Doncaster and Bassetlaw Hospitals NHS
NHS Foundation Trust

Information Risk Management Policy

This procedural document supersedes: Information Risk Management Policy - CORP/ICT 21 v.2

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.**

Author/reviewer: (this version)	Roy Underwood - Information Governance Lead
Date revised:	August 2016
Approved by:	Information Governance Group
Date of approval:	4 October 2016
Date issued:	19 October 2016
Next review date:	June 2019 **– (extended to June 2020)**
Target audience:	Trust-wide

Amendment Form

Version	Date Issued	Brief Summary of Changes	Author
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 IG training	R Underwood S 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 HSCIC IG Toolkit Guidance on Serious Incidents Requiring Investigation (SIRIs)	R Underwood
Version 1	January 2009	This is a new policy	R Underwood

Contents

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.

2. PURPOSE

The information risk policy defines how the Doncaster & Bassetlaw 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 Head of Information Governance

The Trust's Head of Information Governance acts as Assistant to the CG and Deputy to the Trust SIRO, and is responsible for providing ongoing guidance to all managers throughout the Trust.

The Trust's Head of Information Governance will carry out periodic security reviews - as detailed in the IG 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 security and IG 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 IG training commensurate with their job role and as described in Trust Policy CORP/ICT 9.

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 IG Training commensurate with their job role.

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 Information governance strategy[3] (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 Group (IGG), has agreed plans to introduce the necessary changes in culture to ensure that data is valued, protected and used for the public good;

The requirements for Information Governance (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 Information Governance Toolkit and the Trust's responsibilities to MONITOR;

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

Incident reporting, recovery and contingency policy and procedures are published and followed;

The intent set out within this policy is applicable across the Doncaster & Bassetlaw 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.

[3] CORP/ICT 16 Information Governance Strategy

5. RISK MANAGEMENT

5.1 Objective

To identify and counter possible threats to the security policies and standards.

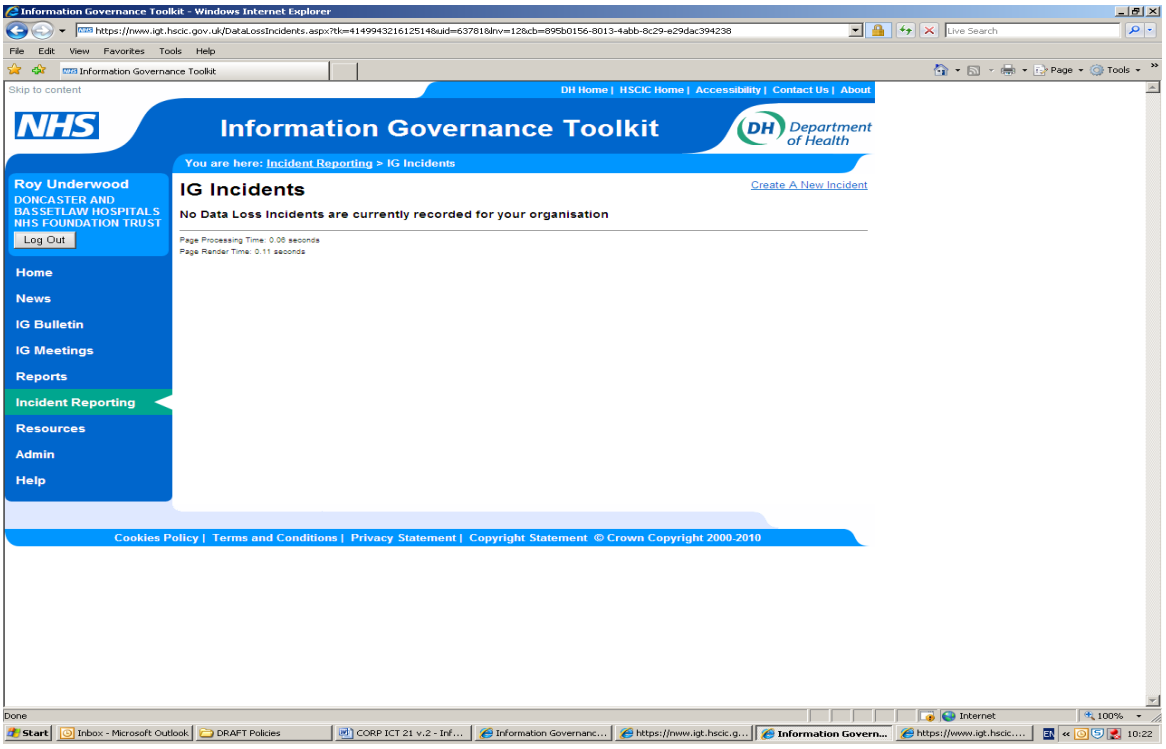
5.2 Methodology

All areas where trust information assets are handled will be subject to periodic security reviews by the Trust CQC and Information Governance Groups and conducted using the IG Toolkit and CQC Outcome 21 compliance measures.

5.3 Reporting

Information Governance Adverse Incidents are reported on through DATIX/DATIXWeb. Serious Incidents must be reported within 24hours.

In addition, from July 2013 the Information Governance Toolkit Standard 302 requires the Trust to carry out a formal management process they have titled Serious Incidents Requiring Investigation (SIRIs). The results of any investigation – where appropriate, are then to be reported using an on-line tool. Any Incident rated as a Serious Incident by the tool will also be reported on through the Trust's normal SI/STEIS reporting process



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 IM&T incidents. Any security reviews will be reported through the Information Governance Group Minutes to the Audit & Non Clinical Risk sub Committee (A&NCRsC).

6. MONITORING COMPLIANCE WITH THE PROCEDURAL DOCUMENT

The Information Governance Group 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	Head of IG	In line with CQC Mock Inspections As alerted by Adverse Incident reports	Report to the IG Group through the Annual IG Report to ANCRC

7. TRAINING/SUPPORT

All staff must be appropriately trained in line with IG Toolkit requirement standard 112, in that they will have access to training opportunities, clear policies and guidelines. This is achieved through mandated SET eLearning and scheduled IG Classroom training sessions. Policies and Procedures are published on the Trust Internet & Intranet websites.

8. DEFINITIONS

Equality Impact Assessment **(EIA)**
Audit & Non Clinical Risk sub Committee **(A&NCRsC)**
Senior Information Risk Owner **(SIRO)**
Caldicott Guardian **(CG)**
Personally Identifiable Data **(PID)**
Care Quality Commission **(CQC)**

9. EQUALITY IMPACT ASSESSMENT

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 Incidents (SI) Policy
CORP/ICT 2 - Information Management and Technology (IM&T) Security Policy
CORP/ICT 9 - Information Governance Policy
CORP/ICT16 - Information Governance Strategy

11. REFERENCES

- Data Protection Act (1998)
- 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
- Checklist Guidance for Reporting, Managing and Investigating Information Governance Serious Incidents Requiring Investigation (SIRIs) - DoH 1st June 2013
- Information Governance Toolkit Standards
- EU General Data Protection Regulation 2016

APPENDIX 1 – EQUALITY IMPACT ASSESSMENT - PART 1 INITIAL SCREENING

Service/Function/Policy/Project/ Strategy	Care Group/Executive Directorate and Department	Assessor (s)	New or Existing Service or Policy?	Date of Assessment
Information Risk Management Policy	Medical Director	Roy Underwood	Existing	4 October 2016

1) Who is responsible for this policy? Name of Care Group/Directorate: Corporate - Medical Director

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

3) Are there any associated objectives? Compliance with Data Protection Act 1998 & 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: June 2019

Checked by: Roy Underwood **Date: 4 October 2016**