Pennine Care NHS
NHS Foundation Trust

Policy Document Control Page

Title

Title: Confidentiality Policy

Version: 7

Reference Number: CO4

Supersedes

Supersedes: Version 6
Description of Amendment(s): Inclusion of polices to be read in conjunction with this policy

Important Notice
From May 2018 the UK will be adopting the European General Data Protection Regulations. These regulations will be replacing the Data Protection Act 1998. In the UK we are still awaiting some health sector specific guidance and instruction regarding GDPR, and as such have deemed that, unless there is a legal requirement or a fundamental change that is required in a policy, all policies, regardless of review date, shall remain current, valid and must be followed for the foreseeable future, to be reviewed prior to the implementation of GDPR from May 2018. Any queries in relation to this statement should be directed to the Trust Information Governance Manager.

Originator

Originated By: Jenny Spiers
Designation: Information Governance Manager

Equality Impact Assessment (EIA) Process
Equality Relevance Assessment Undertaken by: Information Risk Manager
ERA undertaken on: 17th May 2012
ERA approved by EIA Work group on: 1st June 2012

Where policy deemed relevant to equality-
EIA undertaken by Information Risk Manager
EIA undertaken on 1st June 2012
EIA approved by EIA work group on 1st June 2012

Approval and Ratification

Referred for approval by: Information Governance Manager

Date of Referral: 1st March 2017

Approved by: Information Governance Assurance Group

Approval Date: 1st March 2017

Date Ratified by Executive Directors: 20th March 2017

Executive Director Lead: Medical Director/Caldicott Guardian

Circulation

Issue Date: 22nd March 2017

Circulated by: Information Department

Issued to: An e-copy of this policy is sent to all wards and departments

To be updated to the Trust's external website? Yes

Review

Review Date: March 2018 (or as GDPR changes require a change).

Responsibility of: Jenny Spiers

Designation: Information Governance Manager

This policy is to be disseminated to all relevant staff.

This policy must be posted on the Intranet.

Date Posted: 22nd March 2017

CONTENTS

This Policy should be read in conjunction with the following policies/procedures:

Information Governance Staff Handbook
Data Protection Policy
Information Governance Policy
Information Security Policy
Access to Health Records
Freedom of Information Policy
Information Risk Management Policy
Information Sharing Policy
Records Management Policy
IG Requirements for New Processes and Systems
Environmental Impact Regulations

1 Introduction and Aims

1.1 Pennine Care NHS Foundation Trust (PCFT) has a statutory duty to safeguard the confidential information it holds, from whatever source, that is not in the public domain. The principle of this policy is that no individual or company working for or with PCFT shall misuse any information or allow others to do so.

1.2 During the course of their day to day work, many individuals working within or for PCFT will often handle or be exposed to information which is deemed personal, sensitive or confidential (including commercially confidential – see 2.2 below) information. It is a requirement that any individual, company or other organisation to which this policy applies shall not at any time during the period they work for or provide services to PCFT nor at any time after its termination, disclose confidential information that is held or processed by PCFT.

1.3 All staff working for PCFT are bound by a common law duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement of the Data Protection Act 1998 and, for health and other professionals, through their own professions' Code of Conduct.

1.4 PCFT places great emphasis on the need for the strictest confidentiality in respect of personal health data. This applies to manual and computer records and conversations about service users treatments. Everyone working for PCFT is under a legal and common law duty to keep service users information, held in whatever form, confidential. Service users who feel that confidence has been breached may issue a complaint under the PCFT complaints procedure or they could take legal action.

1.5 Confidentiality must only be breached in exceptional circumstances, with appropriate justification and be fully documented.

1.6 PCFT is committed to the delivery of a highly confidential service. This means ensuring that all personal service user and staff information is processed fairly, lawfully and as transparently as possible so that the public can:

- Understand the reasons for processing personal information
- Give their consent for the disclosure and use of their personal information where necessary
- Gain trust in the way PCFT handles information, and
- Understand their rights to access information held about them

1.7 The aims of this policy are:

- To safeguard all confidential information within PCFT
- To provide guidelines for all individuals working with the organisation
- To ensure a consistent approach to confidentiality across PCFT
- To ensure all staff are aware of their responsibilities with regards to confidential information
- To provide all individuals working within PCFT access to documents which set out the laws, codes of practice and procedures relating to confidentiality and which apply to them.

These include:

- The common law Duty of Confidentiality
- Caldicott Principles
- Data Protection Act 1998
- Freedom of Information Act 2000
- Human Rights Act 1998
- Department of Health 'Confidentiality: NHS Code of Practice including supplementary guidance 'Public Interest Disclosure'
- The Public Interest Disclosure Act- 1998
- The Computer Misuse Act 1990

2 Scope

2.1 This policy applies to those members of staff that are directly employed by PCFT and for whom PCFT has legal responsibility. For those staff covered by a letter of authority/honorary contract or work experience the organisations policies are also applicable whilst undertaking duties for or on behalf of PCFT. Further, this policy applies to all third parties and others authorised to undertake work on behalf of PCFT.

2.2 For the purposes of this policy, confidential information shall include any confidential information relating to PCFT and/or its agents, customers, prospective customers, suppliers or any third parties connected with PCFT and in particular can include:

- Service user information
- Ideas/programme plans/forecasts/risks/issues
- Trade secrets
- Business methods and business design
- Finance/budget planning/business cases
- Prices and pricing structures
- Sources of supply and costs of equipment and/or software
- Prospective business opportunities in general
- Computer programs and/or software adapted or used
- Policy advice and strategy
- Corporate or personnel information
- Contractual and confidential supplier information

2.3 This is irrespective of whether the material is marked as confidential or not.

3 Conduct

3.1 Individuals shall not be restrained from using or disclosing any confidential information which:

- They are authorised to use or disclose by PCFT
- Has entered the public domain unless it enters the public domain as a result of an unauthorised disclosure by the individual
- They are required to disclose by law.
- They are entitled to disclose under the Public Interest Disclosure Act 1998 provided that the disclosure is made in an appropriate way to an appropriate person having regard to the provision of the Act.

3.2 All individuals must:

- Exercise all due care and diligence to prevent unauthorised disclosure of personal confidential data
- Ensure the physical security of all confidential documents and/or media, including storage of files on PCs. Confidential information must never be unattended and should be secure when not in use
- Only use Trust authorised equipment to process personal confidential data, which is encrypted to national standards
- Comply with password guidance by not disclosing passwords to anyone, including colleagues

3.3 All individuals will be required to comply with this policy whilst working within PCFT and thereafter for as long as the information remains personal confidential data.

3.4 If an individual is unclear if information should be classified as confidential, they must discuss the issue with their manager who will offer advice.

4 The Duty of Confidence

4.1 All NHS bodies and those carrying out functions on behalf of the NHS have a duty of confidence to service users and a duty to support professional ethical standards of confidentiality.

4.2 Everyone working for or with the NHS records that handles, stores or otherwise comes across information that is capable of identifying individual service users has a personal duty of confidence to the service user and to his/her employer.

4.3 The duty of confidence is conferred by common law, statute, contract of employment, disciplinary codes and policies and professional registration.

4.4 Service users expect that information given by them to their doctors, nurses and other members of the healthcare team is treated in confidence and not passed to others without their permission. Particular care must be taken to avoid inadvertent or accidental disclosure. The underlying principle is that all information that can be related to an individual must be treated as confidential and it must not be communicated to anyone who is unauthorised to receive it. Unauthorised staff include those who are not involved in either the clinical care of the service user or the associated administration processes.

4.5 No personal information, given or received in confidence, may be passed to anyone else without the consent of the provider of the information. This is usually the service user but sometimes another person may be the source (e.g. relative or carer). There are some exceptions to this see 6.5 and 6.6 below.

4.6 Service users are entitled to object to the use of their personal health data for purposes other than their direct care.

4.7 No personal information, given or received in confidence for one purpose, may be used for a different purpose without the consent of the provider of the information.

4.8 The duty of confidentiality owed to a deceased service user should be viewed as being consistent with the rights of living individuals.

5 What is personal information?

5.1 Personal confidential data/information is anything that contains the means to identify a person e.g. name, address, postcode, data of birth, NHS number, National Insurance number etc. Any data or combination of data and other information, which can indirectly identify the person, will also fall into this definition.

5.2 Information that identifies individuals personally must be regarded as confidential, and should not be used without a justifiable and legal purpose.

5.3 Whenever possible, anonymised data, that is where all personal details have been removed and which therefore cannot identify the individual, should be used.

5.4 Confidential information is information entrusted by an individual in confidence where there is a general obligation not to disclose that information without consent.

5.5 Confidential information may include personal information such as name, age, address and personal circumstances, as well as sensitive personal information (as defined by the Data Protection Act 1998 – DPA) regarding race, health, sexuality etc.

5.6 Confidential information may be known, or stored on any medium. Photographs, videos etc. are subject to the same requirements as information stored in health records, on a computer, or given verbally.

6 Disclosing service user information

6.1 The NHS Confidentiality: Code of Practice provides advice on using and disclosing confidential service user information and has models for confidentiality decisions and all staff should adhere to this guidance.

http://systems.hscic.gov.uk/infogov/codes/confcode.pdf

6.2 Personal information may be disclosed on the basis of implied consent where the disclosure is necessary for healthcare purposes and is undertaken by a health professional or a person owing an equivalent duty of confidentiality.

6.3 PCFT will inform service users, staff and any other data subjects why, how and for what purpose personal information is collected, recorded and processed.

6.4 Consent of the data subject will be required where a disclosure of personal information is not directly concerned with healthcare/treatment of a service user e.g. medical research, health service management, financial audit, personnel data or where disclosure is to a non-health care professional.

6.5 Under common law, personal information may be disclosed without consent (see Information Sharing without Consent form at appendix 2) for example:

- In order to prevent abuse or serious harm to others
- Where the public good that would be achieved by the disclosure outweighs both the obligation of confidentiality to the service user concerned and the broader public interest in the provision of a confidential service

6.6 Where information is required by the police, If possible, the consent of the service user should be obtained to the release of any information. If the consent of the service user cannot be obtained please refer to the Information Governance Staff Handbook for more detailed guidance

7 Personnel information

7.1 In keeping with good workforce and organisational development practice, PCFT retains and processes personal data on its employees. In addition, PCFT may from time to time, retain and process 'sensitive personal data' as defined by the DPA for example in relation to sickness and occupational health records, performance reviews, equal opportunities monitoring for the prevention of fraud or other illegal activities.

7.2 PCFT may process such data and such data may be legitimately disclosed to appropriate employees and to PCFT professional advisors, in accordance with the principles of the DPA.

7.3 PCFT takes all reasonable steps to ensure that the data it holds is accurate, complete, current and relevant. If a member of staff considers that data held on him/her is or may be inaccurate, or if he/she wishes to have access to such data, then contact should be made with the Head of Workforce and Organisational Development.

8 Media enquiries

8.1 All requests for information by the media, other than those made under Freedom of Information (FOI) Act, should be referred to the Communications Team.

communications.penninecare@nhs.net

9 Termination or expiry of a staff / work contract with PCFT

9.1 On leaving PCFT any copies of software, documents or correspondence, diaries, plans, specifications or any other information

relevant to PCFT (whether or not prepared or produced by the individual) must be returned to PCFT possession and under no circumstances must the leaver take this information with them. This relates to both paper and electronic information, including that saved to corporate or personal folders on the Trust network drives (e.g. 'F' drive and 'G drive'.

9.2 All individuals that have left PCFT are bound by the Confidentiality Policy that was in publication at the time of their departure.

10 Awareness and compliance

10.1 It is important to PCFT to protect its legitimate business interests and in particular its confidential information. Breaches of confidentiality, of any sort, including breach of this policy may result in legal action taken against the individual, and will be considered under the appropriate Disciplinary Policy.

10.2 If an individual unintentionally divulges confidential information, or they are aware of any individual doing so, he or she must report it immediately to their line manager and complete an electronic incident form on Safeguard.

10.3 Everyone in PCFT must be aware of the importance of confidentiality. All staff need to be aware of their responsibilities for safeguarding service user confidentiality and keeping information secure.

10.4 The duty of confidentiality is written into employment contracts. Breaches of confidentiality are a serious matter. A breach of confidentiality of information gained, whether directly or indirectly, in the course of duty is a disciplinary offence which could result in dismissal and/or prosecution. No employee shall knowingly misuse any information or allow others to do so.

10.5 It is a disciplinary offence to access records/information that you have no legitimate reason to view this includes, records about yourself, your family, friends, neighbours, acquaintances. If you do not have a legitimate reason to access, do not browse. Remember all transactions are auditable.

11 Accountability, responsibilities and training

11.1 Overall accountability for procedural documents across the organisation lies with the Chief Executive who has overall accountability for establishing and maintaining an effective document management system, for meeting all statutory requirements and adhering to guidance issued in respect of procedural documents.

11.2 Overall responsibility for the confidentiality policy lies with the Caldicott Guardian with delegated responsibility for managing the development and implementation of confidentiality policy procedural documents to the Information Governance Manager.

11.3 The Caldicott Guardian is responsible for overseeing and advising on contentious issues of service user confidentiality for PCFT.

11.4 Line Managers are responsible for ensuring that all staff, particularly new staff, temporary staff, contractors and volunteers, know what is expected of them with respect to confidentiality and protecting information. They and are also responsible for monitoring compliance with this policy . The Trust has a dedicated Privacy Officer who will monitor for inappropriate access via regular auditing of access, including Break glass processes.

11.5 Staff are responsible for maintaining the confidentiality of all personal and corporate information gained during their employment with PCFT and extends after they have left the employ of PCFT.

11.6 Individual staff members are personally responsible for any decision to pass on information that they may make.

11.7 All staff are responsible for adhering to the Caldicott principles, the Data Protection Act and the Confidentiality Code of Conduct.

11.8 Staff will receive instruction and direction regarding the policy from a number of sources:

- Policy/strategy and procedure manuals
- Line manager
- Specific training courses
- Other communication methods (team brief/team meetings/IG bulletins)
- Staff Intranet

11.9 All staff are mandated to undertake Information Governance training on an annual basis. This training should be provided within the first year of employment and then updated annually as appropriate in accordance with the Core and Essential Skills Policy and the Information Governance training plan.

12 Monitoring and review

12.1 Performance against key performance indicators will be reviewed on an annual basis and used to inform the development of future procedural documents.

12.2 This policy will be reviewed annually, re-ratified every 3 years, and in accordance with the following, on an ‘as and when’ required basis:

- Legislative changes
- Good practice guidance
- Case laws
- Significant incidents reported
- New vulnerabilities
- Changes to organisational infrastructure

13 Legislation and related documents

13.1 A set of procedural document manuals will be available via the PCFT staff intranet such as the Staff IG Handbook

13.2 Staff will be made aware of procedural document updates as they occur via team briefs, team meetings, IG bulletins and notification via the PCFT staff intranet

13.3 All documents in the PCFT Policies and Procedures register are relevant

Appendix 1

LIST OF CONTACTS

Chief Executive
Pennine Care NHS Trust HQ
0161 716 3002

Caldicott Guardian (Medical Director)
Pennine Care NHS Trust HQ
0161 716 3005

Information Governance Manager
Pennine Care Trust HQ
0161 716 3145

ICT Helpdesk
Pennine Care NHS Trust HQ
0161 716 1234

Communications Manager
Pennine Care NHS Trust HQ
0161 716 3150

Complaints Manager
Pennine Care NHS Trust
0161 716 3083

Out of Hours advice in cases of urgency
Executive Director on Call
0161 331 6000 (Via Tameside Hospital Switchboard)

Appendix 2

Pennine Care NHS
NHS Foundation Trust

INFORMATION SHARING WITHOUT CONSENT FORM

Service user information:

Name :---------- dob ----------

RT2 no. ----------

Address ----------

Names and dob of children: ---------- ----------
(if applicable)

---------- ----------

---------- ----------

CONCERNS

Child(ren) at risk/Danger to child(ren) ☐

Danger to client ☐

Client poses a risk to self or others ☐

DETAILS OF INCIDENT/INFORMATION CAUSING CONCERN:
(include source of information)

BALANCING CONSIDERATIONS
All practitioners should consider the following:

- Pressing need
- Respective risks to those affected
- Risk of not disclosing
- Interest of other agency/person in receiving it
- Public interest in disclosure
- Has there been an actual/potential serious crime[1]
- Human rights
- Duty of confidentiality

PRACTITIONER COMMENTS:

Internal consultations: (e.g. names, dates and advice/decisions)
(Decisions to disclose do not need to be made in isolation, consider discussion amongst wider multi-disciplinary team/colleagues)

External consultations: (e.g. Trust solicitor, Professional body)

CLIENT NOTIFICATION
Client notified of disclosure(s)? YES/NO Date:

If not, why not?

KEEP A RECORD

Date information shared:

Agency and name of person informed:

Method of contact (by phone etc.)

[1] The definition of serious crime is not entirely clear. Murder, manslaughter, rape, treason, kidnapping, child abuse or other cases where individuals have suffered serious harm may all warrant breaching confidentiality. Serious harm to the security of the state or to public order and crimes that involve substantial financial gain or loss will also generally fall within this category. In contrast, theft, fraud or damage to property where loss or damage is less substantial would generally not warrant breach of confidence.

File this form in the clinical record