Doncaster and Bassetlaw Teaching Hospitals
NHS Foundation Trust

Information Governance Policy

This procedural document supersedes: CORP/ICT 9 v.5 – Information Governance Policy

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):	Chief Information officer (CIO) and Senior Information Risk Owner (SIRO)
Name of author	Roy Underwood – Data Protection Officer David Linacre – IT Ops Security & Continuity Manager
Date revised	June 2021
Approved by (Committee/Group)	Information Governance Committee
Date of approval	28 June 2021
Date issued	16 September 2021
Review date	April 2024
Target audience:	Trust-wide

Amendment Form

Version	Date Issued	Brief Summary of Changes	Author
Version 6	16 Sept 2021	• Periodic review • Change references from Care Groups to Divisions • Ensure that the policy is UK GDPR 2021/DPA 2018 compliant defined as 'current Data Protection Legislation'	Data Protection Officer (DPO) Head of IT Ops/Digital
Version 5	Sept 2018	• Periodic review, changes to Policy Format, and to Monitoring detail • Change references from Care Groups to Divisions • Ensure that the policy is GDPR/DPA 2018 compliant defined as 'current Data Protection Legislation' • Introducing the Data Security & Protection (DSP) Toolkit as a direct replacement for the outgoing Information Governance (IG) Toolkit v14	Data Protection Officer (DPO)
Version 4	April 2015	• Periodic review, changes to Policy Format, and to Monitoring detail • Change references from CSUs to Care Groups	Head of Information Governance
Version 3	December 2011	• Change of reporting committee name to the Trust Audit & Non Clinical Risk Sub-Committee • New Serious Incident (SI) Reporting section • Tri-Annual review • New reference to the Information Governance Framework • IG Training requirements for all staff • New section on monitoring compliance	Head of Information Governance
Version 2	July 2008	• Changes to Information Governance Toolkit Standard 107 • Changes to reporting authority • Reference to CORP/ICT 20 – Bulk Data Transfer (BDT) Policy	Head of Information Governance

Contents

Page No.

1 POLICY AIM

The aim of this policy is to provide the Doncaster & Bassetlaw Teaching Hospitals NHS Foundation Trust with a simple framework through which the elements of Information Governance will be met.

2 POLICY PRINCIPLES

The Trust fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about patients and staff and commercially sensitive information[1]. The Trust also recognises the need to share patient information with other health organisations and other agencies in a controlled manner consistent with the interests of the patient and, in some circumstances, the public interest.

The Trust believes that appropriate access to accurate, timely and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of all clinicians and managers to ensure and to promote the quality of information and to actively use information in decision-making processes.

There are four interlinked strands to the scope of the Information Governance policy:

- Openness
- Legal compliance
- Information security and confidentiality
- Quality assurance

2.1 Openness

- The Trust recognises the need for an appropriate balance between openness and confidentiality in the management and use of information.
- Information will be defined and where appropriate kept confidential, underpinning the principles contained in the recommendations of the Caldicott Committee and the regulations embedded in current Data Protection Legislation. Non-confidential information on the Trust and its services will be available to the public through a variety of means, in line with the Trust's code of openness. Work is ongoing to ensure continued compliance with the Freedom of Information Act 2000 through the continuous update of a publication scheme.
- Patients will have access to information relating to their own health care, options for treatment and their rights as patients.

[1] Information Governance Framework

- There will be clear procedures[2] and arrangements for handling queries from patients and the public.
- The Trust will have clear procedures and arrangements for liaison with the press and broadcasting media.
- Integrity of information will be developed, monitored and maintained to ensure that it is appropriate for the purposes intended.

2.2 Legal Compliance

- The Trust regards all identifiable personal information relating to patients as confidential. Compliance with legal and regulatory framework and the recommendations of the Caldicott Committee will be achieved, monitored and maintained.
- 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 current Data Protection Legislation, the Human Rights Act 2018, the common law duty of confidentiality, and the Freedom of Information Act 2000.
- Awareness and understanding of all staff with regard to responsibilities will be assessed and appropriate training and awareness provided. Some form of annual Data Security and Protection (DSP) Training is now mandated for all Trust staff.

2.3 Information Security

- The Trust will establish and maintain policies for the effective and secure management of its information assets and resources[3].
- The Trust will undertake or commission 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. In addition, The Head of Information Governance, on behalf of the Senior Information Officer (SIRO) is responsible for informing the Strategic Health Authority of any category 3 - 5 information security incidents[4].

[2] Trust Freedom of Information Policy CORP/ICT 15
[3] Trust IM&T Security Policy CORP/ICT 2
[4] CORP/RISK 15: SERIOUS INCIDENTS (SI) Policy, Para 6.7

2.4 Information Quality Assurance

- The Trust will establish and maintain policies and procedures for information quality assurance and the effective management of records[5].
- The Trust will undertake or commission assessments and audits of its data quality and records management arrangements.
- Managers are expected to take ownership of, and seek to improve, the quality of information within their services.
- Wherever possible, information quality should be assured at the point of collection.
- The Trust will promote data quality and effective records management through policies, procedures/user manuals and training.

3 RESPONSIBILITIES

The Information Governance Committee is responsible for coordinating Information Governance Management across the organisation. This Committee reports to the Trust's Audit & Risk Committee (ARC).[6]

Managers within the Trust are responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance.

All staff, whether permanent or temporary and contractors are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with these on a day to day basis.

4 YEAR ON YEAR IMPROVEMENT PLAN AND ASSESSMENT

An assessment of compliance with the assertions made within the DSP Toolkit (DSPT), will be undertaken each year. Annual DSPT progress and Internal Audit reports and the proposed Information Governance Assurance Framework (IGAF) will be presented to the Trust Board of Directors – through the ARC - for approval. The requirements are grouped into the following Information Governance initiatives:

- Confidentiality
- Data Protection
- Cyber Security
- Freedom of Information
- Registration Authority – for Smartcards
- Information Quality Assurance

[5] Trust Information Records Management - Code of Practice CORP/ICT 14
[6] The Audit & Non Clinical risk sub-Committee is a formal sub-committee to the Trust Board of Directors

5 SERIOUS INCIDENT (SI) REPORTING[7]

5.1 Identifiable Data

There is no simple definition of a serious incident. What may at first appear to be of minor importance may, on further investigation, be found to be serious and vice versa. As a guide, any incident involving the actual or potential loss of personal information that could lead to identity fraud or have other significant impact on individuals should be considered as serious. This definition applies irrespective of the media involved and includes both loss of electronic media and paper records.

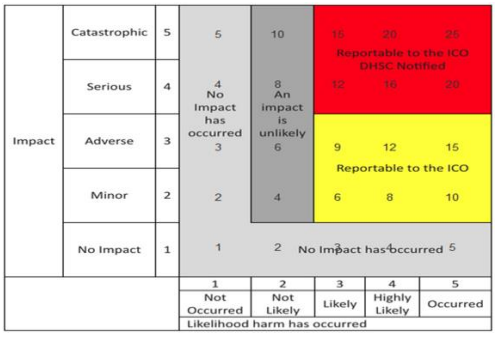
5.2 Immediate Response to Serious Untoward Incident

The Trust has robust policies in place to ensure that appropriate senior staff are notified immediately of all incidents involving data loss or breaches of confidentiality. The Trust use the Datix-Web Application to manage any and all incidents.

Where significant incidents occur out of hours, arrangements are in place to ensure on-call Directors or other nominated individuals are informed of the incident and take action to inform the appropriate contacts.

5.3 Assessing the Severity of the Incident

The immediate response to any incident and the escalation process for reporting and investigating this will vary according to the severity of the incident. The Serious Incidents Requiring Investigation – the DSP Toolkit SIRI process – which may attract the ICOs attention, must be completed – under current Data Protection Legislation - within 72 hours following any reported incident. This is where the incident is likely to attain a **YELLOW** or **RED** score within the SIRI algorithm.



5.4 Complete the Information Required for STEIS

Reporting incidents – STEIS will be used for reporting all SIs and an initial report should be made as soon as possible and no later than within 24 hours of the incident or first becoming aware of the incident. Further information will become available as the investigation takes place and STEIS should be regularly updated as appropriate.

[7] Checklist for Reporting, Managing and Investigating Information Governance Serious Untoward Incidents (Gateway Ref: 13177)

The relevant Clinical Commissioning Group (CCG)'s monitor STEIS, and will therefore be aware of all DSP Toolkit reported SIs

Ensure that the following are included in the report:

- Date, time and location of the incident
- Type of Incident: "Confidential Information Leak" (NB this may be subject to change as improvements to STEIS data incident reporting are being pursued)
- Contact details for local incident manager
- Confirmation that appropriate and documented incident management procedures are being followed and that disciplinary action will be invoked where appropriate following the investigation
- Description of what happened:
    - Theft, accidental loss, inappropriate disclosure, procedural failure etc.
    - The number of patients/staff (individual data subjects) involved
    - The number of records involved
    - The media (paper, electronic) of the records
    - If electronic media, whether encrypted or not
    - The type of record or data involved and sensitivity
    - Whether the SUI is in the public domain
    - Whether the media (press etc.) are involved or there is a potential for media interest
    - Whether the SUI could damage the reputation of an individual, a work-team, an organisation or the NHS as a whole
    - Whether there are legal implications for the trust
    - Initial assessment of level of SUI (see table in Para 5.3 above).
    - Whether the following have been notified (formally or informally):

        - ✓ Data subjects
        - ✓ Head of Information Governance
        - ✓ Caldicott Guardian
        - ✓ Senior Information Risk Owner (SIRO)
        - ✓ Chief Executive
        - ✓ Accounting Officer
        - ✓ Information Commissioner for SUI level 3 and above
        - ✓ Police, Counter Fraud Branch, etc
        - ✓ Relevant Clinical Commissioning Group (CCG)
        - ✓ NHSD

- Immediate action taken, including whether any staff have been suspended pending the results of the investigation.

6 TRAINING

All staff receive annual SET Information Governance awareness and training as part of their induction and subsequently as part of a rolling programme.[8]

Data Security & Protection (IG) Training & Education is now **MANDATORY** for **ALL** Trust staff[9]. The Trust has a comprehensive and embedded annual SET IG Training philosophy.

All staff, including new starters, locum, temporary, student and contract staff members to complete (or to be in the process of completing) mandated IG training within the Statutory & Essential Training (SET) regime, or an equivalent classroom or work based session, both are entirely based on the Data Security & Protection (DSP) Toolkit Training Materials, and successful completion of the training will be recorded on their ESR Training Record[10].

At the Trust Welcome Session, all staff will be reminded – as will their managers – of the need to complete their SET IG training compliance as soon possible following that Welcome Session, and certainly within 1 month:

7 REVIEW

The Information Governance Policy will be reviewed every three years. Regular reports are provided to the ACR Committee through the Information Governance Committee minutes and other significant papers and reports as appropriate.

8 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)

---

[8] NHS Chief Executive Information Governance letters and directives Dec 07 – June 08

[9] Information Governance Policy: CORP/ICT 9

[10] Some staff, like Volunteers and Locums etc, may not have an ESR training record however, that does not mean that they are excluded from the same levels of training expected of 'employed staff' who have the same or similar access to the Trust's Confidential and Sensitive Information Assets

9 MONITORING COMPLIANCE WITH PROCEDURAL DOCUMENT

The Information Governance Group will monitor compliance within its overall Data Security & Protection (DSP) requirements under NHS Digital's DSP Toolkit Compliance Framework.

What is being Monitored	Who will carry out the Monitoring	How often	How Reviewed/ Where Reported to
• Adverse IG Incidents • Freedom of Information requests • Health records management	The Trust Information Governance Committee (IGC)	Monthly – through the IGC Agenda and Minutes	The Trusts • Information Governance Committee • Audit & Risk Committee (ARC)

10 ASSOCIATED TRUST PROCEDURAL DOCUMENTS

CORP/EMP 4 – Fair Treatment for All Policy
CORP/EMP 27 – Equality Analysis Policy
CORP/ICT 2 – Information Management and Technology (IM&T) Security Policy
CORP/ICT 14 – Information Records Management – Code of Practice
CORP/ICT 15 – Freedom of Information (FOI) Policy
CORP/ICT 21 – Information Risk Management Policy
CORP/RISK 15 – Serious Incidents (SI) 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 (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

Caldicott Report
Human Rights Act 2018
Data Protection Act 2018
General Data Protection Regulation (UK GDPR 2021)
Freedom of Information Act 2000
NHS Digital: Data Security & Protection 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 Governance Policy - CORP/ICT 9 v.6	Digital Transformation	Roy G Underwood	Existing Policy	18/06/2021

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

2) Describe the purpose of the service / function / policy / project/ strategy? Who is it intended to benefit? To embed IG in the organisation

3) Are there any associated objectives? GDPR/Data Protection Act 2018/NHS Digital Code of Practice for Records Management

4) What factors contribute or detract from achieving intended outcomes? Information Governance Training & Education

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: April 2024

Checked by: Head of IT Ops & Digital **Date:** 28/06/2021