NHS
South Central
Ambulance Service
NHS Foundation Trust

CODE OF CONDUCT FOR EMPLOYEES IN RESPECT OF CONFIDENTIALITY

South Central Ambulance Service NHS Foundation Trust
Unit 7 & 8, Talisman Business Centre, Talisman Road, Bicester, Oxfordshire, OX26 6HR

DOCUMENT INFORMATION

Author:	Barbara Sansom, Information Governance Manager
Consultation & Approval:	Staff Consultation 21 days Audit Committee: 10th September 2018 Board Ratification: N/A
Equality Impact Assessment:	December 2014 – Stage 1 Assessment undertaken – no issues identified
Data Protection Impact Assessment:	April 2018 – Initial/High Level Assessment undertaken – no issues identified
Notification of Policy Release:	All Recipient email Intranet Website
Date of Issue:	June 2018
Next Review:	June 2021
Version:	**7.0** – content changes to reflect General Data Protection Regulations (GDPR) & Data Protection Act (DPA) 2018 **6.1** no content changes – period extended to 30th June 2018 to allow for review under new DPA / GDPR rules **6** (no content changes)

Contents

Please note that this document should be read and understood prior to the Contract of Employment or other confidentiality agreement being signed. If there is anything that is not clear, please contact your Manager.

1. Purpose of the Code

1.1 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. This is not just a requirement of their contractual responsibilities but also a requirement of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018). In addition for health and other professionals, are bound by their own profession's Code(s) of Conduct.

1.2 Employees are obliged to keep any Personal Confidential Data (PCD), ie personal identifiable information – patient and employee records, strictly confidential. It should be noted that employees also come into contact with nonperson identifiable information which should also be treated with the same degree of care, ie business in confidence information such as patient referral letters.

1.3 Disclosure and sharing of PCD is governed by statutory requirements of Acts of Parliament along with Government and Department of Health Guidelines.

1.4 The principle behind this Code of Practice (Code) is that 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.

1.5 This code has been written to meet the requirements of:

- The General Data Protection Regulation (GDPR) (EU) 2016/679
- Data Protection Act 2018
- The Human Rights Act 1998
- The Computer Misuse Act 1990
- Common Law Duty of Confidence
- The Copyright, Designs & Patent Act 1998
- Caldicott Principles (initial Caldicott Report of 1997 then Review of 2013)
- Confidentiality NHS Code of Practice (Nov 2003 Department of Health)

1.6 This code has been produced to protect staff by making them aware of the correct procedures so that they do not inadvertently breach any of these requirements.

2. Detailed Provisions

2.1 Confidentiality of Information

All employees are responsible for maintaining the confidentiality of information gained during their employment by the Trust.

2.2 Definitions

2.2.1 Confidential information

Confidential information can be anything that relates to patients, staff (including non-contract, volunteers, bank and agency staff, locums, student placements), their family or friends, however stored. For example, information may be held on paper, CD, flash drive, computer file, printout, video, audio, photograph, or even heard by word of mouth. It includes information stored on portable devices such as laptops, palmtops, mobile phones and digital cameras. It can take many forms including medical notes, audits, employee records, occupational health records, along with any Trust Confidential (corporate) information.

2.2.2 Personal data

Personal data or person identifiable information is anything that contains the means to identify an individual, ie name, address, postcode, date of birth, NHS number, National Insurance number, visual images, online identifiers such as IP addresses, etc.

2.2.3 Sensitive data (Special categories of data)

Certain categories of information are legally defined as particularly sensitive and should be most carefully protected by additional requirements stated in legislation (ie information regarding to race/ethnicity, religious beliefs, political opinions, sexual life, physical or mental health or condition, HIV status, pregnancy terminations).

Employees should consider all information to be sensitive with the potential to lead to the identity of an individual and confidentiality standards should be applied to all information that you come into contact with.

Patient identifiable information, including photographs, must <u>not</u> be kept in staff portfolios.

2.3 Requests for Information about Patients

- Unless the individual has consented, NEVER give out information on patients or staff to persons unless that person asking has a “need to know” for the direct care/wellbeing of the individual
- All requests for person identifiable information must have lawful justification which sometimes may need to be provided by the Trust’s Information Governance Manager or Caldicott Guardian
- Any exceptions to these rules may require written consent from the patient in advance of the disclosure. If the patient is unconscious and unable to give consent, then consult with the health professional in charge of the individual’s care.

If you have concerns about disclosing/sharing patient information, you must discuss this with your Manager and if they are not available, someone with the same/similar responsibilities. Do not allow yourself to be pressured into disclosing information – if you have been contacted by telephone and cannot find anyone to discuss the issue with, then take the caller's contact details so you can respond back when you are satisfied that a disclosure can be justified.

2.4 Telephone enquiries

If a request for information is made by telephone:

- Always check the identity of the caller
- Check whether they are entitled to the information they request
- If they are entitled to the information, take a number (try to avoid mobile numbers), verify it independently and then call back with the information.

If in doubt, consult with your Manager or the Information Governance Manager or the Data Protection Officer.

2.5 Requests for information by the Police and the Media

- All types of request for information by the Police should always be referred to the Information Governance team
- All types of request for information by the Media should always be referred to the relevant Communications Manager. Only Senior Manager/Communications Managers are authorised to disclose information to the Media.

2.6 Disclosure of Information to other Employees of the Trust

Information on patients should only be released on a "need to know" basis

- Always check the member of staff is who they say they are (check their ID badge and/or internal extension number) prior to disclosing any information
- Don't be bullied into giving information – if in doubt, check with the consultant/clinician in charge of the patient's care.

2.7 Abuse of Privilege

It is strictly forbidden for employees to look at any information relating to their own family, friends, acquaintances or any other individual unless they are directly involved in that individual's direct clinical care or with the individual's administration on behalf of the Trust. Unlawful access is a breach of confidentiality and a breach of the General Data Protection Regulations / Data Protection Act 2018. This is likely to result in disciplinary action being taken and you may be prosecuted by the Information Commissioner's Office.

If you have any concerns about this issue, please discuss with your Manager, the Information Governance Manager or the Data Protection Officer.

2.8 Carelessness

- Do not talk about patients/individuals in public places or where you can/may be overheard
- Do not leave any medical records or confidential information lying around unattended
- Make sure that any computer screens or other displays of information cannot be seen by others and are **locked** when left unattended
- Remove smartcard from the card reader whenever a computer is left unattended.

2.9 Use of external and internal post

Best practice with regard to confidentiality requires that all correspondence containing personal information should always be addressed to a named recipient. This means personal information/data should be addressed to a person, a post holder, consultant or a legitimate Safe Haven, but not to a department, unit or organisation. In cases where the mail is for a team, it should be addressed to an agreed post holder or team leader.

- Internal mail containing confidential data should only be sent in a securely sealed envelope and marked accordingly, eg “Confidential” or “Addressee Only” as appropriate
- External mail must also observe these rules. Special care should be taken with personal information sent in quantity, such as patient records on paper, disk or other media. These should be sent via trackable mail (ie recorded/registered mail or courier) to safeguard that these are signed for and then seen only by the authorised recipient(s). It is advisable to obtain a receipt of proof of delivery (eg patient records to a solicitor).

2.10 Emailing Confidential Information

2.10.1 Patient identifiers should be removed wherever possible and only the minimum necessary information sent (suggestion - using incident number as opposed to name / address).

2.10.2 Special care should be taken to ensure the information is sent only to recipients who have a right to know and always double check that you are sending the email to the intended recipients only.

2.10.3 The transmission of information **internally** over the Trust network by email or other communication channels such as Skype for business, chats on Microsoft Teams, Yammer, etc, although considered secure, can present confidentiality risks – for example, distributing to those that do not have a “need to know” and the onward transmission/sharing of the content by recipients).

2.10.4 **External** transmissions of information should be considered **insecure** and should never contain identifiable/confidential information. Due to its insecure nature, any information transmitted over the internet should be considered to be in the public domain and therefore should be anonymised or encrypted to prevent inappropriate intervention or disclosure.

2.10.5 Person identifiable/confidential information should **NEVER** be sent to "Hotmail" accounts.

2.10.6 NHS employees do have the facility to send **secure / encrypted** email if they set up an nhs.net email address and transmit to another nhs.net email address. A list of other "secure" recipient addresses (ie .gsi.gov and .pnn.police) is available if required from the Information Governance Manager.

2.10.7 If an employee requires an nhs.net email address, please log an ICT Helpdesk service call.

2.11 Faxing

- Remove patient/person identifiable data from any faxes unless you are faxing to a known secure and private area – so called "Safe Havens"
- Always use a fax header, clearly written with a named recipient/ addressee and state the number of pages being transmitted
- Always check the receiving number to avoid misdialling and ring the recipient to check they have received the fax
- Wherever possible, only transmit information to numbers stored in the machine's memory – to prevent the possibility of misdialling
- If storing a number in the fax memory, ensure it is correct before transmitting sensitive/identifiable information.

2.12 Storage of Confidential Information

Paper and disk based confidential information should always be kept locked away when unattended, particularly at nights and weekends or when the building/office is less occupied for longer periods of time.

PC based information should not be saved onto local hard drives or onto removable media, but onto the Trust's network drives. Disks, CDs and other media should be kept in locked storage

2.13 Disposal of Confidential Information

When disposing of paper-based person/identifiable information or confidential information, always use "confidential waste" sacks/shredders/bins. Waste must be kept in a secure (ie locked) place until it can be collected for secure disposal.

Computer printouts should either be shredded or disposed of as paper-based confidential waste.

Disks/CDs containing confidential information must be either reformatted or destroyed. Computer files with confidential information no longer required must be deleted from both the PC and the server if necessary.

Computer hard disks are securely destroyed/disposed of by an external firm organised through the IT Department within the Trust. This ensures that all information is deleted from the hard drives as re-formatting does not completely delete the original data.

2.14 Confidentiality of Passwords

Personal passwords issued to or created by employees should be regarded as confidential and those passwords must not be communicated to/shared with anyone Employees have a legal responsibility for the content/activity whilst logged in with their username and password

A password is a privilege for the employee to access appropriate systems and work areas. If other colleagues need access to systems/files then they must apply to their Manager for access to be granted if it is considered appropriate.

- Passwords should not be written down
- Passwords should be changed regularly
- A password must be changed straight away if there is suspicion that it has been disclosed/discovered by another individual.

No employee should attempt to bypass the security systems or attempt to obtain or use passwords or privileges issued to other employees. Any attempts to breach security should be immediately reported to the ICT Department and may result in a disciplinary action. Legal action against an employee may also be taken if an issue breaches the GDPR and DPA 2018 or the Computer Misuse Act 1990

2.15 Working Remotely or at Home

It is sometimes necessary for employees to work remotely or from their home. If this is necessary and if access is required to Trust information, networks and files, then authorisation must be sought initially from the individual’s Manager. If it is agreed, employees must consider their personal liability under the GDPR and DPA 2018 and their Contract of Employment for any breaches of requirements.

- An employee’s Manager must approve the removal of any records for remote working
- If manual records are being taken off-site, this must be documented (ie signed out and then signed back in again on their return).

This is particularly important for patient/staff records and their removal from site should be actively discouraged unless absolutely necessary for the task required. Employees must:

- Ensure any manual (patient/staff/confidential) or electronic (disk/CDs) records are afforded all possible steps to protect the information

- Make sure the information is held out of sight (in the boot of a car for example) during transit or carried in person securely
- Not let anyone else have access to the information/record.

If an employee is authorised to take home computer records on disk/CD then he/she must ensure all of the above apply. The Trust discourages the use of personal devices for work related activity but if it is unavoidable and if information is being put onto a non-Trust PC, then the employee has a duty to ensure that no one else can access the information and that the information is removed again once the work is finished.

When taking records back to work, they must be securely carried (as described above) and logged/signed back in again. Disks/CDs must be virus checked before being (re)loaded onto any Trust systems, especially any which can be accessed via the network

2.16 Copying of Software

All computer software used within the Trust is regulated by licence agreements. A breach of licence agreement could lead to legal action against the Organisation and/or the "offender".

It is important that software on the PCs/systems used for work purposes must not be copied and used for personal use – such activity would breach a licence agreement.

3. General Provisions

3.1 Interpretation

If any person requires an explanation concerning the interpretation or the relevance of this code of conduct, they should discuss the matter with their Manager and if further clarification is required, refer to the Information Governance Manager or the Data Protection Officer or Caldicott Guardian (Director of Patient Care).

3.2 Non-compliance

Non-compliance with this Code of Conduct by any individual working for the Trust may result in disciplinary action being taken in accordance with the Trust's disciplinary procedure and could lead to dismissal for gross misconduct.

To obtain a copy of the disciplinary procedures, please refer to the intranet/website or discuss with your Manager or the Human Resources department.

3.3 Amendments

This Code will be amended as necessary to reflect the Trust's development of policies and procedures and the changing needs of the NHS.

4. Equality Statement

4.1 The Trust is committed to promoting positive measures that eliminate all forms of unlawful or unfair discrimination on the grounds of age, marital status, disability, race, nationality, gender, religion, sexual orientation, gender reassignment, ethnic or national origin, beliefs, domestic circumstances, social and employment status, political affiliation or trade union membership, HIV status or any other basis not justified by law or relevant to the requirements of the post.

4.2 By committing to a policy encouraging equality of opportunity and diversity, the Trust values differences between members of the community and within its existing workforce, and actively seeks to benefit from their differing skills, knowledge, and experiences in order to provide an exemplary healthcare service. The Trust is committed to promoting equality and diversity best practice both within the workforce and in any other area where it has influence.

4.3 The Trust will therefore take every possible step to ensure that this procedure is applied fairly to all employees regardless of race, ethnic or national origin, colour or nationality; gender (including marital status); age; disability; sexual orientation; religion or belief; length of service, whether full or part-time or employed under a permanent or a fixed-term contract or any other irrelevant factor.

4.4 Where there are barriers to understanding e.g. an employee has difficulty in reading or writing or where English is not their first language additional support will be put in place wherever necessary to ensure that the process to be followed is understood and that the employee is not disadvantaged at any stage in the procedure. Further information on the support available can be sought from the Human Resource Department.

This Code of Conduct will be included in any induction processed throughout the Trust and will be added as an appendix to the Confidentiality Policy.

Appendix 1

A confidentiality form for all employees – including contracted employees, non-contract employees, bank and agency staff, volunteers, locums, student placements, suppliers (ie cleaners, engineers) – needs to be signed.

Many of our policies have an ‘Internal staff form’ attached that is relevant to the document. The ‘Confidentiality agreement’ form is included with this policy but for security and accessibility reasons it is only available on our Staff Intranet..