Doncaster and Bassetlaw Hospitals NHS
NHS Foundation Trust

Bulk Data Transfer Guidelines

This procedural document supersedes: CORP/ICT 20 v.2 – Bulk Data Transfer.

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. • Introduction amended • Amendment to Head of IG responsibilities • Introducing the EU's General Data Protection Regulation 2016 • Revised BDT Matrix	R Underwood
Version 2	January 2013	• New style format in accordance with CORP/COMM 1. • New sections added: - Equality Impact Assessment - Associated Trust Procedural Documents - Definitions - References • FTP section changed to Direct Electronic Transfer	R Underwood
Version 1	January 2009	This is a new policy	R Underwood

Contents

1. INTRODUCTION

The NHS, has directed that there should be no transfers of unencrypted person identifiable data held in electronic format across the NHS. This is the default position to ensure that patient and staff personal data are protected. Any data stored on a PC or other removable device in a non-secure area or on a portable device such as a laptop, PDA or mobile phone should also be encrypted. This is also now a requirement across all public sector.

2. PURPOSE

This guidance document is in the format of the standard Trust procedure for Information Governance for common approach and consistency, and to include all of the mandatory elements of such documentation as agreed by the Information Governance Group. It incorporates DH guidance.

3. ROLES AND RESPONSIBILITIES

3.1 Chief Executive

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

3.2 Caldicott Guardian/Senior Information Risk Owner (SIRO)

The Trust's Caldicott Guardian and SIRO have a particular responsibility for reflecting patients' interests regarding the use of patient identifiable information. The SIRO in particular is responsible for ensuring that patient identifiable information is stored and shared in an appropriate and secure manner.

3.3 Head of Information Governance

The Trust's Head of Information Governance is responsible for providing updated guidance to all managers throughout the Trust. The Trust's Head of Information Governance will carry out periodic security reviews in all areas where trust patient identifiable information is transferred in bulk, reporting findings to the Trust Board via the Controls Assurance sub-Committee.

Some information transfers are necessarily ad-hoc in their nature. The Head of Information Governance must always be consulted - wherever practical - in the approval of all data transfers involving 'bulk' personal data.

3.4 Line Managers

Managers should ensure all current and future staff are instructed in their security and IG responsibilities including Standing Orders and policy on potential personal conflicts of interest, and all policies and procedures concerning confidentiality and information security.

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. 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. LEGAL AND PROFESSIONAL OBLIGATIONS

All NHS records and most information are Public Records under the Public Records Acts. The Trust will take actions as necessary to comply with the legal and professional obligations set out in the Information Security Management: NHS Code of Practice.

The key statutory requirement for NHS compliance with Information Security Management principles, is the Data Protection Act 1998 and in particular its seventh principle.

The Trust has legal obligations to maintain security and confidentially, in particular in accordance with the following:

Data Protection Act (1998)
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
any new legislation affecting records management – such as the recently published EU General Data Protection Regulation 2016 - as it arises.

5. RISK MANAGEMENT

5.1 Objective

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

5.2 Methodology

All areas where trust patient identifiable information is taken off site will be subject to periodic security reviews by the Information Governance Group and conducted using the IG Toolkit and with specific reference to ISO/ISE 27001

The Trust has a corporate risk management strategy[1] and procedures in place.

5.3 Reporting

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 Committee (ANCRC).

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	As and when requests are made to transfer data. As alerted by the weekly reports of downloads to USB devices through the Network reporting functionality	Report to the IG Group through the Annual IG Report to A&NCRsC

[1] Risk Management Strategy CORP/RISK 10

7. GUIDELINES

Good Practice Guidelines are provided for the transfer of bulk person identifiable data (PID) as follows:

- **Moveable media**
  - USB Memory Sticks & Pen Drives
  - Tapes
  - Floppy discs
  - Removable hard discs
  - Laptop & handheld computers
  - Optical discs – DVD & CD-rom
  - Solid state memory cards

Bulk Data Transfer Matrix

Electronic devices							
Organisationally sanctioned transfer of removable media containing personal data	RDaSH	CCGs	DMBC	HMP	Other NHS Trusts	GP	3rd Parties
DBHFT	**Encrypt**	**Encrypt**	**WZ**	**WZ**	**Encrypt/ WZ/CG**	**Encrypt**	**Encrypt**
eMail							
Organisationally sanctioned transfer of email containing personal data	RDaSH	DPCT	DMBC	HMP	Other NHS Trusts	GP	3rd Parties
DBHFT	**NHSMail**	**NHSMail**	**CG**	**CG**	**NHSMail**	**NHSMail**	**CG**
Normal Mail							
(Letters, Med Recs etc) >50 records = Bulk Data Transfer (BDT)	RDaSH	DPCT	DMBC	HMP	Other NHS Trusts	GP	3rd Parties
DBHFT	**MV**	**MV**	**NM**	**NM**	**NM**	**MV**	**CG**

Key:
Encrypt - 256k SSL Encryption
WZ - Winzipped [Document/s] Password Protected
CG - Risk Assessment & Caldicott Guidance - from Head of Information Governance on a case by case basis
MV - RDaSH Mail Van
SM - Normal Mail

- **Electronic:** Transfer of bulk data via Direct Electronic Transfer covers all of the various mechanisms that allow the DBHFT to safely and securely share information with other organisations. The transfer must be authorised, and carried out over secure or encrypted channels (ordinary FTP isn't secure). Some examples would include Secure Web-based transfers, NHS Commissioning Data Sets (CDS) and other Secure File Transfer Protocol (SFTP) mechanisms.

- **E-Mail:** The trusts preferred E-Mail medium for the authorised transfer of patient data is **NHS Mail** which is encrypted end-to-end. The Use of the Internet and E-Mail Policy - CORP/ICT 26 also allows the use of Trust E-Mail where some files may need to be appropriately password protected.

- **Hard Copy:** The bulk data transfer of hard copy documents should in the main be handled by the Trust's inter-site NHS Mail Service. On occasion where it is necessary to mail personal data documents – in bulk – then that posting process must be very carefully considered and agreed with the Care Group managers or the Head of Information Governance. Senders should always consider the relative merits and costs of registered and recorded delivery, and the use of professional courier services.

8. TRAINING/SUPPORT

Ensure that all staff involved in data transfer are appropriately trained and have access to clear policies and guidelines. This is achieved through Statutory & Essential to role Training (SET) programs managed by the Education Centre and the Head of Information Governance.

9. DEFINITIONS

Equality Impact Assessment (EIA)
Audit & Non Clinical Risk Committee (ANCRC)
Senior Information Risk Owner (SIRO)
Personally Identifiable Data (PID)
Secure File Transfer Protocol (SFTP)
Commissioning Data Sets (CDS)

10. 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).

11. ASSOCIATED TRUST PROCEDURAL DOCUMENTS

Risk Identification, Assessment and Management Policy - CORP/RISK 30
Use of the Internet and E-Mail Policy - CORP/ICT 26

12. REFERENCES

Data Protection Act (1998)
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
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
Bulk Data Transfer Guidelines	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**