The Tavistock and Portman NHS
NHS Foundation Trust

Confidentiality code of conduct for staff

Version	4.3
Approved by:	PASC
Lead Manager:	Caldicott Guardian
Lead Director	Chief Executive
Approved on	8.6.16
Date issued	Jun 16
Review Date	May 19

Contents

Confidentiality Code of Conduct for Staff

Summary Code of Confidentiality

1. As a member of staff at the Tavistock and Portman NHS Foundation Trust you are responsible for ensuring that you use and handle confidential or person identifiable information in a secure and confidential way.

2. Unauthorised disclosure of confidential information is an offence under law.

3. Suspected or known breaches of confidentiality must be reported as incidents through the Trust's incident reporting system.

4. Confidential patient information can only be used for the purpose of providing healthcare to an individual, and, other than in clearly defined circumstances, such information can only be disclosed with informed patient consent.

5. Circumstances when confidential or patient identifiable information can be disclosed without patient consent are:

    a) when required by statute law
    b) when required by court order
    c) And when it may be in the public interest.

6. If a patient lacks capacity and cannot consent, then confidential or patient-identifiable information can only be disclosed in the best interests of the patient.

7. Where there is concern that a child may be suffering harm or is at risk of suffering harm, the child's safety and welfare are the overriding consideration.

8. Access to confidential information is restricted to people on a "need to know" basis.

9. All staff must ensure that confidential information in all formats is securely stored at all times.

10. Only the minimum necessary information should be disclosed and to the minimum number of recipients.

11. All staff must attend internal training on confidentiality and information governance.

12. Access to clinical information for research purposes can only occur with the explicit informed consent of the patient.

1 Introduction

Patients disclose confidential, person identifiable and sensitive information about themselves while in the care of the Trust and they must be assured that Trust staff will protect this information and safeguard their right to privacy.

All staff working at the Tavistock and Portman NHS Foundation Trust (the Trust) are legally bound by a duty of confidence to protect personal confidential information. This requirement is contractual, and is based on the common law duty of confidentiality the Data Protection Act (1998), and set out in the NHS Care Record Guarantee (2011).

This Code is intended to provide guidance on the practice, principles, and ethics underpinning the protection of patient information in this Trust. It sets out the requirements for all staff when sharing information within NHS organisations and between the Trust and its partners. It does not aim to offer a "rule" for every possible situation that may arise.

2 Purpose

The main purpose of this Code is to provide guidance on matters concerning patients' confidential information and how it is to be protected and stored. It also enshrines the patient's rights to privacy under Article 8 of the Human Rights Act.

Confidential information also includes information about staff and confidential business information.

3 Scope

This code applies to all staff including locum, trainees and honorary staff who are employed by or working at the Trust whether employed directly or not. This code applies within the Trust to all aspects of identifiable and confidential information. For ease of reference, references to 'staff' encapsulates all those who might have access to confidential information; this term does not imply employment status for those to whom employment does not apply.

This Code of Conduct follows the **Caldicott Principles** which apply to the handling of patient-identifiable information. These principles are:

Principle 1
You must be able to justify the purpose(s) of every proposed use of confidential patient information.

Principle 2
You must only use personal confidential information when absolutely necessary.

Principle 3
You must use the minimum information necessary.

Principle 4
Access to personal confidential information must be on a strict need-to-know basis.

Principle 5
All staff must understand their responsibilities.

Principle 6
All staff must understand and comply with the law.

Principle 7

The duty to share personal confidential data can be as important as the duty to respect service user confidentiality.

4 Definitions

Data Subject is the person about whom the information is about.

Confidential information is information that identifies patients or their family or friends. Storage of confidential information relates to records and that retained in an employee's memory.

Paper record is the paper file and any other letters, reports, notes recording confidential information.

Electronic records include records which are held a retrievable electronic form.

Person/Patient-identifiable confidential information is information that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number, National Insurance Number, a physical description, a location, etc. A visual image (e.g. photograph) is sufficient to identify an individual.

Sensitive personal information refers to personal information about: race or ethnicity, political opinions, religious or similar beliefs, physical or mental health condition, commission or alleged commission of offences or a legal proceeding, sexual orientation, trades' union membership.

Human Rights Act (1998) Article 8 offers general protection for a person's private and family life. This right affects a large number of areas of life and is framed extremely broadly. Compliance with the Common Law Duty of Confidentiality and Data Protection Act should fulfil Human Rights requirements.

The **Common Law Duty of Confidentiality** comes from case law and requires that information that has been provided in confidence should not be disclosed except as intended by the person who confided the information or with that individual's subsequent permission.

5 Duties and responsibilities

The **Chief Executive** is ultimately responsible for the Trust's compliance with the Data Protection Act and associated legislation regarding the confidentiality of personal data.

The **Senior Information Risk Owner** (SIRO) holds overall responsibility for the Trust's information risk management.

The **Governance Manager** has responsibility to ensure that the Trust complies with Information Governance requirements, including, confidentiality and data protection. The Governance Manager can also arrange access to legal advice.

The **Caldicott Guardian** is a senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information sharing. Acting as the 'conscience' of an organisation, the Guardian actively supports work to enable information sharing where it is appropriate to share, advises on options for lawful and ethical processing of information.

HR business partners will issue a copy of this Code to all new staff. Each new member will be asked to sign the acceptance form at the end of the document. This will be retained in the individual's personnel file.

Directors will ensure that their staff comply with this code, and use appraisal and supervision to oversee and review practice.

Clinical team managers must ensure that arrangements are in place to implement the code, and in particular, the provisions relating to providing information about handling information and the consent or otherwise for sharing.

Individual **staff** are required to familiarise themselves with the Code and ensure that they follow the principles of the Code in all the work they do on behalf of the Trust.

Any attempts to breach security should be immediately reported as an incident.

Consulting with senior clinical staff, the safeguarding lead or with the Caldicott Guardian in the event of uncertainty.

6 Complying with the code

6.1 Legal principles

The eight principles of the **Data Protection Act 1998** (DPA) apply to all staff handling personal information (applies to all forms of media) as follows:

1. Personal data shall be processed fairly and lawfully.
2. Personal data shall be obtained for one or more specified purpose(s)
3. Personal data shall be adequate, relevant and not excessive for the purpose(s).
4. Personal data shall be accurate and up to date.
5. Personal data shall not be kept for longer than is necessary.
6. Personal data shall be processed in accordance with the rights of data subjects.
7. Personal data shall be protected by appropriate technical and organisational security.
8. Personal data shall not be transferred outside the European Economic Area.

6.2 Understanding the use of confidential patient information and consent in relation to disclosure

Clinical team managers must ensure that their patients using their services are aware that the information they give may be recorded, and shared, for the purposes of assessment and treatment, and for the secondary purpose of managing the respective service. Staff should ensure that they are able to explain the implications of disclosing or not disclosing information so that the patient can make valid choices. The Trust can provide information in an accessible format or language if required.

Patients have the right to object to the disclosure of confidential and personal information. Where the patient is competent to make the decision this should be respected. Other than in exceptional circumstances, confidential patient information can only be disclosed to third parties with the informed consent of the patient.

Patient information cannot be used for purposes other than the purposes for which it was originally obtained without seeking patient consent (e.g. for research purposes).

6.3 Exceptions

Confidential personal identifiable information can be disclosed without patient consent (in a patient with capacity to consent) in the following circumstances:

- When statute law requires disclosure
- When there is a court order
- When it may be necessary in the public interest, for example, when there is a risk to others of serious harm or death.

Each case must be considered separately and discussed as indicated with Named Doctor, clinical manager, clinical supervisor, respective safeguarding lead, or Caldicott Guardian. In complex situations or where there is uncertainty senior staff can seek specialist advice.

6.4 Patients who lack capacity

Staff who wish to seek consent for use of personal information from patients whose mental capacity to make such decisions is affected by "an impairment of, or a disturbance in the functioning of, the mind or brain" (physical illness such as dementia, learning disability, brain injury, mental illness) must be familiar with the Mental Capacity Act (2005). The Act is for the protection of those over 16 years who lack capacity to make decisions about themselves. The fact that someone has a mental illness does not necessarily mean that they lack capacity. Also it must be remembered that a lack of capacity may be temporary or permanent. The MCA Code of Practice places certain legal duties on health and social care professionals and also offers general guidance and information to anyone caring for someone who may lack capacity to make a decision.

Each case must be considered separately and discussions with senior staff are good and safe practice.

6.5 General care

- All information relating to patients should be considered by all staff to be sensitive; even a patient's name on a list or a patient's identity in a waiting room is sensitive information.

- No employee should attempt to bypass or defeat the security systems or attempt to obtain or use passwords or privileges issued to other staff or, allow others to do so.

- Do not talk about patients in public places or where you can be overheard.

- If a request for information is made by phone, always try to check the identity of the caller, check whether they are entitled to the information they request. Take a number, verify it independently and call back if necessary.

- Do not leave patients' records or any confidential information lying around unattended.

- Make sure that any computer screens, or other displays of information, cannot be seen by the general public and are protected by passwords and screensavers.

- Any Trust stationery must be stored securely to prevent possible fraudulent use.

- Any redundant equipment, especially computers, laptops must be disposed of through the ICT department in accordance with ICT procedures.

- All letters/reports containing confidential or personal patient or staff identifiable information must always be addressed to a named person.

- All letters/reports (other than appointment letters) containing patient identifiable information must be checked and signed by the author of the letter.

- Internal hard copy mail containing confidential or patient identifiable information should only be sent in a securely sealed envelope, and marked confidential/addressee only.

- External mail containing confidential or patient identifiable information must also be sent in securely sealed envelopes and marked confidential/addressee only. In some circumstances it is also advisable to send information by Recorded Delivery to safeguard that information is only seen by the authorised recipient(s).

- Sometimes a member of staff may recognise somebody coming into the Trust. It may not be obvious whether the person is a patient or visiting. As well as keeping the information confidential, the right to privacy must also be observed.

- Person Identifiable Data stored electronically must be encrypted to NHS standards. Advice on what and how to encrypt is available from the ICT Helpdesk.

- Paper records must be safely and securely stored at night in a locked filing cabinet in a locked room. Tracer systems should be in place for filing cabinet storage to reduce risk of loss of records. Further details on the management of Health records can be found in the Health Records Procedure. No record should be seen by any visitor in a way that could identify a patient.

- Fax is not a permitted method of sending information.

- Staff should consult the Data Protection Procedure and the ICT procedures for detailed information on handling data.

6.6 Children and young people

This is a complex area and there should be a low threshold for consulting with senior clinical staff, the safeguarding lead or with the Caldicott Guardian in the event of uncertainty.

The following basic principles apply:

- Young people are entitled to the same duty of confidentiality as adults.

- Children under 16 who are competent to make decisions about their own treatment are entitled to decide whether personal information may be passed on and generally to have their confidentiality respected (e.g. they may be receiving treatment about which they do not wish their parents to know).

- Decisions to pass on personal information may be taken by a person with parental responsibility in consultation with the health professionals involved only if the child does not have capacity.

- Where there are safeguarding concerns the overriding principle is to secure the best interests of the child. Therefore, if a health professional (or other member of staff) has knowledge of abuse or neglect it is necessary to discuss the issues with senior clinical staff and with the respective safeguarding lead. Information may need to be shared with others and this will be done on a strictly "need to know" basis so that decisions relating to the child's welfare can be taken in the light of all relevant information.

6.7 Audit, teaching, and training

Clinical audit, teaching and training are highly important for the maintenance and improvement of care within the NHS, for inter-agency care and public health generally. Anonymised or aggregated patient information may sometimes be used for these purposes but those handling the data are required to treat it in confidence and must not use it for other purposes. Patients are informed generally (posters, patient information leaflets) about the use of anonymised data in relation to these activities.

6.8 Research and teaching

Patient consent **must** be sought for the use of information in activity relating to teaching or research that would involve them personally.

- Any research proposals involving access to patient records require clearance by a Research Ethics Committee (REC), which must be satisfied that:
    - arrangements to safeguard confidentiality are satisfactory;
    - any additional conditions relating to the use of information that the REC thinks are necessary can be met;
    - patients must have given consent;
    - any published research findings will not identify a patient without specific agreement.

Publications must comply with the Trust's publication guidelines.

7 Training Requirements

Staff must:

- complete local induction
- attend corporate or clinical induction day at the outset of employment
- attend INSET training every two years
- complete annual mandatory IG training and other IG training as required

8 Process for monitoring compliance with this Code

Compliance with this code will be monitored through the applicable requirements of NHS Digital's IG Toolkit.

All staff are duty bound to report an observed breach. Regular audit of patient records may also reveal those instances where lack of knowledge or awareness has caused a breach of confidentiality.

Any identified breach or other confidentiality incident will be reviewed under the arrangements for risk management and reported to the IG work stream of the Clinical Quality Safety and Governance Committee.

The EMT will monitor progress against any action plan agreed to address any breach in compliance with the Code.

9 Associated Policies and Procedures

The Confidentiality Code of Conduct for Staff informs a wide number of Trust Policies and Procedures and should be read in conjunction with the following:

Clinical Record Keeping Standards
Clinical Risk Assessment Procedure
Data Sharing Procedure
Email and Internet Use Procedure
Encryption Procedure
Freedom of Information Procedure
Guidelines for the Use of Patient Information
Health Records Procedure
Incident Reporting Procedure
Information Governance Policy
Mobile Devices Safe Use Procedure
Patient Information Procedure
Procedure for Electronic Communication
Safeguarding Children Policy
Safeguarding of Adults at Risk Policy
Video Recording Consent Procedure

10 References

The Data Protection Act 1998

http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1

Human Rights Act (1998)
http://www.legislation.gov.uk/ukpga/1998/42/contents

Caldicott review: Information governance in the health and care system (2013)
https://www.gov.uk/government/publications/the-information-governance-review

NHS: Confidentiality Code of Practice 2003 (DoH)
http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4069253

NHS: The Care Record Guarantee
http://www.nigb.nhs.uk/guarantee/2009-nhs-crg.pdf

Mental Capacity Act 2005
http://www.legislation.gov.uk/ukpga/2005/9/contents

Mental Capacity Act Code of Practice 2007
https://www.justice.gov.uk/downloads/protecting-the-vulnerable/mca/mca-code-practice-0509.pdf

Information Commissioners Office http://ico.org.uk/

Appendix A: Equality Impact Assessment

Completed by	**Jonathan McKee**
Position	**Governance Manager**
Date	**19.5.16**

The following questions determine whether analysis is needed	**Yes**	**No**
Does the policy affect service users, employees or the wider community? The relevance of a policy to equality depends not just on the number of those affected but on the significance of the effect on them.	X	
Is it likely to affect people with particular protected characteristics differently?		X
Is it a major policy, significantly affecting how Trust services are delivered?	X	
Will the policy have a significant effect on how partner organisations operate in terms of equality?		X
Does the policy relate to functions that have been identified through engagement as being important to people with particular protected characteristics?		X
Does the policy relate to an area with known inequalities?		X
Does the policy relate to any equality objectives that have been set by the Trust?		X
Other?		X

If the answer to *all* of these questions was no, then the assessment is complete.

If the answer to *any* of the questions was yes, then undertake the following analysis:

	Yes	**No**	**Comment**
Do policy outcomes and service take-up differ between people with different protected characteristics?		X	

What are the key findings of any engagement you have undertaken?			The was public engagement at national level
If there is a greater effect on one group, is that consistent with the policy aims?		X	
If the policy has negative effects on people sharing particular characteristics, what steps can be taken to mitigate these effects?			Na
Will the policy deliver practical benefits for certain groups?	X		May encourage users to engage clinically
Does the policy miss opportunities to advance equality of opportunity and foster good relations?		X	
Do other policies need to change to enable this policy to be effective?		X	
Additional comments			

If one or more answers are yes, then the policy may unlawful under the Equality Act 2010 –seek advice from Human Resources (for staff related policies) or the Trust's Equalities Lead (for all other policies).

7 Appendix B : receipt of code form

This form must be signed by all staff and those working for or on behalf of the trust who may have access to confidential information (including contracted consultants, bank, agency, volunteers, locums, student placements, suppliers working on site) Completed forms will be retained for inspection by the HR department

Your personal responsibility concerning security and confidentiality of information (relating to patients, staff and the organisation)

During the course of your time at the Trust, you may acquire or have access to confidential information which must not be disclosed to any other person unless in pursuit of your duties or with specific permission given by a person on behalf of the Trust. This condition applies during your relationship with the Trust and after the relationship ceases.

Confidential information includes all information relating to the Trust and its patients and staff. Such information may relate to patient records, telephone enquiries about patients or staff, electronic databases or methods of communication, use of fax machines, hand-written notes made containing patient information etc. If you are in doubt as to what information may be disclosed, you should check with a manager.

The Data Protection Act 1998 regulates the use of computerised information and paper records of identifiable individuals (patients and staff). The Trust is registered in accordance with this legislation. If you are found to have made an unauthorised disclosure you may face legal action.

I understand that I am bound by a duty of confidentiality and agree to adhere to this Code of Conduct and the requirements of the Data Protection Act 1998.

Print name:	
Signature:	
Date:	
ON BEHALF OF THE TRUST	
Witness Name	
Signature	
Date:	