governance.

8. Monitoring and Auditing

The focus is on sustaining robust Information Governance by:

- Continuing to demonstrate compliance with the key Information Governance standards through achievement of at least level 2 performance in terms of the

NHS Information Governance Toolkit, and ensuring plans are in place to progress beyond this minimum where it has not been achieved;

- Management of Information Group to review key performance indicators (Appendix 2);
- An Information Governance audit utilising the centrally provided audit methodology in Internal Audit's Trust Work Plan.

9. Review

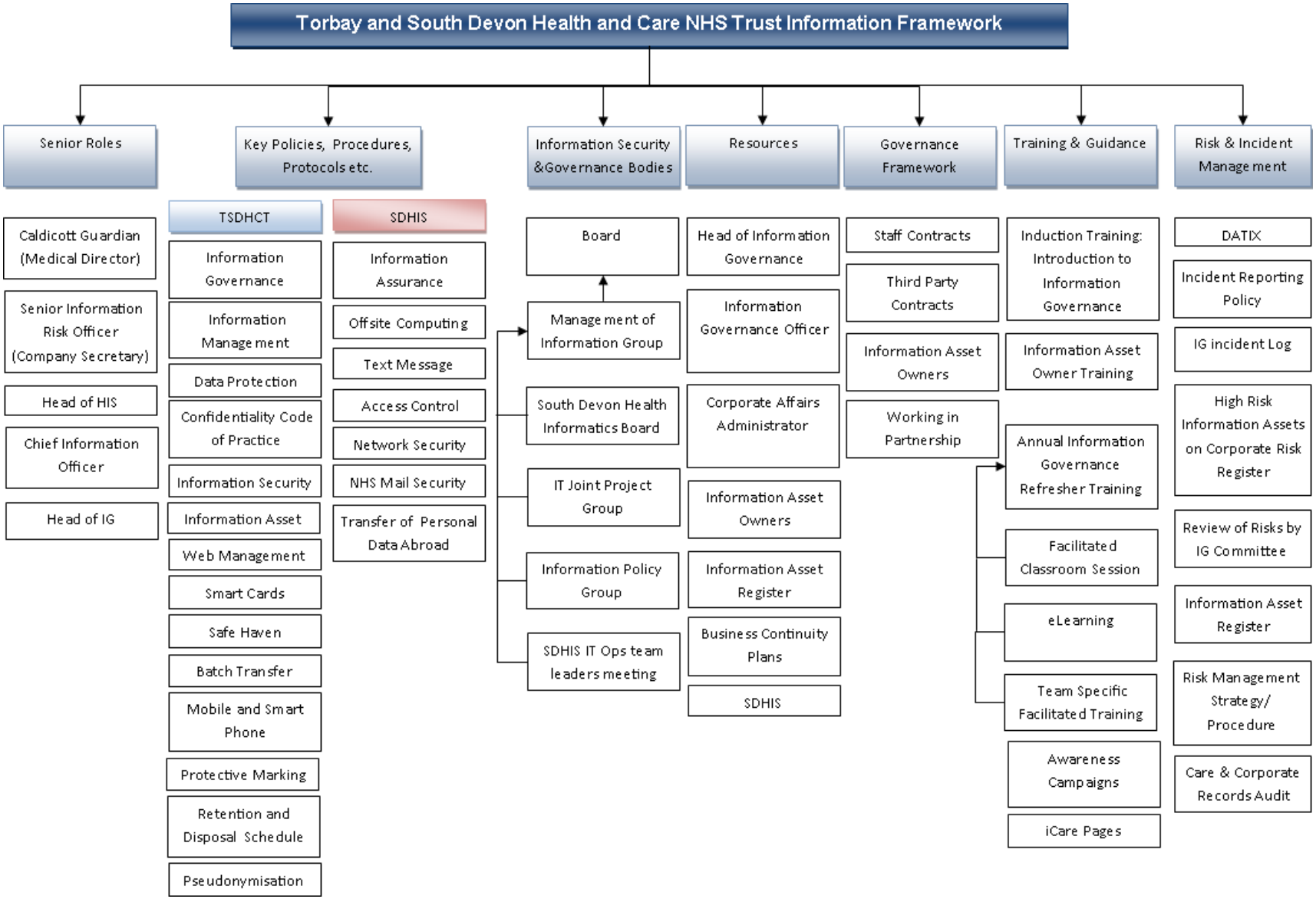
This Policy will be reviewed in two years or earlier if appropriate, to take into account any changes to legislation that may occur, and/or guidance from the Health and Social Care Information Centre and/or the Information Commissioner's Office.

10. Distribution

To all Trust employees via the Staff Bulletin, through training and iCare.

Appendix 1: Information Governance Management Framework
Appendix 2: Information Governance Performance Indicators
Appendix 3: National and Local programmes, Initiatives, Standards and Frameworks which drive the Information Governance Agenda

Appendix 1 – Information Governance Management Framework



Appendix 2 – IG Performance Indicators

	Apr 15	May 15	June 15	July 15	Aug 15	Sept 15	Oct 15	Nov 15	Dec 15	Jan 16	Feb 16	Mar 16	*Total*
Performance Indicators													
Information Governance Toolkit Level 3 (x/39)													
Information Governance Toolkit Level 2 (x/39)													
Information Governance Toolkit Level 1 (x/39)													
Information Governance Toolkit Level 0 (x/39)													
% of NHS Numbers recorded on PARIS (Target 99.00%)													
Number of duplicate records Archived on PARIS													
% of staff trained in IG (Target 95%)													
Incident Reporting													
No of incidents - Severity 2+ (further details in Table 1)													
No of Personal Data related incidents - Severity 0-1 (further details in Table 2)													
Records Management incidents - Severity 0-1 (further details in Table 2)													
Data Management													
No of Batch transfers													
No of boxes archived off site													
No of boxes returned from off site													
No of boxes destroyed off site in line with Retention & Disposal Schedule													
Information Assets													
No of Information Assets													
without an Information Asset Owner													
% of high risk Information Assets													
% of medium risk Information Assets													
% Information Asset Owners trained													
% Paper Assets													
% Electronic Assets													
Requests for Information													
Freedom of Information/ Environmental Information Regulations requests													
Data Protection / Access to Health Records Requests													
% acknowledged with 3 working days													
% responded within legislative timeframe													
Number under Internal Review													
Number under ICO Reviews													

Information Governance Relation Incidents – Breach of Confidentiality/Data Loss

Table 1

Summary of Serious Untoward Incidents involving Personal Data as Reported to the Health and Social Care Information Centre in 2015-16 (Severity Rating 2+)				
Date of incident (month)	**Nature of incident**	**Nature of data involved**	**Number of People potentially affected**	**Notification steps**
n/a				
Further action on information risk				

Table 2

Category	Nature of Incident	Apr 15	May 15	Jun 15	Jul 15	Aug 15	Sep 15	Oct 15	Nov 15	Dec 15	Jan 16	Feb 16	Mar 16	Total
I	Loss of inadequately protected electronic equipment, devices or paper documents from secured NHS premises													
II	Loss of inadequately protected electronic equipment, devices or paper documents from outside secured NHS premises													
III	Insecure disposal of inadequately protected electronic equipment, devices or paper documents													
IV	Unauthorised Disclosure													
V	Other													
TOTAL														

All incidents are classified in terms of severity on a scale of 0-2+ in terms of either/both risk to reputation and risk to individuals in accordance with Health and Social Care Information Centre Incident Reporting Guidance. All incidents are fully investigated and appropriate action taken to mitigate further risks.
Table 1 gives summary details of any incident that have a severity rating of 2+. Table 2 is a summary of incidents with a severity rating of 0-1.

Appendix 3 - National and Local Programmes, Initiatives, Standards and Frameworks which drive the Information Governance Agenda

Data Protection Act 1998
The Act makes provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information.

Data Protection (Subject Access Modification) (Health) Order 2000
This Order provides for the partial exemption from the provision of DPA which confer rights on data subjects to gain access to data held about them of data relating to the physical or mental health or condition of the data subject.

Data Protection (Subject Access Modification) (Social Work) Order 2000
This Order provides for the partial exemption from the provisions of the DPA of certain data where the exercise of rights under the Act would be likely to prejudice the carryout of social work by causing serious harm to the physical or mental health or condition of the data subject or another person.

Freedom of Information Act 2000
An Act that makes provision for the disclosure of information held by public authorities or by persons providing services for them and to amend the DPA 1998 and the Public Records Act 1958; and for connected purposes
DH NHS IG – Checklist for Reporting, Managing and Investigating Information Governance Serious Untoward Incidents 2010 (Last Reviewed April 2012)

DH: NHS Operating Framework for England for 2010/11
The Operating Framework for the NHS for 2010/11 sets out the priorities for the NHS for the year ahead to enable them to begin their planning. The Operating Framework 2010/11 confirms that informatics will be included in operational plans and this document provides guidance on the informatics components of these plans. National expectations for the NHS for delivery of national and local objectives are set out, building on existing investments to strengthen local information and data management.

HSCIC Confidentiality NHS Code of Practice
The Code is a guide to required practice for those who work within or under contract to NHS organisations concerning confidentiality and patients' consent to use their information.

DH: Confidentiality NHS Code of Practice: Supplementary Guidance – Public Interest Disclosures 2010
The guidance is aimed at aiding decisions about disclosures of information in the public interest.

DH: NHS Information Governance Guidance on Legal and Professional Obligations
There is a range of complex legal and professional obligations that limit, prohibit or set conditions in respect of the management, use and disclosure of information and similarly a range of statues that permit or require information to be used or disclosed. This document, which is best practice guidance, outlines the likely impact of these provisions on NHS information but also includes some social care information. This document lists the relevant legal and professional obligations.

DH: Records Management NHS Code of Practice (2006)
The Code is a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. It is based on current legal requirements and professional best practice. The guidance applies to all NHS records and contains details of the recommended minimum retention period for each record type.

DH: Information Security Management Code of Practice (2007)
The Code is a guide to the methods and required standards of practice in the management of information security for those who work within or under contract to, or in business partnership with NHS organisations in England. It is based on current legal requirements, relevant standards and professional best practice and replaces HSG 1996/15 – NHS Information Management and Technology Security Manual.

DH: NHS IG – Information Risk Management – Good Practice Guide 2009
This guidance reflects the Government guidelines and is consistent with the Cabinet Office report on '*Data handling Procedures in Government'*. This also includes guidance on the need for Forensic Readiness Policy and local implementation.

DH: The Caldicott Guardian manual 2010
The manual sets out the role of the Caldicott Guardian within an organisational Caldicott/confidentiality function as a part of broader information governance.

DH NHS IG – Guidance for the Classification markings of the NHS Information 2009
This guidance is provided as good practice to consider in marking the records for which they are responsible.

BS ISO/IEC 2700 Series of Information Security Standards
The ISO/IEC standard provides a useful reference for those wishing to gain a greater understanding of the security controls, or those who wish to become fully compliant with the standard.

Professional Codes of Confidentiality
Professional Codes of Confidentiality from the General Medical Council, the Nursing & Midwifery Council and the British Association of Social Workers.

NIGB: NHS Care Record Guarantee for England
The Guarantee sets out the rules that govern how patient information is used by all organisations providing care for or on behalf of the NHS and what control the patient can have over this.

NIGB: The Social Care Record Guarantee for England
The Guarantee explains to service users how the information they provide to social care staff is used and what control have over this.

Care Quality Commission: Guidance about compliance with the Essential Standards
Outcome 21: Records, sets out the requirement for people's personal records, including medical records, to be accurate and kept safely and confidential.

HM Government: Information Sharing Guidance
Cross Government guidance that aims to provide practitioners with clear guidance about when and how they can share information legally and professionally about the individual they are in contact with.

NHS Litigation Authority: Risk Management Standards
The core of the NHS LA risk management programme is provided by a range of standards and assessments.

NHS Information Standards Board: Health Record and Communication Practice Standards
A set of health record and communication practice standards for team based care, which brings together the standards already in existence and common to GMC, NMC, HPC.

Electronic Social Care Record (ESCR)
This briefing defines the content of an ESCR and outlines the background and current developments in implementation.

The National Archives: Records Management Standards
A set of standards and guidance which covers all aspects of records management. These represent best practice and focus on public record bodies.

Lord Chancellor's Code of Practice on the Management of Records, Section 46 of the Freedom of Information Act
The Code sets out the practices that organisations should follow in relation to the creation, keeping, management and destruction of their records.

Information Governance Toolkit
The IG Toolkit is an online system which allows NHS organisations and partners to assess themselves against Department of Health Information Governance policies and standards. It also allows members of the public to view participating organisations' IG Toolkit assessments.

NHS Constitution – has many commitments on information, some explicit references to IG matters (section 2a; 3b;
You have the right to privacy and confidentiality and to expect the NHS to keep your confidential information safe and secure. (Right - Section 2a)
Your have the right of access to your own health records. These will always be used to manage your treatment in your best interests. (Right - Section 2a)
To protect the confidentiality of personal information that you hold unless to do so would we put anyone at risk of significant harm. (Duty - Section 3b)

Care Quality Commission National Study "The right information, in the right place, at the right time"
"The right information, in the right place, at the right time states "Good information governance means having efficient and effective structures, policies and practices in place to ensure the confidentiality and security of the records of patients and service users." This report places the emphasis on improving the quality of data, keeping information confidential and sharing information effectively. The report also provides recommendations to healthcare providers and commissioners which include: accuracy of patient data should be treated in a similar fashion to that of financial data; review and develop good IG systems as a means of delivering better care; training and development is tailored to particular roles and addresses the different perceptions of risk associated with IG and through World Class Commissioning use the commissioning function as a lever to improve IG in organisations from which we commission care.

DH: The Power of Information: Putting all of us in control of the health and care information we need
This Strategy embraces the changes in information and technology and marks a shift in the way information must drive better health, care and support – to improve service users experience, quality and outcomes of health and care services, putting people truly at the heart of care.

Caldicott2 Review
Following a request from the Secretary of State for Health, Dame Fiona Caldicott carried out this independent review of information sharing to ensure that there is an appropriate balance between the protection of patient information and the use and sharing of information to improve patient care.