South Central Ambulance Service
NHS Foundation Trust

CORPORATE POLICY & PROCEDURE NO. 8

CONFIDENTIALITY POLICY

June 2018

DOCUMENT INFORMATION	
Author: Barbara Sansom, Information Governance Manager	**Consultation & Approval** Staff Consultation N/A (no content changes) Audit Committee: January 2015 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

1 Introduction

This Policy details the general responsibilities for confidentiality within the Trust, including the responsibilities for ensuring confidentiality of patient related data and requirements under the General Data Protectio4n Regulation (GDPR) (EU) 2016/679, Data Protection Act 2018 (DPA2018) and the Caldicott Report & Review 1997/2013

This Policy, together with other policies and procedures detailed in Related Documents below, will ensure that the Trust operates in such a way that our stakeholders will have confidence in us

This Policy should also be read in conjunction with the various IM&T Department Policies which outline the requirements when using technology in conjunction with daily activities

This document

- Introduces the concept of confidentiality
- Provides a high level description of the main legal requirements including the GDPR, DPA 2018 and the Caldicott Report & Review 1997/2013
- Introduces the concept of information sharing
- Is a key component of Information Governance arrangements for the NHS

This document is based upon the Department of Health "Confidentiality: a Code of Practice for NHS Staff" which was published in November 2003

2 Glossary of Terms

2.1 Anonymised Information

This is information which does not identify an individual directly and which cannot reasonably be used to determine identity. Anonymisation requires the removal of name, address, full post code, date of birth, or any other details or combination of details that may lead to identification

2.2 Clinical Audit

The evaluation of clinical performance against standards or through comparative analysis, with the aim of informing the management of services. This should be distinguished from studies that aim to derive, scientifically confirm and publish generalised knowledge

2.3 Direct Care Purposes (previously known as Healthcare Purposes)

These include all activities that directly contribute to the diagnosis, care and treatment of an individual and the audit/assurance of the quality of the healthcare provided. They do not include research, teaching, financial audit and other management activities

2.4 Disclosure

The divulging or release or provision of access to data

2.5 Information Sharing & Protocols

Document rules and procedures for the disclosure/sharing of patient information between two or more organisations or agencies. The procedures specifically relate to security, confidentiality, data handling and destruction and must provide a lawful justification for the disclosure/sharing to take place

2.6 Legitimate Relationship

The legal relationship that exists between an individual and the health and social care professionals and staff providing or supporting their care

2.7 Medical Purposes

As defined in the Data Protection Act 2018, medical purposes include but are wider than healthcare purposes. They include preventative medicine, medical research, financial audit and management of healthcare services. The Health and Social Care Act 2001/2012 explicitly broadened the definition to include social care

2.8 Patient / Person Identifiable Information

Any data/information which relates to an individual which alone, or with other data/information can lead to the identity of that individual. This can include

- Individual's name, address, post code, date of birth
- Pictures, photographs, videos, audio-tapes, CDs or other images/recordings
- NHS number and local patient identifiable codes
- Online identifiers such as IP addresses
- Anything else that may be used to identify an individual. For example, rare diseases, drug treatments or statistical analyses which have very small numbers within a small population may allow individuals to be identified

2.9 Public Interest

Exceptional circumstances that justify overruling the right of an individual to confidentiality in order to serve a broader societal interest. Decisions about the public interest are complex and must take account of both the potential harm that disclosure may cause and the interest of society in the continued provision of confidential health services

2.10 Sensitive / Special Categories of Personal Data

Means personal data consisting of information such as

- The racial or ethnic origin of the individual
- His/her political opinions
- His/her religious beliefs or other beliefs of a similar nature
- Whether he/she is a member of a trade union (as defined by the Trade Union and Labour Relations (Consolidation) Act 1992)
- His/her physical or mental health or condition

- His/her sexual life
- HIV status

Personal information relating to criminal offences and convictions require extra safeguards before it can be processed. Such information includes

- The commission or alleged commission by him/her of any offence
- Any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings

3 What is Confidential Information?

A duty of confidence arises when one person shares information with another in circumstances where it is reasonable to expect that the information will be held in confidence

This confidence is

- A legal requirement, which is backed up by case law (the Common Law Duty)
- A requirement of professional codes of conduct
- A specific requirement of Trust Contracts of Employment and is linked with disciplinary procedures

3.1 Compliance

All personnel are required to comply with the general provisions of this document and with the specific requirements of their departments

3.2 Failure to comply will be treated as a disciplinary offence

Patients entrust us with the most sensitive of personal information, which relates to their health and many other matters in the course of our contact with them. Not only do they give us this information, they also allow us to gather information from other sources. They do this because they have confidence in us to treat this information in an appropriate fashion and have a legitimate expectation that all Trust employees will respect their privacy and act appropriately.

On occasions the patient will be unable to extend this trust, either through lack of competence or they may be unconscious. This in no way diminishes our responsibilities.

It is essential that the Trust operates in such a way that our legal obligations are met and the trust of the patient is retained. Without this, it is impossible for the Trust to offer the type of service that it prides itself on.

Information that can identify an individual patient must not be disclosed or used for any other purpose except for the provision of the healthcare of that individual, without the explicit consent of that patient, or where there is a lawful basis to do so. Where a lawful basis meeting the requirements of the GDPR cannot be established, then anonymised information should be used, which can be passed with few constraints

4 Information Sharing

There are many occasions when information needs to be shared with other service providers and, indeed, areas that are not directly associated with care, such as clinical audits.

It is imperative that our patients are aware that information must be shared. A patient would expect information to be shared with other service providers, but would not perhaps, expect clinical governance or clinical audit teams to be privy to their records.

It is a legal requirement to inform patients of the full extent of information sharing. This is explained in our Privacy Notice which is available on the Trusts website. This should also be done with Patient Information leaflets, provided when a request for information, complaint, or Patient Experience request is made by a patient or their representative. There should also be laminated sheets displayed in Ambulances explaining how the information may be used. It is particularly important that patients are aware that, on occasion, information is released to non-NHS bodies.

Less obvious still, is the need for confidential information to be shared with areas that do not contribute to or support the healthcare that a patient is receiving. Although the patient may not consider these areas important, they underpin the functioning of the NHS and contribute to the society that we live in. Examples of these are medical research, health service management and financial audit.

4.1 Patient Consent to Sharing

Patient consent should be sought before their information is released. However, there are situations where consent cannot be obtained for the use of disclosure of patient identifiable information, yet the public good for this outweighs issues of privacy. S251 of the Health and Social Care Act 2012 currently provides an interim power to ensure that patient identifiable information, needed to support a range of important work such as clinical audit, record validation and research, can be used without the consent of patients

4.2 Information Sharing outside the NHS

When information needs to be shared outside the NHS, wherever possible, it should be anonymised. In such cases, we must observe the following

- If the information is shared with other organisations, they must have equal or superior levels of information governance, security and confidentiality
- It continues to be our responsibility to ensure this information is protected, therefore we must seek assurances that this is the case

Therefore it is vital that we establish who, where and why we are sharing information and what will happen to it once it leaves our care, including emphasis on the need to use and dispose of this disclosure appropriately. Protocols are in existence with some external organisations and assistance should be sought from the Caldicott Guardian or Information Governance Manager if there are any concerns or queries regarding the need to share such information

4.3 Obligations on individuals working in the NHS

All employees are required to meet the standards and practices laid out in this document in addition to the requirements of their contracts of employment. These form the very core of good practice

If particular issues arise, then these must be reported through the employee's line manager to the Information Governance Manager or the Caldicott Guardian of the Trust

5 Responsibilities for Confidentiality

The Chief Executive Officer (CEO) is responsible to the Department of Health for the Trust's compliance with all current information security directives and legislation. The CEO exercises these responsibilities through the Director of Patient Care as Caldicott Guardian, the Director of Finance as Senior Information Risk Owner (SIRO), the Associate Director of Information Management & Technology (IM&T), the Clinical Governance Committee and the Information Governance Steering Group

The Caldicott Guardian is an executive member of the Trust Board who is responsible, among other issues, for agreeing and reviewing the internal protocols governing the protection and use of patient related data by employees of the Trust

The Director Finance, as SIRO is responsible for ensuring periodic audit reviews of confidentiality and reporting corrective action, as appropriate

The Information Governance Manager supports the Director of Patient Care in relation to Caldicott and the Associate Director of IM&T on Data Protection and wider Information Governance issues

The Data Protection Officer informs and advises the Trust of obligations under the GDPR and DPA 2018. The DPO will monitor compliance with the policies of the Trust in relation to the protection of personal data and will train staff and raise awareness as the need arises.

The Heads of ICT report to the Associate Director of IM&T and are responsible for overseeing aspects of confidentiality within the Trust related to IT. The specific duties are

- To advise managers and procurement staff on the security requirements associated with the purchase of new systems
- To advise the Capital Planning Group
- To advise the Trust, via the Clinical Governance Committee and the Information Governance Steering Group, on confidentiality issues and related matters with regards to IT
- To ensure IT policy is current with regards to confidentiality

The Information Governance Steering Group meets quarterly to consider, amongst other things, all aspects of patient and personal data

All staff

- Need to be aware of the issues surrounding confidentiality and seek training or support where uncertain, in order to deal with them appropriately (ignorance is no excuse)
- Must work with Trust policies and procedures and be able to demonstrate that they are making every reasonable effort to comply with them

6 Confidentiality of information

6.1 Protect Patient and Personal Information

Patient's health information and their interests must be protected at all times through a number of measures, as should personal information relating to employees and other stakeholders

- Recognising that confidentiality is an obligation for all staff, contractors, volunteers and temporary staff with no exceptions
- Patient and personal information must be recorded accurately and consistently
- Patient and personal information is private and must remain so
- Patient and personal information, in all its various formats, must be kept physically secure
- Exceptional care must be taken when sharing information with other bodies and agencies and where appropriate ensure an information sharing agreement is in place.

6.2 Inform Patients Effectively

Patients should, where possible, be fully aware that information about them may be recorded, may be shared to provide them with the care they need and may be used for the purposes not directly associated with their care such as clinical audit and other methods of monitoring the quality of care provided

7 Using and sharing confidential patient information

The use and sharing of confidential patient information must be both lawful and ethical. Although lawful and ethical are largely in step with each other, there are minimum legal requirements, which provide a minimum standard to work to. These minimum legal requirements may not reflect the appropriate ethical standards laid down by professional bodies.

Although there is no clear legal obligation of confidentiality to the deceased, there is an ethical basis for requiring confidentiality to continue to apply. More detail can be found in the Public Records Act 1967 and the Access to Health Records Act 1990

There are a number of legal documents that cover the disclosure of confidential information, the outlines of which can be found below. These outlines are for guidance only and should not be seen as the definitive resource

7.1 Common Law of Confidentiality

Common law is not a single bill or Act of Parliament but is built up from a number of individual cases where judgements have been made. The underlying principle is that information that has been confided must not be used or disclosed, except as originally understood by the confider or with their permission

In very exceptional circumstances, confidentiality may be broken for the "public interest". However these judgements are made on a case by case basis and are very rare

The Common law of confidentiality can be overridden or set aside by legislation

7.2 General Data Protection Regulation (GDPR) / Data Protection Act 2018 (DPA 2018)

The new legislation became law on 25 May 2018 and establishes a framework of rights and duties which are designed to safeguard personal data. Although this is a complex piece of legislation, full details and explanations can be found at www.ico.gov.uk the website of the Information Commissioner's Office.

The legislation covers all forms of recorded data that relates to a living individual, in whatever format it may be stored – on computer, manual records, microfilm, CD, audio, video etc

It is everyone's legal obligation to observe all principles at all times and staff should be familiar with their obligations under the Trust's Data Protection Policy

7.3 Human Rights Act 1998

The Human Rights Act became law in the UK in October 2000. It incorporates the rights and freedoms set out in the European Convention for Human Rights. The UK courts must take into consideration, the decisions made by the European Court of Human Rights

The Act applies to all public authorities and established a right to "respect for private and family life" which underscores the duty to protect the privacy of individuals and protect confidentiality. Current understanding is that compliance with the Data Protection Act 2018 and the common law of confidentiality should satisfy the Human Rights Act requirements.

Legislation generally must also be compatible with the provisions of the Human Rights Act, so any proposed setting aside obligations of confidentiality through legislation must:

- Pursue a legitimate aim
- Be considered necessary in a democratic society

- Be proportionate to the need

7.4 Access to Health Records Act 1990

This Act has now been repealed by the Data Protection Act 1998, which in turn has been replaced by the Data Protection Act 2018, except in sections that deal with the records of the deceased

7.5 Freedom of Information Act 2000

The right under the Freedom of Information Act to request official information held by public bodies (known as Right to Know) came into force in January 2005. This is governed by the Trust's Freedom of Information Policy

8 Protecting information

8.1 Confidentiality obligation for staff

The duty of confidentiality arises out of common law, professional obligations and the Contract of Employment. Breaching confidentiality – by improper use of health records, computer misuse or any other manner may lead to disciplinary action being taken. It could also call into question any professional registration and could lead to possible legal proceedings.

Voluntary staff and external contractors are also bound by the same terms of confidentiality and must sign an Agreement indicating that they understand fully what is required of them when working with the NHS (See Appendices)

8.2 Recording patient information accurately

Maintaining proper records is vital to patient care. If records are inaccurate, future decisions may be wrong and harm the patient. If information is recorded inconsistently, then records are harder to interpret, resulting in delays and possible errors. The information may be needed not only for the immediate treatment of the patient and the audit of that care, but also to support future research that can lead to better treatments in the future. The practical value of privacy enhancing measures and anonymisation techniques will be undermined if the information they are designed to safeguard is unreliable

8.3 Keeping information private

Key points are

- Not gossiping – this is clearly an improper use of confidential information, whether it be about the Trust, colleagues or patients
- Taking care when discussing cases in public places – there are obviously occasions when it is necessary to discuss cases with colleagues for professional reasons – this can be to gain advice and to share experiences and knowledge, but care must be taken to ensure that these discussions are not overheard. Rarely would there be a need to reveal the identity of the patient concerned

8.4 Accurate Recording of Patient Information

It is imperative that patient information is recorded both accurately and consistently. If it is not, then the resulting errors can directly affect patient care. The information may also be needed for future audit of the care the patient received and in future research. If the recorded information is not of a suitably high standard, then it is devalued.

8.5 Record keeping good practice

Patient records should

- Be factual , consistent and accurate
- Be written as soon as possible after an event has occurred, providing current information on the care and condition of the patient
- Be written clearly, legibly and in such a manner that they cannot be erased
- Be written in such a manner that any alterations or additions are dated, timed and signed in such a way that the original entry can still be read clearly
- Be accurately dated, timed and signed, with the name of the author being printed alongside the first entry
- Be readable on any photocopies
- Be written, wherever possible, with the involvement of the patient or carer
- Be clear, unambiguous, concise and written in terms that the patient can understand. Abbreviations should not be used, but if so, should follow common conventions
- Be consecutive
- Use standard coding techniques and protocols in electronic records

Be relevant and useful

- Identifying problems that have arisen and the action taken to rectify them
- Providing evidence of the care planned, the decisions made, the care delivered and the information shared
- Providing evidence of actions agreed with the patient (including consent to treatment and/or consent to share)

And include

- Medical observations, advice given, examinations, tests, diagnoses, prognoses, prescription and treatment
- Relevant disclosures by the patient – pertinent to understanding cause or effecting cure/treatment
- Facts presented to the patient
- Correspondence from the patient or other parties

Patient records should not include

- Unnecessary abbreviations, jargon, meaningless phrases, irrelevant speculation and offensive subjective statements

- Personal opinions regarding the patient – restrict to professional judgements on clinical matters

8.6 Physical and Electronic Security of Information

The security of both manual and electronic patient/staff records is obviously key to maintaining confidentiality, whether these records are on site or need to be taken away from site, certain practices must be followed as listed below

8.6.1 For all types of records, staff working in offices where records may be seen must:

- Shut/lock doors and cabinets
- Wear building passes/ID at all times
- Query strangers – why are they here?
- Tell the relevant people if you see anything remotely suspicious
- Do not tell unauthorised people how security systems work
- Do not breach security or fail to comply with this and associated policies

8.6.2 Manual records must be:

- Formally booked out from the normal filing system – not simply "borrowed"
- Tracked if transferred, with a note made or sent to the location of the transfer
- Returned to the filing location as soon as possible after use
- Stored securely within office, arranged so that the record can be found easily if needed urgently
- Stored closed when not in use, so that accidental viewing is prevented
- Inaccessible to the public and not left, even for the shortest of times
- Held in secure storage with clear labelling

8.6.3 With electronic records, staff must:

- Always log-out of any computer system or application when work is finished
- Never leave a computer logged on and unattended, even for the shortest of time
- Never share log-ins with other people. If other staff need to access records, then appropriate access should be organised for them
- Never reveal passwords to anyone else
- Change your password when requested to do so
- Avoid short or obvious passwords, such as pets name or car registration

- Use password protected screensavers at all times
- Remove smartcard from card reader whenever leaving a computer unattended

Failure to comply with these measures may lead to disciplinary action

9 The Caldicott Report – Sharing with care

Sharing information within the NHS and other associated agencies is imperative for ensuring good quality care to all our patients. However, such information sharing can also introduce potential threats to confidentiality. The Caldicott Report was commissioned in 1997 to set a standard to information sharing that all NHS Trusts were to work to. This original report quoted 6 mains principles for safe/appropriate sharing of information. The Caldicott Review of 2013 reiterated the requirement for appropriate information sharing and added a seventh principle.

The seven Caldicott Principles are

1. Justify the purpose(s)
   Every proposed use or transfer of patient-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by an appropriate guardian

2. Don't use patient-identifiable information unless it is absolutely necessary
   Patient-identifiable information items should not be included unless it is essential for the specified purpose(s) of that flow and justified as lawful. The need for patients to be identified should be considered at each stage of satisfying the purpose(s)

3. Use the minimum necessary patient-identifiable information
   Where use of patient-identifiable information is considered to be essential, the inclusion of each individual item of information should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as is necessary for a given function to be carried out

4. Access to patient-identifiable information should be on a strict need to know basis
   Only those individuals who need access to patient-identifiable information should have access to it and they should only have access to the information items that they need to see. This may mean introducing access controls or splitting information flows where one information flow is used for several purposes

5. Everyone with access to patient-identifiable information should be aware of their responsibilities

Action should be taken to ensure that those handling patient-identifiable information – both clinical and non-clinical staff – are made fully aware of their responsibilities and obligations to respect patient confidentiality

6. Understand and comply with the law
   Every use of patient-identifiable information must be lawful. Someone in each organisation handling patient information should be responsible for ensuring that the organisation complies with legal requirements

7. The duty to share information can be as important as the duty to protect patient confidentiality
   Health and social care professions should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies

10 Communication ground rules

With so many means of communication now available, it is useful to have some ground rules to follow to ensure that information does not go astray. These rules are designed to ensure that information is transferred with minimum risk. You should also make yourself aware of any local requirements

10.1 Email

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

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

The transmission of information by email **internally** over the Trust network 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)

10.2 External Communication

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.

Identifiable/confidential information should **NEVER** be sent to “Hotmail” accounts

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

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

10.3 Fax

- 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

10.4 Phone

- Confirm the name, job title, department and organisation of the person requesting the information
- Confirm the reason for the information request if appropriate
- Take a contact telephone number, eg main switchboard – never a direct line or mobile number
- Check whether the information can be provided. If in doubt, check
- Provide the information only to the person who has requested it – never leave messages with another person or on an answering machine
- Ensure that you record your name, date and the time of disclosure, the reason for it and who authorised it. Also record the recipient’s name, job title, organisation and telephone number

10.5 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)

10.6 Disclosing personal information to the Police

Under both the Data Protection Act 2018 and the Caldicott guidance, The Trust is under a duty to keep personal/patient information confidential and secure. There are, however, a few exceptions to this; the most relevant to the Trust is when dealing with the police.

If you are requested by the police to disclose personal information you must refuse, unless that person has given their consent for this information to be released or there are circumstances present which allow for the release without consent (below). It is not, however, enough to accept verbal consent. You must obtain written consent from the patient, which must be kept on record. Also be aware that any information released should have any reference to a third party, other than a health professional, deleted before release. All requests for information have to be authorised by the Caldicott Guardian or authorised Information Governance Manager or travel through agreed safe haven procedures before release.

However, there are a few exceptions to the above where the police may insist on information being released:

10.6.1 Prevention of Terrorism Act (1980) and Terrorism Act (2000)

If you gain information, including personal information about terrorist activity you must inform the police.

10.6.2 The Road Traffic Act (1988)

You have a duty to inform the police when asked the name and address of any driver who is allegedly guilty of an offence under this act. Clinical information, however, must not be disclosed.

10.6.3 The Police and Criminal Evidence Act 1984

You can pass on information to the police if you believe someone may be seriously harmed or death may occur if the police are not informed. Serious arrestable offences include murder, rape, kidnapping and causing death by dangerous driving.

10.6.4 The Children Act 2004

There is no single piece of legislation which covers Child Protection but a large number of constantly changing laws and guidance. Information relating to a child may be passed without the parent's permission where the child is in a position of potential harm.

10.6.5 Data Protection Act 2018 Exemption – Schedule 2, Part 1, Paragraph 2

The police may also seek personal information under an exemption of the Data Protection Act 2018 Exemption – Schedule 2, Part 1, Paragraph 2. The exemption is used by the police when making enquiries which relate to

- The prevention and detection of crime
- The apprehension and prosecution of offenders

The police need to produce a form requesting the information, which has been signed by a police inspector.

Information should only be supplied if it is considered appropriate, or if the police issue a formal court order giving them the right to access the patients' personal information.

Staff should not feel pressured or intimidated into giving the police information, It is perfectly reasonable and good practice to ask why the information is needed and exactly what is required before deciding whether it is appropriate to release the information.

Important

If you are unsure whether you should be releasing information to the police or not, then you **must** check with your manager, Caldicott Guardian or Information Governance Manager.

Do not assume the police are entitled to view this information

11 Incident reporting

Confidentiality concerns of any sort are reportable occurrences and must be brought to the attention of the Information Governance Manager without delay and in accordance with the Trust's Risk Management and Incident Reporting Policy

It is as much an offence to have knowledge of a potential confidentiality problem and to have taken no action, as it is to be the cause of an actual incident

12 Related Documents

- Risk Management and Incident Reporting Procedure.

- Confidentiality Code of Conduct
- Data Protection Policy
- Freedom of Information Policy
- Information Management and Technology Policy
- Confidentiality Agreement for Staff
- Confidentiality Agreement for External Contractors
- Patient related information to Third parties – Including the Police
- Information Sharing Protocols

Appendix 1: Confidentiality Agreement

CONFIDENTIALITY AGREEMENT

THIS AGREEMENT is made on (insert date here)
BETWEEN

1) South Central Ambulance Service NHS Foundation Trust of 7-8 Talisman Business Centre, Talisman Road, Bicester, Oxon, OX26 6HR ("the Trust") and;

2) [ ] of [insert address] ("the Recipient")

WHEREAS The Recipient

The Recipient being either an external contractor, supplier or Consultant acknowledges that, by virtue of their position and in carrying out the duties associated with their role with the Trust, they will have access to and will receive from the Trust Confidential Information (as defined below)

NOW IT IS HEREBY AGREED as follows:

1 DEFINITION

In this Agreement Confidential Information" means any information which may be disclosed to the Recipient in anyway whatsoever relating to purchasers, marketing and sales plans and information, pricing information, annual and strategic plans, Trust secrets, information concerning employees or patients, information relating to financial and business dealings, research activities policies, procedures, service orders or any other document marked confidential or which the Recipient is advised to be confidential or which it might reasonably expect to be regarded by the Trust as confidential.

2 UNDERTAKING

2.1 In consideration of the disclosure to the Recipient of Confidential Information the Recipient undertakes that neither during its term of office or after the termination of such and without limitation of time it will not:-

2.1.1 publish, disclose or otherwise communicate to any person, company, business entity or other organisation whatsoever, any or Confidential Information;

2.1.2 make use of any Confidential Information for its own purposes or benefit, or for the purpose or benefit of any other person, company, business entity or other organisation whatsoever.

2.2 The Recipient undertakes to notify the Trust immediately of any breach of the obligations of confidentiality to which the Recipient is subject to by the operation of clauses 2.1 and 2.2. The Recipient further undertakes to take such action as the Trust may reasonably require to prevent further breaches or to restrain unauthorised use of the Confidential Information.

2.3 The Recipient undertakes not to make or retain any copy of, nor make any notes, nor remove from the premises of the Trust, Confidential Information, save with the prior written consent of the Trust and to the extent that such copying or making of notes is strictly necessary for the proper and efficient discharge of its duties.

2.4 In the event of any such authorised removal or copying of Confidential Information, the Recipient shall return such documents, papers, copies or notes to the Trust after the authorised purpose has ceased or has been completed or on demand by the Trust.

4 LIMITATION

The Recipient's obligations shall not apply in relation to any Confidential Information which:-

4.1 it is required by law or any Court or other similar judicial body or authority to disclose, publish or communicate;

4.2 has come into the public domain other than by way of unauthorised disclosure whether by its or by any other person, company, business entity or other organisation whatsoever.

5 ENFORCEMENT

5.1 Any failure by the Trust in exercising any right, power or privilege under this Agreement shall not act as a waiver hereunder, nor shall any single or partial such exercise preclude any further such exercise.

5.2 The Recipient acknowledges that damages alone would not be an adequate remedy for any breach of the provisions of this Agreement and that (without prejudice to any and all other rights or remedies the Trust may have) the Trust shall be entitled to apply for the remedies of injunction, specific performance and other equitable relief for any threatened or actual breach of the provisions of this Agreement without being required to adduce proof of special damages.

5.3 The Recipient undertakes to indemnify the Trust on a continuing basis against all costs, claims, losses, liabilities, injuries or expenses (including legal expenses)

incurred or suffered by it as a result of any breach by the Recipient of this Agreement.

6 GOVERNING LAW

This Agreement shall be governed and interpreted in accordance with the laws of England and any disputes arising in relation hereto shall be submitted to the exclusive jurisdiction of the English courts.

7 SUCCESSORS AND ASSIGNS

This Agreement shall continue for the benefit of the parties and their respective successors in title.

8 THIRD PARTY RIGHTS

A person who is not a party to this Agreement has no rights under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Agreement but this does not affect any right or remedy of a third party which exists or is available apart from that Act.

9. NOTICES

All notices, requests, demands or other communications to or upon the parties shall be in writing and delivered by first class post to the address of the respective party as set out above.

This Agreement has been entered into on the date at page 1.

Signed by [ ]
as authorised signatory for and on behalf of
South Central Ambulance Service NHS Foundation Trust ……
[insert position]

Signed by [ ]
as authorised Signatory for and on behalf of ……
[ ] [insert position]

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

During the course of your time within the Trust buildings, 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 employees. 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 or corporate details. If you are in doubt as to what information may be disclosed, you should check with a manager.

The Data Protection Act 2018 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 2018.

PRINT NAME:	
SIGNATURE:	
DATE:	
ON BEHALF OF THE TRUST	
WITNESS/MANAGERS NAME:	
SIGNATURE	
DATE	