Doncaster and Bassetlaw Teaching Hospitals
NHS Foundation Trust

Information Risk Management Policy

This procedural document supersedes: Information Risk Management Policy - CORP/ICT 21 v.4

Did you print this document yourself?

The Trust discourages the retention of hard copies of policies and can only guarantee that the policy on the Trust website is the most up-to-date version. **If, for exceptional reasons, you need to print a policy off, it is only valid for 24 hours.**

Executive Sponsor(s):	Ken Anderson – Chief Information Officer (CIO) & Senior Information Risk Owner (SIRO)
Author/reviewer: (this version)	Roy Underwood, Data Protection Officer/Head of Information Governance
Date revised:	January 2024
Approved by:	Information Governance Group
Date of approval:	22nd January 2024
Date issued:	28 February 2024
Next review date:	January 2027
Target audience:	Trust-wide

Amendment Form

Version	Date Issued	Brief Summary of Changes	Author	Executive Sponsor
Version 5	January 2024	• Tri-annual review • Amend to meet UK GDPR and DPA 2018 compliance	Roy Underwood Rhona McCleery	Dan Howard
Version 4	21 July 2020	• Tri-annual review • Amend to meet GDPR and DPA 2018 compliance • Amend IG Toolkit SIRI reporting to DSP Toolkit SIRI reporting	Roy Underwood	Ken Anderson
Version 3	19 October 2016	• Tri-annual review • Name change MONITOR → NHS Improvement • Introducing Statutory & Essential Training (SET) for all staff alongside the ongoing historical classroom based DSP training	Roy Underwood	Simon Marsh
Version 2	23 October 2013	• New style format in accordance with CORP/COMM 1. • New sections added: - Roles and Responsibilities - Equality Impact Assessment - Associated Trust Procedural Documents - Definitions - References • Expansion of the Monitoring & Training arrangements • Incorporation of NHS Digital DSP Toolkit Guidance on Serious Incidents Requiring Investigation (SIRIs)	Roy Underwood	Mark Norwood
Version 1	January 2009	This is a new policy	Roy Underwood	Dr E W Jones

Contents

Page No.

1. INTRODUCTION 4
2. PURPOSE 4
3. ROLES AND RESPONSIBILITIES 4
   - 3.1 Chief Executive 4
   - 3.2 Caldicott Guardian (CG) & Senior Information Risk Owner (SIRO) 4
   - 3.3 Data Protection Officer (DPO)/Head of Information Governance 5
   - 3.4 Line Managers 5
   - 3.5 All Staff 5
   - 3.6 Other Authorised Users 5
4. MANAGING INFORMATION RISKS 6
   - 4.1 Policy Statements: 6
5. RISK MANAGEMENT 7
   - 5.1 Objective 7
   - 5.2 Methodology 7
   - 5.3 Reporting 7
   - 5.4 Security review 8
6. MONITORING COMPLIANCE WITH THE PROCEDURAL DOCUMENT 8
7. TRAINING/SUPPORT 8
8. DEFINITIONS 8
9. EQUALITY IMPACT ASSESSMENT 9
10. ASSOCIATED TRUST PROCEDURAL DOCUMENTS 9
11. DATA PROTECTION 10
12. REFERENCES 10

APPENDIX 1 – EQUALITY IMPACT ASSESSMENT - PART 1 INITIAL SCREENING 11

1. INTRODUCTION

This policy is based on generic Information Assurance guidance originally set out by CESG[1] and published in ISO27001. It is written from the perspective of the requirement of the final report on Data Handling Procedures in Government to protect information, including personal information and of 'current data protection legislation' (UK GDPR 2021 & DPA 2018).

2. PURPOSE

The information risk policy defines how the Doncaster & Bassetlaw Teaching Hospitals NHS Foundation Trust (the Trust[2]) and its delivery partners will manage information risk and how its effectiveness will be assessed. In so doing the policy supports the organisation's strategic aims and objectives and NHS Improvement's Compliance Framework (including the Information Governance Toolkit requirements) and should therefore enable employees throughout the delivery chain to identify an acceptable level of risk, beyond which escalation of risk management decisions is always necessary. The policy fits within the organisation's overall business risk framework; information risk need not be managed separately from other business risks.

3. ROLES AND RESPONSIBILITIES

3.1 Chief Executive

The Chief Executive has overall responsibility for security of data in the Trust. This responsibility should be discharged through designated members of staff who have lead responsibility for information security management within the Trust.

3.2 Caldicott Guardian (CG) & Senior Information Risk Owner (SIRO)

The Trust's Caldicott Guardian and SIRO have a particular responsibility for reflecting patients' interests and those of the Trust as a whole regarding the use of all Trust information Assets and they are responsible for how and where Trust Information Assets are stored, managed and shared – where necessary and appropriate - in a safe and secure manner.

[1] http://www.cesg.gov.uk/policytechnologies/assuance/index.shtml
[2] references to "the Trust" includes its delivery partners

3.3 Data Protection Officer (DPO)/Head of Information Governance

The Trust's Data Protection Officer (DPO)/Head of Information Governance (IG) acts as Assistant to the Caldicott Guardian and Deputy to the Trust SIRO and is responsible for providing ongoing guidance to all managers throughout the Trust.

The Trust's DPO/Head of IG and IG Manager will carry out periodic security reviews - as detailed in the Data Security & Protection (DSP) Toolkit - in all areas where information assets are held and managed, and then report findings to the Trust Board via the Audit and Non Clinical Risk Committee (ANCRC).

3.4 Line Managers

Line Managers should ensure all current and future staff are instructed in their DSP responsibilities including Local Standing Orders and Policy on potential personal conflicts of interest, and all policies and procedures concerning confidentiality and information security. They should also ensure that all their staff receive annual mandated DSP training commensurate with their job role and as described in Trust Policy - CORP/ICT 9: Information Governance Policy.

3.5 All Staff

Each employed, contracted and voluntary staff member is personally responsible for ensuring that no breaches of information security result from their actions, and that they receive annual mandated DSP Training commensurate with their job role. All DSP Incidents must be reported on the trust DATIX Incident reporting system, the DPO will then catalogue, risk assess and report further via the DSP Toolkit as necessary. Serious Incidents must be reported on **within 72 hours of the trust becoming aware** that a potentially serious incident has occurred. A serious incident can be downgraded as more information becomes available, but the key is to report as soon as possible to ensure appropriate and timely risk assessment, intervention and additional controls if necessary.

Each staff member (as above) must comply with the Trust's relevant security and confidentiality policies and procedures. Failure to comply with these responsibilities could result in disciplinary action.

3.6 Other Authorised Users

Other NHS and authorised external users are personally responsible for ensuring that no breaches of information security result from their actions and shall comply with the Trust's security policies and procedures.

4. MANAGING INFORMATION RISKS

4.1 Policy Statements:

Managing information risks effectively and in line with current guidance and best practice is an important means of enabling the effective use of data for the public benefit;

Managing information risks supports the business strategy and objectives including where the organisation can influence or satisfy its delivery partners;

The information risk management structure within the organisation applies specific roles and responsibilities – through the SIRO and his Deputy – to named individuals including an agreed approval route for facilitating deviations from the policy;

The Trust's Risk Management Policy: CORP/RISK 30 – Risk Identification, Assessment and Management Policy details the organisation's approach to risk appetite, risk tolerance and the sharing of data) details the risk assessment methodology;

The applicable legal and regulatory requirements and the government's minimum mandatory measures and other policies and guidance are to be used in the management of information risk covering physical, procedural, personal and technical measures;

The SIRO has in place escalation and anonymous reporting procedures for risk management decisions;

The Trust, through its Information Governance Committee (IGC), has sight of the Caldicott Incident Reports, and has agreed plans to introduce the necessary changes in culture to ensure that data is valued, protected and used for the public good. Incidents that are classed as Serious Incidents (SIs) go to the Trust SI panel and hence to board as well as their journey through the DSP Toolkit SIRI process;

The requirements for Data Security & Protection (including Information Risk Management) awareness training are included in the Corporate Statutory & Essential Training (SET) education programme, and individual consequences of failure to apply the organisation's policies and practices are regarded as serious disciplinary issues;

There are published HR policies associated with failure to adopt departmental procedures on handling Trust personal or sensitive data;

Minimum requirements for inspections, reviews (internal and external), monitoring and audit are defined and managed through the NHS on-line DSP Toolkit

External accountability and progress reporting are facilitated through agreed External Audit and DSP Toolkit reporting mechanisms;

Incident reporting – initially through DATIX – recovery, and contingency policy and procedures are published and followed. Significant events may then be reported on to NHSE and the ICO through the DSPT SIRI; Incident Reporting Tool. Serious IG Incidents should be reported on with 24hrs of the facts being reported on DATIX, or otherwise and when necessary. In those cases, a DATIX Event will be reported on retrospectively.

The intent set out within this policy is applicable across the Doncaster & Bassetlaw Teaching Hospitals NHS Foundation Trust and its delivery partners and contains sufficient detail to ensure consistency across the Trust's full range of business environments and functions.

5. RISK MANAGEMENT

5.1 Objective

To identify and counter possible threats – including cyber threats - to the security policies and standards.

5.2 Methodology

All areas where trust information assets are handled will be subject to periodic security reviews by the Information Governance Group and conducted using the DSP Toolkit assertions.

5.3 Reporting

All Information Governance Adverse Incidents are reported on through DATIX/DATIXWeb.

In addition, current data protection legislation requires the Trust to investigate and report (within 72 hours) on all serious DSP incidents/events. The results of any investigation – where appropriate - are then to be reported to NHS Digital through the DSP Toolkit SIRI Tool. Any Incident rated as a 'Serious Level 2 and above Incident' by the tool will be automatically reported on to the ICOs Office. Where the incident is therefore deemed to be a Trust Serious Incident as defined in CORP/RISK 15, then STEIS reporting actions may be appropriate in accordance with the Trust's Corporate Risk Policy.

In all cases, the Trust DPO and/or Deputy must be informed at all times and as soon as possible: dbth.dpo@nhs.net

5.4 Security review

Security reviews can come about because changes to National Policy, the Law, and as a result of actions from local and external adverse Information Management & Technology (IM&T) incidents. Any security reviews will be reported through the Information Governance Committee Minutes to the Audit & Risk Committee (ARC).

6. MONITORING COMPLIANCE WITH THE PROCEDURAL DOCUMENT

The Information Governance Committee will monitor the implementation of these guidelines, and any subsequent revisions, as part of the annual Information Governance Self Assessment during collection of evidence that the correct actions have been carried out.

What is being Monitored	Who will carry out the Monitoring	How often	How Reviewed/ Where Reported to
Staff adherence to the policy	DPO/Head of IG	As alerted by DATIX Adverse Incident/Event reports	Reported to the Information Governance Committee, and then on to ARC for their deliberation and notice to the Trust BoD as necessary

7. TRAINING/SUPPORT

All staff must be appropriately trained in line with DSP Toolkit requirement, in that they will have access to training opportunities, clear policies and guidelines. This is achieved at the DBTH through mandated SET eLearning and scheduled DSP Classroom training sessions. Policies and Procedures are published on the Trust Internet & Intranet/Extranet websites.

The training requirements of staff will be identified through a training needs analysis. Role specific education will be delivered by the service lead.

8. DEFINITIONS

Data Security & Protection **(DSP)**
Equality Impact Assessment **(EIA)**
Audit & Risk Committee **(ARC)**
Senior Information Risk Owner **(SIRO)**
Caldicott Guardian **(CG)**
Personally Identifiable Data **(PID)**

Care Quality Commission **(CQC)**
Serious Incidents Requiring Investigation **(SIRI)**
National Technical Authority for Information Assurance **(CESG)**
General Data Protection Regulation **(GDPR)**
Data Protection Act **(DPA)**
Data Protection Officer **(DPO)**
Information Governance **(IG)**
Information Governance Committee **(IGC)**
Audit and Risk Committee **(ARC)**
Serious Incidents **(SIs)**
Information Commissioners Office **(ICO)**
Strategic Executive Information System **(STEIS)**
Information Management and Technology **(IM&T)**
Statutory & Essential Training **(SET)**

9. EQUALITY IMPACT ASSESSMENT

The Trust aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are disadvantaged over others. Our objectives and responsibilities relating to equality and diversity are outlined within our equality schemes. When considering the needs and assessing the impact of a procedural document any discriminatory factors must be identified.
An Equality Impact Assessment (EIA) has been conducted on this procedural document in line with the principles of the Equality Analysis Policy (CORP/EMP 27) and the Fair Treatment for All Policy (CORP/EMP 4).

The purpose of the EIA is to minimise and if possible remove any disproportionate impact on employees on the grounds of race, sex, disability, age, sexual orientation or religious belief. No detriment was identified. (see Appendix 1).

10. ASSOCIATED TRUST PROCEDURAL DOCUMENTS

CORP/RISK 30 - Risk Identification, Assessment and Management Policy
CORP/RISK 15 - Serious Incident (SI) Policy
CORP/ICT 2 - Information Management and Technology (IM&T) Security Policy
CORP/ICT 9 - Information Governance Policy
CORP/ICT 7 – Data Protection Policy
CORP/EMP 4 – Fair Treatment for All Policy
CORP/EMP 27 – Equality Analysis Policy

11. DATA PROTECTION

Any personal data processing associated with this policy will be carried out under 'Current data protection legislation' as in the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR) 2021.

For further information on data processing carried out by the trust, please refer to our Privacy Notices and other information which you can find on the trust website: https://www.dbth.nhs.uk/about-us/our-publications/information-governance/

12. REFERENCES

- Data Protection Act (2018)
- UK General Data Protection Regulation (2021)
- Access to Health Records Act (1990)
- Copyright Patents and Designs Act (1988)
- Computer Misuse Act (1990)
- Public Records Act (1958)
- Freedom of Information Act (2000)
- Common Law Duty of Confidentiality
- NHS Confidentiality Code of Practice
- DSP Toolkit Assertions
- Reporting incidents post the adoption of GDPR 25 May 2018 and NIS Directive 10 May 2018 through the DSP Toolkit

APPENDIX 1 – EQUALITY IMPACT ASSESSMENT - PART 1 INITIAL SCREENING

Service/Function/Policy/Project/ Strategy	Division/Executive Directorate and Department	Assessor (s)	New or Existing Service or Policy?	Date of Assessment
Information Risk Management Policy – CORP/ICT 21 v.5	Digital Transformation Directorate	Roy Underwood	Existing	January 2024

1) Who is responsible for this policy? Name of Division/Directorate: Digital Transformation Directorate

2) Describe the purpose of the service / function / policy / project/ strategy? Trust-wide Information Governance Policy

3) Are there any associated objectives? Compliance with GDPR, the Data Protection Act 2018 & Confidentiality Legislation

4) What factors contribute or detract from achieving intended outcomes?

5) Does the policy have an impact in terms of age, race, disability, gender, gender reassignment, sexual orientation, marriage/civil partnership, maternity/pregnancy and religion/belief? No

- **If yes, please describe current or planned activities to address the impact** [e.g. Monitoring, consultation]

6) Is there any scope for new measures which would promote equality? No

7) Are any of the following groups adversely affected by the policy?

Protected Characteristics	Affected?	Impact
a) Age	No	
b) Disability	No	
c) Gender	No	
d) Gender Reassignment	No	
e) Marriage/Civil Partnership	No	
f) Maternity/Pregnancy	No	
g) Race	No	
h) Religion/Belief	No	
i) Sexual Orientation	No	

8) Provide the Equality Rating of the service / function /policy / project / strategy – tick (✓) outcome box

Outcome 1 ✓	Outcome 2	Outcome 3	Outcome 4

If you have rated the policy as having an outcome of 2, 3 or 4, it is necessary to carry out a detailed assessment and complete a* **Detailed Equality Analysis form in Appendix 4

Date for next review: January 2027

Checked by: **Date:**