Directorate of Performance Assurance

CONFIDENTIALITY POLICY

Reference:	DCP029
Version:	1.5
This version issued:	20/01/17
Result of last review:	Minor changes
Date approved by owner (if applicable):	N/A
Date approved:	23/11/16
Approving body:	Information Governance Steering Group
Date for review:	November, 2019
Owner:	Wendy Booth, Director of Performance Assurance
Document type:	Policy
Number of pages:	10 (including front sheet)
Author / Contact:	Jeremy Daws, Head of Quality Assurance

Contents

1.0 Introduction

Patients have the right to expect that the information about them will be held in confidence by their doctors. Confidentiality is central to trust between doctors and patients. Without assurances about confidentiality, patients may be reluctant to give doctors the information they need in order to provide good care.

2.0 Purpose

2.1 This policy sets out Northern Lincolnshire and Goole NHS Foundation Trust's commitment to the confidentiality of patient/service users' information and its responsibilities with regard to the disclosure of such information.

2.2 All employees working in the NHS are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work.

2.3 The policy is also to protect staff by making them aware of the correct procedures for maintaining confidentiality of patient information so that they do not inadvertently breach any requirements of law or good practice.

2.4 The legal and best practice guidance informing the development of this policy includes:

- Common law duty of confidence
- All contracts of employment in the Trust
- Data Protection Act 1998
- Human Rights Act 1998
- Computer Misuse Act 1990
- Caldicott Report 1997
- NHS confidentiality code of practice
- Codes of conduct for all health professionals

2.5 Under the Data Protection Act 1998 the Trust has to ensure that the appropriate security measures are in place to safeguard patient information.

2.6 The Trust is held accountable, through clinical and information governance frameworks, specifically the Information Governance Toolkit, for continuously improving confidentiality and security procedures governing access to and storage of personal information.

3.0 Area

3.1 This policy applies to all person identifiable information, whether written, computerised, visually or audio recorded or any other medium.

3.2 This policy applies trustwide to:

- All members of staff, including non-executive directors
- Students/Placement/Agency staff/Apprentices
- Volunteers
- Locums
- Contractors/Sub-Contractors
- Governors

4.0 Duties and Responsibilities with Information Governance

4.1 The Chief Executive

The Chief Executive has overall accountability for ensuring that there are appropriate arrangements in place for maintaining the confidentiality of information at all times; any disclosures are for legitimate purposes and conform to this policy and other legal requirements.

4.2 Caldicott Guardian

The Director of Performance Assurance and Trust Secretary is the designated Trust Caldicott Guardian who acts as the conscience of the organisation. The Caldicott Guardian actively supports and facilitates appropriate information sharing, advises on the options for lawful and ethical information processing. The Caldicott Guardian is responsible for maintaining the currency of this policy, providing advice upon request to any member of staff on the issues covered within it. The Caldicott Guardian has the responsibility for ensuring that national and local guidelines are in place and overseeing the arrangements for the use and sharing of person identifiable information.

4.3 Health Records Support Manager

The Health Records Manager is responsible for providing a health record availability service to the organisation and a service to patients to access their own health records, further details of which are provided in the Trust's Subject Access Policy.

4.4 All Line Managers

All Managers have a duty to ensure that their staff are aware of their responsibilities to protect the confidentiality of patient/service user information. Managers are also responsible for the dissemination and implementation of this policy to all its staff members.

4.5 All Staff

All staff are individually responsible for compliance to the policy, and risk disciplinary action if they are found to have disclosed information outside of the boundaries of this policy which should be documented. All staff will be aware of their responsibilities and obligations to respect patient confidentiality. In addition, all professional health staff are bound to follow existing professional ethical principles of confidence as set out by the various bodies.

4.6 Information Asset Owner (IAO)

Information Asset Owners are responsible for ensuring that access to electronic and manual confidential information is strictly controlled within their system. They will be responsible for monitoring access attempts in order to highlight potential areas for concern, for example regular access attempts by the same individual. They will be responsible for ensuring that confidentiality audits and subsequent recommendations are complied with within the specified timescales.

5.0 Actions

5.1 No employee shall breach their legal duty of confidentiality, allow others to do so, or attempt to breach any of the Trust's security systems or controls in order to do so.

5.2 No employee shall knowingly browse, search for or look at any Trust information relating to themselves, their own family, friends or other persons without a legitimate Trust purpose. Action of this kind will be viewed as a breach of confidentiality and of the Data Protection Act, and may result in disciplinary action.

5.3 All information about patients must be treated as confidential and be only used for the purposes for which it was given i.e. to provide care, or for local clinical audit of that care. The duty of confidentiality is owed to all patients and endures beyond the individual's death.

5.4 Information necessary to provide care or treatment for an individual patient should be shared on a 'need to know basis', i.e. with others in the healthcare team for that episode of care.

5.5 As it is impractical to obtain consent every time information needs to be shared, patients must be informed and understand that some information may be made available to other members of the team involved in the delivery of their care.

5.6 Disclosure of information outside the team that will have personal consequences for patients must be with the consent of the patient.

5.7 If the patient withholds consent, or if consent cannot be obtained for whatever reason, disclosures may be made only where:

- They can be justified in the public interest (usually where disclosure is essential to protect the patient or client or someone else from risk of significant harm)
- They are required to by law or by order of a court

- Where there is an issue of child protection; in this case local polices should be consulted for further details

5.8 Further details of these exceptional cases and appropriate justification for disclosing information without consent are set out in the Trust's Data Protection and Personal Information Fair Processing policy.

5.9 The Trust will allow the use of patient information without consent for medical research, keeping registers of cancer patients, or checking quality of care (clinical audit), in line with the permissions granted by the independent, national Ethics and Confidentiality Committee (ECC).

5.10 If you have any concerns about disclosing or sharing personal information you must discuss them with your line manager. If they are unavailable consult someone with the same or similar responsibilities or the Caldicott Guardian.

6.0 Information Use for Other than Direct Care

6.1 In addition to direct care, patient information is also needed for a range of wider services as follows:

- Assuring and improving the quality of care and treatment (e.g. through clinical audit)
- Monitoring and protecting public health
- Co-ordinating NHS care with that of other agencies (e.g. local authority, voluntary and independent services)
- Effective healthcare administration:
  - Managing and planning services
  - Contracting for NHS services
  - Auditing NHS accounts
  - Risk Management
  - Investigating complaints and notified or potential legal claims
  - Teaching
  - Statistical analysis and medical or health services research

6.2 Wherever it is possible anonymised information should be used, by removing as many personal identifiers as possible, e.g. name and address.

6.3 The use of NHS number is encouraged as a means of all organisations in the NHS being sure that the same patient is being discussed, and as a means of effective anonymisation transit.

7.0 Protection of Personal Information

7.1 Staff must guard against breaches of confidentiality by protecting information from improper disclosure at all times.

7.1.1 Patients may sue the Trust for unlimited damages if they can prove that they have suffered significant harm or distress as a result of an unlawful disclosure of their information. This may be by any means, i.e. by electronic or paper means, by telephone, fax or face to face conversation.

7.1.2 Arrangements for the storage and disposal of all personal information (both manually recorded and computer based) must protect confidentiality and be in line with the Records Management: NHS Code of Practice retention recommendations.

7.1.3 Care should be taken to ensure that unintentional breaches of confidentiality do not occur. Many improper disclosures are unintentional.

7.1.4 Staff should not discuss patients where the conversation can be overheard or leave patients' records where they can be seen by other members of the public.

7.1.5 Wherever it is possible consultations with patients should be in private.

7.1.6 The Trust seeks to ensure that any contractors and their staff coming onto any of the Trusts sites in the course of their work are also aware of their responsibilities regarding confidential patient and staff information.

7.1.7 Access to rooms and offices where terminals are present or data relating to individuals are stored should be controlled.

7.1.8 Wherever it is possible doors should be locked with keys or swipe access when data and terminals are unattended.

7.1.9 Case notes, and all other patient information should be stored securely in lockable desk drawers or filing cabinets, within rooms which should be locked when left unattended.

7.1.10 Any patient information taken outside of the Trust must be appropriately protected at all times for further advice consult the Information Security Policy.

7.2 Computers

7.2.1 Patient's information must only be stored on Trust equipment and not on personally owned laptops or home desk computers.

7.2.2 Where staff needs to work from home, the Trust Information Security Policy must be consulted for further advice.

7.2.3 All files containing patient-identifiable information, held on Trust owned computer equipment should be password protected.

7.2.4 Particular care should be taken with portable devices and these should be encrypted to national minimum standard as set out in the Information Security Policy.

7.2.5 Patient named data should not be kept on the hard drives of PCs due to the risk of theft and breach of confidentiality. Such files should be stored securely on the network, where they will be backed up centrally by the IT department.

7.2.6 Users should not leave terminals logged in and unattended, unless the account is locked for short term absences from the terminal. This is an issue of great concern and importance in the public areas of the Trust.

7.2.7 Computers should not be transferred between users or disposed of other than the IT department, as they have the means of transferring or removing all data from the hard drive.

7.3 Telephone

7.3.1 All possible steps must be taken to ensure that patient information is not divulged over the telephone to anyone without appropriate authority. Where relatives' telephone on the patient's behalf to enquire about appointment dates etc, all effort should be made to speak to the patient him/herself. Just asking for one of the key qualifying questions about the patient e.g. date of birth may not always be sufficient to ensure the caller is genuinely a relative and has the need to know the information.

7.3.2 Where there is any doubt regarding the identity of the person requesting the information, guidance should be sought from the line manager. If advice is not immediately available then the information should not be disclosed. If the caller is claiming to be from an organisation e.g. social services then the switchboard telephone number should be obtained (rather than a direct line), checked and then used to ensure that the caller is from the agency stated.

7.3.3 Where relatives are asking for clinical information about an inpatient this would not usually be given over the telephone. If however this is felt to be appropriate, due to geographical location of the relative, the patient must be consulted and give consent for information to be divulged, and a password arrangement made with the patient and relative.

7.3.4 The use of mobile telephones to discuss named patient data is discouraged.

7.3.5 The use of Vocera communication badges must be conformant to the Vocera user responsibilities agreement.

8.0 Monitoring Compliance and Effectiveness

8.1 The Information Governance Steering Group is tasked with the responsibility of overseeing the implementation of this policy and to monitor compliance.

8.2 Compliance with this policy will be monitored through regular confidentiality audits carried out by the Information Asset Administrators. Any incidents or potential concern will be raised with, in the first instance, the Information Asset Owners and in the second instance the IG Operational Lead or Caldicott Guardian. All potential breaches will be investigated in line with Trust policy.

8.3 The group will monitor progress in year with the Information Governance Toolkit and associated action plans giving auditable evidence of the Trust's compliance with confidentiality and data protection requirements.

8.4 The Trust Governance and Assurance Committee (a sub-group of the Board) is informed on any confidentiality/data protection issues requiring escalation, and is responsible for ratifying documents approved by the Information Governance Steering Group.

8.5 In the event of a breach of confidentiality, the reporting and escalation processes are in line with the Risk Management Strategy, the Incident Reporting Policy and Procedure and the Policy for dealing with Serious Incidents (Clinical & non-Clinical).

9.0 Associated Documents

9.1 Safe Haven Policy.

9.2 Data Protection & Personal Information Fair Processing Policy.

9.3 Information Security Policy.

9.4 Information Governance Policy.

9.5 Health Records Management Policy & Strategy.

9.6 Corporate (Non-Clinical) Records Management Policy.

9.7 Risk Management Strategy.

9.8 Subject Access to Health Records Policy.

9.9 Incident Reporting Policy/Procedure.

9.10 Policy for Dealing with Serious Incidents (Clinical & Non Clinical).

10.0 References

10.1 Department of Health (2003) Confidentiality: NHS Code of Practice.

10.2 Connecting For Health – Information Governance Toolkit.

10.3 The Data Protection Act (1998).

10.4 Freedom of Information Act (2000).

11.0 Definitions

Information Governance Toolkit – This is an online self-assessment tool, where the Trust is obligated to demonstrate compliance with standards required by Connecting for Health on an annual basis.

12.0 Consultation

Information Governance Steering Group.

13.0 Dissemination

This policy will be issued to all staff via the intranet.

14.0 Equality Act (2010)

14.1 In accordance with the Equality Act (2010), the Trust will make reasonable adjustments to the workplace so that an employee with a disability, as covered under the Act, should not be at any substantial disadvantage. The Trust will endeavour to develop an environment within which individuals feel able to disclose any disability or condition which may have a long term and substantial effect on their ability to carry out their normal day to day activities.

14.2 The Trust will wherever practical make adjustments as deemed reasonable in light of an employee's specific circumstances and the Trust's available resources paying particular attention to the Disability Discrimination requirements and the Equality Act (2010).

The electronic master copy of this document is held by Document Control, Directorate of Performance Assurance, NL&G NHS Foundation Trust.