Doncaster and Bassetlaw Hospitals NHS
NHS Foundation Trust

Please Note: This policy is currently under review and is still fit for purpose.

Confidentiality Code of Conduct

This procedural document supersedes: CORP/ICT 10 v.3 – Confidentiality Code of Conduct

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.**

Name and title of author/reviewer: (this version)	Roy G Underwood, Head of Information Governance
Date revised:	March 2015
Approved by (Committee/Group):	Information Governance Group
Date Approved:	24 March 2015
Date issued:	1 April 2015
Next Review Date	March 2018 **– extended to June 2020**
Target audience:	Trust-wide

Amendment Form

Version	Date Issued	Brief Summary of Changes	Author
Version 4	1 April 2015	• Periodic review with changes to Policy Layout and Monitoring arrangements • Change references from CSUs to Care Groups	Head of Information Governance
Version 3	May 2012	• Changes to Information Governance Toolkit Standards in v10 (2012) • WPR14452: Your Health Record • Requests by individuals and 3rd Parties to access patient records • Incident Reporting including SI's and the use of STEIS: Strategic Executive Information System • Training • EIA process • Monitoring arrangements	Head of Information Governance
Version 2	October 2008	• Changes to Information Governance Toolkit Standard • Changes to reporting authority • Reference to CORP/ICT 20 – Bulk Data Transfer (BDT) Policy • Made reference to the Patient's Charter for England 1996 – page 5 • Reference to Bassetlaw PCT Information Sharing Protocol – page 6	Head of Information Governance

Contents

1. INTRODUCTION

Much of our work involves us in one way or another, whether on or off of any of the Trust's premises, in having access to confidential and/or sensitive information. Often this can be personal information about staff or patients. We trust our staff to respect these confidences. It is very important. We have produced this Code of Conduct in order to reinforce not only to you, but also to others with whom we do our work, how seriously we treat this matter.

This Code of Conduct also binds our staff to comply with the Statutory Requirements which are;

i) The Data Protection Act 1998

ii) Copyright, Designs and Patents Act 1988

iii) Computer Misuse Act 1990

iv) Health Records Act 1990

2. PRINCIPLES OF CONFIDENTIALITY

In accordance with the Data Protection & Caldicott Principles, patients have a right to expect that a doctor, nurse or other members of our Health Care Teams will not disclose any personal information that is learnt during the course of their professional duties, unless the patient gives their permission or statute permits otherwise. Without assurances about confidentiality patients may be reluctant to give information which is needed in order to provide good care. For these reasons:

- When you are responsible for confidential information you must make sure that the information is effectively protected against improper disclosure when it is 'processed' i.e. manipulated, disposed of, stored, transmitted or received etc;
- When patients give consent to the disclosure of information about them, you must make sure they understand what will be disclosed, the reasons for disclosure, and the likely consequences[1];
- You must make sure that patients are informed whenever information about them is likely to be disclosed to others involved in their health care, and that they have the opportunity to withhold permission. They may also request this consideration after death, so it is very important that access is through the proper channels where staff understand the process;
- You must respect requests by patients that information should not be disclosed to third parties, save in exceptional circumstances (for example, where the health or safety of others would otherwise be at serious risk);

[1] WPR14452: Your Health Record

- If you disclose confidential information you should release only as much information as is necessary for the purpose[2]. If it is appropriate to share information gained in the course of your work with other health or social work practitioners, you must make sure that as far as is reasonable, the information will be kept in strict professional confidence and used only for the purpose for which the information was given (shared);

- If you decide to disclose confidential information, you must be prepared to explain and justify[2] your decision;

- You must abide by these principles in perpetuity (forever!)

3. GUIDANCE ON THE USE AND PROTECTION OF PERSONAL INFORMATION

3.1 People expect that information about them will be treated as confidential.

3.2 "Everyone working for the NHS is under a legal duty to keep your records confidential". (The Patient's Charter for England 1996).

3.3 Personal information should be anonymised or encrypted wherever possible if it is being moved and it is in electronic format.

3.4 Any personal information held on a computer system is safeguarded by the Data Protection Act. No computerised databases holding personal information should be created without registration[3] under this Act. The Caldicott Guardian and the Head of Information Governance are responsible for maintaining these registrations.

3.5 The unauthorised passing on of personal information by any member of staff is a serious matter, warranting consideration of disciplinary action and possibly risking legal action by others.

3.6 Care should be taken to ensure that unintentional breaches of confidence do not occur, e.g.:

- Do not leave files/computer terminals unattended/unsecured
- Double check to avoid transmitting information to the wrong person or fax machine[4]
- Do not allow sensitive conversations to be overheard
- Guard against people seeking information by deception.
- Do not share your Username & Password or Smartcard & PIN
- Log out or Lock your screen down when leaving your desk for any length of time; don't forget to **save** your work **before** you lose it.

[2] Caldicott et al:1997
[3] Trust Policy: CORP/ICT 3
[4] Safe Haven Guidelines: CORP/ICT 8

3.7 Even if names and addresses are removed, the combination of date of birth and postcode, for example, can allow individuals to be identified.

3.8 Personal information should not be made available to other organisations or individuals without the prior approval of a Senior Manager. In addition, individual **consent** may be required. These measures help to ensure that:

- The Trust complies with the Data Protection Act 1998
- Information is held, moved and stored according to specified security standards[5] and used only for agreed purposes[1&6].
- Information in transit in any form complies with the requirements of the Trust's Bulk Data Transfer (BDT) Policy[7] – CORP/ICT 20, where applicable.

3.9 If personally identifiable data is taken off site for proper business purposes, then appropriate measures[8] must be taken to ensure that the data is safeguarded against unauthorised disclosure, loss or destruction.

3.10 Think carefully before you release information to any 3rd Party. This can be especially complicated after a patient's death when relatives sometimes 'need answers'. Always be polite and respectful, and try to direct any enquiries or 'subject access requests[9]' to the Medical Records Casenote Release teams at our main hospital sites.

3.11 Any breach of information security must be reported immediately to the IT Services 'help desk', Head of Information Governance or Caldicott Guardian. Suspected or actual breaches of a delicate or personal or private nature should be directed to the Caldicott Guardian or Head of Information Governance in confidence; here the IG Toolkit SIRI reporting tool will be actioned when applicable. Trust Adverse Incident reporting processes should also be completed. Serious Incidents must be reported through STEIS[10] within 24 hours of the occurrence.

3.12 Consideration of the 8th Principle of the Data Protection Act must be given when Patient's move abroad outside of the European Economic Community (EEC) where there may be an inadequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. Patient's must be fully informed and should normally consent to their data being transferred outside of the EEC. Schedule 4 of the Act provides for circumstances in which the 8th Principle does not apply, and you should seek guidance from the Head of Information Governance or the Information Commissioner Website http://www.ico.gov.uk/ if you need help.

---

[5] ISO17799 Pt1 / BS7799 Pt 2
[6] Doncaster and Bassetlaw PCT and their Commissioning Body - Information Sharing Protocols
[7] Letters to all Trusts from the NHS Chief Executive of the NHS (December 2007 through May 2008) concerning the carriage and/or transmission of Person Identifying Data (PID)
[8] This usually involves encryption or pseudonymisation if the information is in electronic format
[9] CORP/REC 3: Procedure for Providing Subject Access to Health Records Under the Data Protection Act 1998
[10] STEIS: Strategic Executive Information System

4. TRAINING

Information Governance is now **MANDATORY** for **ALL** Trust staff[11].

Staff - including Volunteers - must complete their Information Governance (IG) training at least annually, and this will be recorded on their ESR Training Record[12]:

5. 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).

6. MONITORING

Monitoring of this Code of Practice will be through staff fliers.

What is being Monitored	Who will carry out the Monitoring	How often	How Reviewed/ Where Reported to
Staff do not leave files/computer terminals unattended/unsecured Staff double check to avoid transmitting information to the wrong person or fax machine[13] Staff do not allow sensitive conversations to be overheard Staff guard against people seeking information by deception. Staff Log out or Lock their screen down when leaving their desk for any length of time	The Trust Information Governance Group – Secret Shoppers	One area per month and in line with IG Toolkit standards	To the IG Group in line with IG Toolkit standards

[11] Information Governance Policy: CORP/ICT 9
[12] 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
[13] Safe Haven Guidelines: CORP/ICT 8

APPENDIX 1 – EQUALITY IMPACT ASSESSMENT - PART 1 INITIAL SCREENING

Service/Function/Policy/Project/ Strategy	CSU/Executive Directorate and Department	Assessor (s)	New or Existing Service or Policy?	Date of Assessment
Confidentiality Code of Conduct	Finance & Infrastructure	Head of Information Governance	Existing Policy	24/03/2015

1) Who is responsible for this policy? Finance & Infrastructure

2) Describe the purpose of the service / function / policy / project/ strategy? Information is treated in Confidence

3) Are there any associated objectives? Data Protection Act 1998/DH 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? NO

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: March 2018

Checked by: Head of Information Governance **Date:** 24/3/2015