Torbay and South Devon NHS
NHS Foundation Trust

Information Governance Management Framework

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 2011	**Next Review Date:**	February 2025
Version:	7.4	**Last Review Date:**	February 2023
Author:	Data Security and Protection Officer		
Directorate:	HIS		
Approval Route: IG Steering Group & IM & T			
Approved By:		**Date Approved:**	
IG Steering Group		February 2023	

Amendment Control/History

Document History Issue	Status	Date	Reason for Change	Authorised
0.1	1st draft	Feb 2011	Submitted to SIRO for comment.	R Scott
1.0	Final	Mar 2011	SIRO	
1.1	DRAFT	Jan 2012	Submitted to IG Steering Group for comments	R Scott
2.1	DRAFT	Jan 2013	Submitted to IG Steering Group for comments	R Scott
3.1	DRAFT	Jan 2014	Submitted to IG Steering Group for comments	R Scott
4.1	DRAFT	Jan 2015	Submitted to IG Steering Group for comments	R Scott
5.1	DRAFT	March 2016	Submitted to IG Steering Group for comments	R Scott
6.1	DRAFT	Jan 2016	Submitted to IG Steering Group for comments	R Scott
7.1	Final	March 2019	New DP regs update	IGSG
7.2	Annual review	April 2021	Annual review	IGSG
7.3	Annual review	February 2022	Annual review	IGSG
7.4	Annual review	February 2023	Annual review	IGSG

Contents

1. Introduction 4
2. Senior Roles 4
3. Key Policies, Procedures and Guidelines 4
4. Key Governance Bodies 5
5. Resources 5
6. Governance Framework 5
7. Training and Guidance 5
8. Incident Management 6
9. Data Protection 6
10. Review 6

1. Introduction

1.1 Robust Information Governance (IG) requires clear and effective management and accountability structures, governance processes, documented policies and procedures, trained staff and adequate resources. The way that Torbay and South Devon NHS Foundation Trust chooses to deliver against these requirements is referred to within the Data Security and Protection Toolkit as the organisation's Information Governance Management Framework.

1.2 This Framework must be documented, approved at the most appropriate senior management level in the organisation (e.g. the Board (or equivalent), senior management team) and reviewed annually.

1.3 The IG Management Framework provides a summary/overview of how the Trust is addressing the IG agenda.

2. Senior Roles

2.1 The Board has appointed the Director of Transformation and Partnerships as the Senior Information Risk Owner (SIRO), a Board level position accountable for information risk. The SIRO is required to report back to the Board on the Information Governance Steering Group's progress and agenda items which may need Board level approval. The SIRO is the Chair of the Information Governance Steering Group.

2.2 The Trust's Caldicott Guardian acts as the conscience of the organisation in relation to patient confidentiality.

2.3 The Trusts Data Protection Officer (DPO) ensures that her organisation processes the personal data of its staff, customers, providers or any other individuals (also referred to as data subjects) in compliance with the applicable data protection rules.

2.4 The Chief Executive has overall accountability for ensuring that the organisation operates in accordance with the law with the support of her subordinates.

3. Key Policies, Procedures and Guidelines

- Information Governance Management Framework
- Information Governance Strategy
- Records Management Strategy
- Information Sharing Strategy
- Information Asset Management Strategy
- Information Governance Policies
- Information Asset Management Policy
- Information Assurance Policy
- Information Management & Technology Policy
- Retention and destruction of corporate records Policy

- Health & Adult Social Care Policies
- Information Governance Guidance
- Information Asset Guidance documents
- Information Governance Procedures
- Information Governance workplan

4. Key Governance Bodies

- Executive Team and Board of Directors – receive reports and direct strategy where appropriate;
- Audit Committee
- Information Governance Steering Group (reports to IM&T);
- Risk Group – tasked with overseeing risk management.

5. Resources

5.1 The key staff involved in the IG agenda below Board of Directors members are as follows:

- Director of Health Informatics Services
- Head of Education
- Company/Corporate Secretary
- DPO - Head of Records, Clinical Coding, Data Protection, FOI, IG
- Data Security and Protection Lead
-
- Information Manager or deputy
- Registration Authority Manager
- Information Asset Support Team Manager
- Information Asset Owners / Administrators; and
- Internal Audit.
- Data Access and Disclosure Office (DADO) & IG Team

6. Governance Framework

6.1 The following list details how responsibility and accountability for IG is cascaded through the organisation:

- staff contracts
- contracts with third parties
- communications and awareness raising
- identification of Information Asset Owners / Administrators and clarification of asset owner responsibilities
- Completion of Data Protection Impact Assessments (DPIA's)
- risk assessments and sharing results of assessments and learning from incidents
- independent audits and
- regular reporting to the Audit Committee, Executive Team and Trust Board of Directors as appropriate

7. Training and Guidance

7.1 This shall be through an annual mandatory training programme for all staff including contractors and temporary staff using an online (local and national) training tool. Training sessions will be available bothe digitally and in person to suit the learner. Training shall be informed by a training needs analysis that is aligned to the priorities of the organisation. The Data Protection and IG staff will be appropriately trained, assessed by the DPO..

8. Incident Management

8.1 The Trust has approved the Information Governance and cyber Security Incident Reporting Procedure which is available on the Trust's Intranet website, held in the Information Governance Procedure book. Raising awareness to staff will be communicated regularly via staff bulletins and Trust Intranet website. External contractors, bank and agency staff, locums and students etc. who do not receive information via the above communication methods will be made aware via the Estates, Procurement and Recruitment departments

9. Data Protection

9.1 Torbay and South Devon NHS Foundation Trust (TSDFT) has a commitment to ensure that all policies and procedures developed act in accordance with all relevant data protection regulations and guidance. This policy has been designed with the UKs current data protection legislation in mind, and therefore provides the reader with assurance of effective information governance practice.

9.2 The UK data protection regime has 7 principles that need following which require that personal data shall be:

1. Processed fairly, lawfully and in a transparent manner.
2. Collected for specified, explicit, and legitimate purposes and not further processed for other purposes, incompatibly with the original purpose.
3. Adequate, relevant and limited to what is necessary in relation to the purposes.
4. Accurate and kept up to date.
5. Kept in a form that permits identification no longer than is necessary.
6. Processed in a way that ensures appropriate security of that personal data.
7. Accountability and responsibility for compliance with the principles

9.3 Have all of the data protection principles been considered in the development or update of this policy? Yes ☒ No ☐

9.4 For more information:

- Contact the Data Access and Disclosure Office on dataprotection.tsdft@nhs.net,
- See TSDFT's Data Protection & Access Policy,
- Visit our Data Protection site on the public internet.

10. Review

10.1 The Information Governance Management Framework will be reviewed annually by the Information Governance Steering Group.