



Confidentiality Code of Conduct

| | |
|-----------------|----------|
| Document Status | Approved |
| Version: | 4.0 |

| DOCUMENT CHANGE HISTORY | | |
|-------------------------|------------------|--|
| Initiated by | Date | Author |
| | | Andrew Broad |
| Version | Date | Comments (i.e. viewed, or reviewed, amended approved by person or committee) |
| 1.0 | | Approved |
| 2.0 | July 2012 | Approved at EMT |
| 3.0 | December 2014 | Extension of review date approved by EMB |
| 3.1 | October 2016 | Review By IG Manager Jill Moseley |
| 3.1 | 19 October 2016 | Recommended by IGG |
| 4.0 | 17 November 2016 | Approved by ELB |

| | |
|------------------------------------|---|
| Document Reference | Standards For Better Health – Relevant to standard(s) Relevant Trust objective: Directorate |
| Recommended at Date | Information Governance Group 19 th October 2016 |
| Approved at Date | Executive Leadership Board 17 th November 2016 |
| Review date of approved document | September 2019 |
| Equality Analysis | October 2016 |
| Linked procedural documents | Safe Haven Procedure Release of Information Procedure NHS Code of Confidentiality Nov. 2003 Data Protection Act 1998 Information Security Policy Professional Codes of Practice Common Law Duty of Confidence Employment Contract – Confidentiality Clause Caldicott principles, Caldicott2, Caldicott Review of Data Security, Consent and Opt-Outs. |
| Dissemination requirements | All Trust staff |
| Checklist completed? | No |
| Part of Trust's publication scheme | No |

The East of England Ambulance Service NHS Trust has made every effort to ensure this policy does not have the effect of discriminating, directly or indirectly, against employees, patients, contractors or visitors on the grounds of age, ethnic origin, gender, transgender, sexual orientation, marital status (including civil partnerships), religion and belief, maternity and pregnancy or disability. This policy will apply to all staff regardless of position or status including volunteers. All East of England Ambulance Service NHS Trust policies can be provided in alternative formats.

Contents

| Paragraph | Page |
|--|-------------|
| 1. Introduction | 5 |
| 2. Purpose | 5 |
| 3. Duties | 6 |
| 3.1 Chief Executive | 6 |
| 3.2 Caldicott Guardian | 6 |
| 3.3 Compliance and Standards Lead | 6 |
| 3.4 Information Governance Manager | 6 |
| 3.5 EEAST Staff | 6 |
| 3.6 Consultation and Communication with Stakeholders | 7 |
| 4. Definitions | 7 |
| 4.1 Confidentiality | 7 |
| 4.2 Confidential Information | 7 |
| 4.3 Caldicott Principles | 8 |
| 4.4 Safe Havens | 8 |
| 5. Development | 8 |
| 5.1 Prioritisation of Work | 8 |
| 5.2 Identification of Stakeholders | 8 |
| 5.3 Responsibility for Document's Development | 8 |
| 6. Disclosure of Confidential Information | 8 |
| 6.1 Intranet, Internet, Website, Journals, etc. | 9 |
| 6.2 Disclosure of Information to Other Employees of the Trust | 9 |
| 6.3 Disclosure of Information to Other Organisations | 9 |
| 6.4 Telephone Enquiries | 10 |
| 6.5 Requests for Information by the Police | 10 |
| 6.6 Requests for Information by the Media | 10 |
| 6.7 Clinical Audit | 10 |
| 6.8 Disclosure of Information for Other Non-Medical Purposes | 12 |
| 6.9 Disclosure of Information for Medical Purposes Other than Healthcare | 12 |
| 7. Safeguarding Information | 12 |
| 7.1 General | 12 |
| 7.2 Storage of Confidential Information | 13 |
| 7.3 Confidentiality of Passwords | 13 |
| 8. Sending and Receiving Information | 13 |
| 8.1 Use of Internal and External Post | 13 |
| 8.2 Faxing | 14 |

Confidentiality Code of Conduct

| | | |
|-----|---|----|
| 8.3 | E-mailing Confidential Information | 14 |
| 9. | Disposal of Confidential Information | 15 |
| 9.1 | CDs/memory pens | 15 |
| 9.2 | Computer Hard Disks | 15 |
| 10. | Working From Home | 15 |
| 11. | Copying Software | 16 |
| 12. | Patients' Rights | 17 |
| 13. | Freedom of Information | 17 |
| 14. | Training | 17 |
| 15. | General Provisions | 17 |
| 16. | Data Protection Act | 17 |
| 17. | Abuse of Privilege | 18 |
| 18. | Non-Compliance | 18 |
| 19. | Possible Breaches or Risk of Breach | 18 |
| 20. | Amendments | 18 |
| 21. | Equality Analysis | 18 |
| 22. | Process for Monitoring Compliance and Effectiveness | 19 |
| 23. | Standards/Key Performance Indicators | 19 |
| 24. | References | 19 |
| 25. | Associated Documents | 19 |

Appendices

| | |
|--|----|
| Appendix A – Summary Confidentiality Code of Conduct for Employees | 20 |
| Appendix B – Monitoring Table | 22 |
| Appendix C – Equality Analysis | 23 |

1. Introduction

The Trust recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The Trust also recognises the need to share information with patients, other health organisations and other agencies in a controlled and legal manner consistent with the interests of the patient and in some circumstances, the public interest. Of equal importance is the need to ensure high standards of quality and accuracy when creating information.

Staff making decisions about sharing health and social care information cannot rely only on compassion and common sense. They must also act within the law. Every minute of every day, staff who are employed across the Trust make lawful use of personal/sensitive confidential data about patients and service users. All information processing must be fair and lawful. There are four legal bases for processing confidential information which meet the common law duty of confidence. These are with consent, through statute, a court order or to meet the public interest test. In addition to one of these legal bases processing must also meet the requirements of the Data Protection Act 1998 and the Human Rights Act 2000. Failure to comply with the law when dealing with people's personal confidential data erodes trust, which can seriously damage the view of the public about the trustworthiness of the Trust and the NHS in general. Decisions about any disclosure of personal/sensitive information must be made on a case by case basis referring to the concepts laid down in this policy.

A duty of confidence arises when a person discloses information to another in circumstances where it is reasonable to expect that the information will be held in confidence. It is therefore:

- A legal obligation that is derived from case law – the Common Law Duty of Confidence
- A requirement established within professional codes of conduct – HCPC, MNC, GMC
- A Clause within your contract of employment linked to internal procedures such as the disciplinary procedures.

2. Purpose

Disclosure and sharing of personal identifiable information is governed by the requirements of Acts of Parliament and government guidelines. 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 data security systems or controls. The purpose of this policy is to assist staff in making what are often difficult decisions on whether a breach of patient confidentiality can be justified in the public interest

This Code has been written to meet the requirements of:

- Consent including Gillick Competence and capacity
- The Data Protection Act 1998
- Common Law Duty of Confidence

- The Human Rights Act 2000
- The Computer Misuse Act 1990
- Use and Disclosure of Health Data – May 2002
- The Privacy and Electronic Communications (EC Directive) Regulations 2011
- Confidentiality – NHS Code of Practice – Nov 2003
- Confidentiality: NHS Code of Practice - Public Interest Disclosures 2010
- East of England Ambulance Trust – Information Security Policy
- Caldicott report 1997, Caldicott2 Report, Caldicott Review of data Security, Consent and Opt-Outs
- EEAST employment contract clause.

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

3. Duties

3.1 Chief Executive

As the accountable officer for the Trust, the Chief Executive is required to provide assurance that all risks to the Trust (including confidentiality risks) are effectively identified, managed and mitigated. Details of Serious Untoward Incidents involving data loss or confidentiality breaches must be reported to the Department of Health's Information Governance Toolkit and also be detailed in the Trust's annual report.

3.2 Caldicott Guardian

The Medical Director is the Caldicott Guardian and is responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing. The Caldicott Guardian is responsible for providing advice within the Trust on the lawful and ethical processing of patient information.

3.3 The Compliance and Standards Lead

The Compliance and Standards Lead is responsible for overseeing information governance systems and processes within the Trust, and ensuring the effectiveness of these systems in protecting the security and confidentiality of all personal and personal sensitive information that is controlled and processed by the Trust.

3.4 The Information Governance Manager

The Information Governance Manager will contribute to the provision of health care to the public by being the lead for the development and co-ordination of effective Information Governance (IG) within the Trust. Under the management of the Compliance and Standards Lead, the Information Governance Manager will develop information systems to support the Trust's Information Governance Assurance Framework, Strategy and Policy requirements incorporating continual assessments both qualitative and quantitative risk treatment plans to reduce risks associated with the use of patient identifiable data and personal/sensitive data.

3.5 EEAST Staff

All employees working in the Trust are bound by a legal duty of confidence to protect any 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 within the

Data Protection Act 1998 and, in addition, for health and other professionals through their own professional Codes of Conduct.

The term 'employee' is considered to include all full time staff, part time staff, bank and agency staff, temporary staff, students, voluntary workers, secondments from other organisations, and any other person working on behalf of or through the Trust.

3.6 Consultation and Communications with Stakeholders

This Confidentiality Code of Conduct is reviewed and approved by the Information Governance Group, which includes key information governance stakeholders from corporate and operational areas in the Trust. All policies approved at the Information Governance Group will be placed on the next scheduled Executive Leadership Board for full sign off.

4.0 Definitions

4.1 Confidentiality

Confidentiality is 'the entrusting of private information to a person with reliance on their fidelity or competence' in circumstances where it is reasonable to expect that the information provided will be held in confidence. The notions of trust and competence are vital. All employees are responsible for maintaining the confidentiality of information gained during their employment with the Trust. A duty of confidence is a legal obligation derived from case law, it is a requirement established within all professional codes of conduct and is incorporated in all staff contracts of employment and job descriptions which are linked to the Trust's disciplinary procedures should a breach be detected and therefore should be read in conjunction with these documents.

4.2 Confidential Information

Confidential information can be anything that relates to patients, staff (including volunteers, bank and agency staff, student placements), their family, or friends, however stored. Patients allow us to gather personal and sensitive information relating to their health and other matters as part of their seeking treatment. Patients do this in confidence and they have a legitimate expectation that staff will respect their privacy and act appropriately. In some circumstances patients may lack the competence to extend this trust, or may be unconscious, but this does not diminish the duty of confidence. It is essential, if the legal requirements are to be met and the trust of patients is to be retained, that the NHS provides, and is seen to provide, a confidential service. Patient information is generally held under legal and ethical obligations of confidentiality. Information provided in confidence should not be used or disclosed in a form that might identify a patient without his or her explicit written consent.

For example, information may be held on paper, CD, computer file or printout, video, photograph, USB stick or even heard by word of mouth. It includes information stored on portable devices such as laptops, PDAs, mobile phones and digital cameras.

Confidential information can take many forms including medical notes, audits, employee records, patient report forms, written notes, carer notes, occupational health records etc. It also includes any confidential information relating to other organisations, such as other NHS Trusts, CCG's, independent contractors (GPs, dentists, pharmacists and optometrists) and local authorities (e.g. social care, education etc.).

Person-identifiable information is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number, National Insurance number etc. Please note even a visual image (e.g. photograph) is sufficient to identify an individual.

Certain categories of information are legally defined as particularly sensitive and are carefully protected by additional requirements as stated in legislation (e.g. information regarding in-vitro fertilisation, sexually transmitted diseases, HIV and termination of pregnancy).

During your work with the Trust you should consider all information to be personal and or personal sensitive, even something as simple as a patient's name and address. The same standards should be applied to all information you come into contact with.

4.3 Caldicott principles

Whether you are requesting, using or disclosing confidential information you should at all times abide by the Caldicott principles. These are:

- Justify the purpose of using confidential information
- Only use it when absolutely necessary
- Use the minimum required
- Access should be on a strict need-to-know basis
- Everyone must understand their responsibilities
- Understand and comply with the law
- The duty to share information can be as important as the duty to protect patient confidentiality

4.4 'Safe Havens'

A Safe Haven describes a set of arrangements whereby an organisation can ensure confidential personal information can be communicated and stored safely. For further clarification please refer to the Trust's Safe Have Procedure document which can be found on the document library in the Trust intranet.

5.0 Development

5.1 Prioritisation of Work

This Code of Conduct is required for staff information and reference and to support the Trust's wider Information Governance Framework.

5.2 Identification of Stakeholders

Primary stakeholders are the SIRO, Caldicott Guardian, Compliance and Standards Lead, the Information Governance Manager, and members of the Information Governance Group.

5.3 Responsibility for Document's Development

The Policy has been developed by the Information Governance Manager, with review and approval by the Information Governance Group and ELB sign off.

6.0 Disclosure of Confidential Information

Remember your duty of care. This means that where you have control of personal and sensitive information about patients and staff, you must not allow disclose of this information to anyone for any purpose, unless the person has given consent or there is a legal reasons for doing so.

Never give out information to persons who do not “need to know” in order to provide health care and treatment, or for any other reason.

All requests for patient identifiable information should be justified. This applies whether the request comes from within the Trust or from some outside organisation. Some requests may need to be agreed by the Trust’s Caldicott Guardian.

Every NHS Trust has a Caldicott Guardian. This is usually a senior manager who is also a doctor or a nurse. In the East of England Ambulance Trust the role of Caldicott Guardian is undertaken by the Medical Director. Their role is to protect patient confidentiality as far as possible. They should be contacted if you are in doubt about disclosure or if you are aware of poor practice within the Trust which may be putting patient confidentiality at risk.

6.1 Intranet, Internet, Website, Journals etc.

Any information, data or other forms of information placed in any article that may viewed by any person either electronically or on paper must be very carefully vetted to ensure that all personal and sensitive information is anonymised and cannot cause distress to individuals or groups unless the person(s) involved have given their explicit permission for such information to be displayed. This permission should be in writing.

6.2 Disclosure of Information to Other Employees of the Trust

Information on patients or staff should only be released on a need-to-know basis.

Always check the member of staff requesting the information is who they say they are. This can be achieved by checking the employee’s ID badge and/or their internal extension number or pager number prior to giving them any information. Also check that they are entitled to receive the information.

Do not be bullied into giving out information!

If in doubt, check with your manager or the health care professional in charge of a patient’s care, or the person(s) themselves or the Information Governance Manager and or the Release of information team.

6.3 Disclosure of Information to Other Organisations

Health and/or social care organisations, Acute Trusts, CCG’s or other NHS organisations.

All NHS employees are bound by the NHS Code of Confidentiality. Information may be shared, provided the Caldicott principles are observed, you apply the checks given above, and abide by any Data Sharing agreements in place. See the Trust’s ‘Release of Information Policy’ for further guidance.

Joint Health/Social Care Teams (e.g. substance misuse or community mental health services)

All team members will be bound by similar codes of confidentiality. Information may again be shared provided you proceed as above.

Others: Police, Solicitors, Safeguarding

This is a complex area. Frequently there will be a specific Information Sharing Agreement (ISA) between these agencies and the Trust, defining what information may be shared and

with whom. The Trust is required to share safeguarding information with the right people at the right time and this will often be without the patients consent. This is to:

- Prevent death or serious harm
- Coordinate effective and efficient responses to those who are vulnerable
- Enable early interventions to prevent the escalation of risk
- Prevent abuse and harm that may increase the need for care and support
- Maintain and improve good practice in safeguarding
- Reveal patterns of abuse that were previously undetected and that could identify others at risk of abuse
- Help people to access the right kind of support to reduce risk and promote wellbeing
- Help identify people who may pose a risk to others and, where possible work to reduce offending behaviour
- Reduce organisational risk and protect reputation.

In the absence of any such agreement or if in any doubt, you should contact your manager, the Caldicott Guardian, or the Trust RFI Lead or the Information Governance Manager. Confidentiality is not absolute. Disclosures may be necessary in the public interest where a failure to disclose information may expose the patients or vulnerable patients or others to risk of death or serious harm or to detect and prevent crime.

6.4 Telephone Enquiries

If a request for information is made by telephone, always to check the identity of the caller and check whether they are entitled to the information they have requested.

Take their number, verify it independently and call back if necessary.

If you have any concerns about disclosing/sharing patient information you must discuss this with your manager and forward the request to the RFI team who will log the request and check the persons ID, gain written consent before releasing the information.

6.5 Requests for Information by the Police

Requests for information received from the Police should always be referred to the RFI team for processing.

6.6 Requests for Information by the Media

Do not give out any information under any circumstances. Always refer to the Communications team who will only be too happy to advise you. If you receive any request from the media by personal visit or by phone, refer the person to your line manager in the first instance.

6.7 Clinical Audit

Data sharing is essential for high quality ambulance health and care services. It is integral to identifying poor care; it is clear that more effective data sharing can enable some of the recent failures to provide proper care to patients to be identified and tackled earlier. Patients you treat provide you with their personal confidential information, without which the care would not be effective or safe. There can be no doubt that such information, drawn from millions of people, can be extremely useful for other purposes, such as clinical audit and research. There are laws to prevent improper disclosure and procedures to ensure that

permission for such 'secondary use' is limited, ethical and secure. However, the laws and procedures are difficult for the experts to understand, let alone the patients and service users. It is hard to argue that patients and service users have consented to uses of their personal confidential information that they cannot anticipate, according to procedures that they cannot understand. This issue is particularly troubling for individuals who have strong views about how their information may be used.

The National Data Guardian (Dame Fiona Caldicott) recommends a new consent/opt-out model to give patients a clear choice about how their personal confidential data is used for purposes beyond their direct care in the future. Until this is confirmed and implemented it is good practice to inform all patients that their anonymised information may be used for clinical audit and/or research. This is currently achieved through the publication of the Trusts patient leaflets on the internet. It may be necessary in the future to obtain written consent to use a patient's data for a secondary use. Dame Fiona Caldicott in her report published in June 2016 suggests that the Trust will need to obtain consent and to also provide the patient with an opt-out option. This means the patient can opt out of their information being used for anything other than their direct care.

Until this is fully confirmed anonymised data should always be used, if the patient has consented to a secondary use of their information whether it is for research or for clinical audit. Disclosure (sharing) of non-anonymised data can only be carried out with the patient's explicit written consent. See below for the only exception to this rule.

If the audit is going to be undertaken within the health care team, then it will be the team's duty to safeguard and anonymise the data before disclosure. You should contact your audit department for advice on the best way of doing this. Occasionally the audit will be undertaken by third parties e.g. the Trust's or another Trust's clinical audit department. It may then be necessary to disclose identifiable data prior to it being anonymised. In such cases, you should ensure that the Caldicott seven principles have been considered and implemented:

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. 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 professionals 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.

6.8 Disclosure of information for other non-medical purposes

This will include the sharing of information with members of parliament, courts and solicitors. The question whether the individual has given informed consent is vital. You should seek guidance from the Information Governance or the Trust's Caldicott Guardian.

6.9 Disclosure of information for medical purposes other than healthcare

This will include the sharing of information for the purposes of research, audit, commissioning etc. In general this information should be anonymised wherever possible. Remember that even anonymised data can lead to patients being identified e.g. if the data relates to a very small number of patients. Also just using the patient's postcode as a means of anonymising is not acceptable.

7. Safeguarding information

7.1 General

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

Do not leave any notes, patient report forms, other medical records or confidential information lying around unattended or on the dash board of a vehicle.

Make sure that any computer screens, or other displays of information, cannot be seen by the general public, members of staff or other visitors etc. Computers should be locked when unattended.

Ensure that during telephone conversations, whether on a land line or mobile device, confidential details cannot be overheard by bystanders.

7.2 Storage of Confidential Information

Paper-based confidential information should always be kept locked away and preferably in a room that is locked, and in some cases alarmed when unattended, particularly at night and during weekends or when the building/office will be un-occupied for a period of time.

Confidential information should not be left lying on desks unattended.

Extreme care should be taken before saving sensitive or personal information onto local hard drives or removable media. You should consider anonymising the data wherever possible. CDs, and other media should be kept in locked storage. You should be aware of the additional risk in storing sensitive data on a laptop. These should always be transported in a lockable container e.g. boot of car.

Personal information held on laptops, USB sticks, CD/DVD's etc. must be encrypted to a Trust-approved standard. The use of 'Freeware' or 'Shareware' that fails to comply with these standards is not permitted. Suitable USB sticks can be supplied to relevant members of staff who can make a case for needing one. Personal USB sticks must not be used and should never be inserted into any Trust equipment.

All stored personal information must be regularly checked for relevance, appropriateness and accuracy. All personal information held must be up to date. Where the information is no longer required it should be removed or suitably archived. Legal action could be taken against individuals or the corporate Trust where inaccurate information is retained, or information is retained for longer than necessary.

7.3 Confidentiality of Passwords

- Personal passwords issued to or created by employees should be regarded as confidential and those passwords must not be communicated to anyone.
- Passwords should never be written down.
- Passwords should not relate to the employee or the system being accessed.
- Smart cards must not be shared and should be looked after in the same way as personal bank cards. Detailed guidance is given in the Smartcard terms and conditions. You will be given more information about password control and format etc. When you receive your system training, password and/or smartcard.
- Passwords should be changed by the user regularly and at least every 30 days.

No employee should attempt to bypass or defeat 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 Head of ICT and may result in a disciplinary action and also to a breach of the Computer Misuse Act 1990 and/or the Data Protection Act 1998, which could lead to criminal action being taken against the offender.

8.0 Sending and receiving information

8.1 Use of Internal and External 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, a consultant or a legitimate Safe Haven, but not to a department, a unit or an 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, e.g. 'Confidential' or 'To be opened by 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 Report Forms, case-notes, or collections of patient records on paper, floppy disc or other media. These should be sent by Recorded Delivery, courier, or the local transport service, to safeguard that these are only seen by the authorised recipient(s). In some circumstances it is also advisable to obtain a receipt as proof of delivery e.g. patient records to a solicitor.

Electronic media (e.g. floppies, CD) with confidential information should be securely encrypted, password protected, and sent by a secure courier service.

Patient Report Forms and other bulky material should only be transported in approved boxes or bags and never in dustbin sacks, carrier bags or other containers. These containers should not be left unattended unless stored, waiting for collection, in a secure area e.g. ideally locked. The containers should only be taken and transported by the approved carrier.

8.2 Faxing

Faxing is not a secure method of transmitting information. It is easy to misdial. Further, you do not always know where in the building the receiving fax machine is located. If it is essential to send a fax, you should:

- Remove person identifiable data from any faxes unless you are faxing to a known secure and private area (e.g. Safe Havens). Please refer to the Trust's Safe Haven Procedure document.
- Faxes should always be addressed to named recipients.
- Always check the number to avoid misdialling and once sent, ring the recipient to check that they have received the fax.
- If your fax machine stores numbers in memory, always check that the number held is correct and current before sending sensitive information.
- Ensure the use of suitable cover sheets that contain a confidentiality statement.

8.3 E-mailing Confidential Information

Please seek advice from your manager if you have the need, or possible need, to e-mail patient or personal identifiable information (PID). This must be either encrypted or sent via a secure NHS Net account.

Firstly, consider whether you actually need to disclose the patient's identity. Most clinical audits, financial payments and some health reports do not need the patient's name for the purposes for which they are being shared.

Patient identifiers should be removed wherever possible and only the minimum necessary information sent. This may be considered to be the NHS number but not the name or address. NB Check that you have typed in the right number.

If it is considered necessary to transfer patient or personal identifiable data (PID), then this should be done by attaching the information in a separate file e.g. a password protected Word document or an Excel spreadsheet. Guidance on how to password protect files can be found on Microsoft Office Help.

Personal identifiable information can only be e-mailed using a national NHS webmail account, one that ends in 'NHS.NET', not a local domain account. This method encrypts the data and is the only acceptable means of using e-mail to transfer staff, patient or other person identifiable information. The recipient's name should be selected from the NHS mail directory ensuring that it is the correct person at the correct organisation. Special care should be taken to ensure the information is sent only to recipients who have a "need-to-know ". REMEMBER always double check that you are sending the e-mail to the correct person(s).

E-mails sent either to or from an nhs.uk address (e.g. joe.bloggs@eastamb.nhs.uk) are not encrypted in transit and therefore must not be used for sending personal identifiable information.

E-mails sent both to and from NHSmail addresses (e.g. from peter.smith@nhs.net to alan.bates@nhs.net) are encrypted in transit and therefore are considered secure. However, it is still good practice to remove patient identifiers wherever possible.

If for some reason it is not possible to use an NHS.Net email address any personal identifiable information must be encrypted to a Trust approved standard and sent as an attachment.

See the Trust's Email Use Policy for further details.

All e-mails containing personal information should contain a confidentiality statement.

9.0 Disposal of Confidential Information

Paper-based confidential information should always be disposed of using 'Confidential Waste' sacks/shredders. This includes such things as rough notes, names, addresses or telephone numbers jotted down on scraps of paper etc. Keep the waste in a secure place until it can be collected for secure disposal.

9.1 CDs

CDs and other devices (including USB memory sticks) 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.

9.2 Computer hard disks

This is a specialist area. Please refer to the Trust's Information Security Policy.

Advice relating to the destruction of ICT equipment may be obtained from the IT Helpdesk.

10. Working from home

It is sometimes necessary for employees to work from their own home. If you need to do this you would first need to gain approval from your line manager. If they agree you would need to ensure the following are considered and remember that there is personal liability under the Data Protection Act 1998 and your contract of employment for breach of these requirements:

Ensure you have authority to take the records away. This will normally be granted by your line manager.

If you are taking manual records please ensure there is a record that you have these records, where you are taking them to, the purpose for taking them and when they will be returned. This is particularly important for patient related records. A tracer card system or electronic tracking system should suffice. If there is not one, an alternative manual system should be in place.

Ensure any personal information in manual form e.g. patient/staff files, or electronic format e.g. CDs, USB sticks etc. are securely housed prior to them being taken out of the Trust's building(s).

Make sure they are put in the boot of the car out of sight (ensuring that the vehicle is locked when unoccupied) or carried on your person while being transported from your work place to your home.

While at home you have personal responsibility to ensure the records are kept secure and confidential. This means that other members of your family and/or your friends/colleagues must not be able to see the content or outside folder of the records.

You must not let anyone have any access to the records.

If you take home computer records on a floppy disc or CD you must ensure all of the above apply. In addition you must ensure if you are putting this information onto your own PC that you take the information off again when you have finished your work.

Other family members must not be able to access this information.

When returning the records to work the same procedure must be carried out, as above, in secure containers etc.

Manual records they should be logged as being back within the Trust. Computer records on CD these MUST be virus free before being loaded onto any of the Trust's systems – especially any which can be accessed via the network. It is the individual's responsibility to ensure such discs etc are virus free.

Laptops containing personal identifiable information must be secured at all times, especially in transit. Laptops containing personal information must be suitably encrypted. (See Section 4.)

Any loss of records or data bearing media, such as laptops, must be reported immediately to the line manager as soon as the loss is known. This must be supported by a full report and investigation report on the Datix incident reporting system. Where appropriate the Police should also be informed.

11. Copying software

All computer software used within the Trust is regulated by licence agreements. A breach of the agreement could lead to legal action against the organisation and/or the offender (member of staff).

It is important that software on the Trust's systems used for work purposes must not be copied and used for personal use. This would be a breach of the licence agreement.

12. Patients' Rights

Under the Data Protection Act all patients have a right of access to their records, (this also applies to staff in respect of their personnel files). Patients have a further right to restrict access to their records. For example they may wish to state that they are happy for sensitive information to be shared with one agency but not another. This needs to be documented and suitable access controls put in place. Patients need to be informed of their rights through appropriate notices and leaflets.

13. Freedom of Information (FOI)

The Freedom of Information Act 2000 makes provision for the disclosure of information held by a public authority such as the Trust or by persons providing services for the Trust. The Trust is required to publish a publication scheme which lists information about its activities. The main principle behind the freedom of information legislation is that people have the right to know about the activities of a public authority unless there is good reason for them not too. This is covered by a number of exemptions which can be applied by the law and which entitles the Trust to withhold the information being requested. FOI information does not give people access to their own information; this should be made via a subject access request. FOI information may include policies and procedures, minutes of meetings, annual reports etc. All FOI requests should be sent to the FOI officers using eoasnt.foi@nhs.net. FOI releases of information must never include patient identifiable information which is covered by the Data Protection Act. If asked to release information under Freedom of Information, please refer the request to the FOI officers. You can also refer to the Trusts FOI Policy for further information.

14. Training

The Trust is responsible for ensuring all staff have a basic level of knowledge and awareness about confidentiality and information security. The subject is covered in the Induction Course and mandatory training handbook. All professional staff have a responsibility against their code of conduct to remain competent.

15. General provisions

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 line manager, the Trust's Information Governance Manager, Trust's Information Security Officer or the Caldicott Guardian.

16. Data Protection Act

Everybody is subject to the provisions of the Data Protection Act 1998.

The Trust has made a corporate registration with the Information Commissioner. It is not therefore necessary for employees to make a separate, individual registration for any work they undertake on behalf of the NHS. However, notification of data collection should be

made to the rfi (EAST OF ENGLAND AMBULANCE SERVICE NHS TRUST) eoasnt.rfi@nhs.net team to ensure that the reason for and type of data is covered under the current registration.

17. Abuse of Privilege

It is strictly forbidden for employees to look at any information relating to their own family, friends, work colleagues or acquaintances unless they are directly involved in the patient's clinical care or with the employee's administration (e.g. payroll) on behalf of the Trust. Action of this kind will be viewed as a breach of confidentiality and may result in disciplinary action.

If you have concerns about this issue please discuss with your line manager.

18. Non-Compliance

All staff are reminded that they have signed a confidentiality agreement when joining the Trust. Temporary staff, students and secondments should be asked to sign the standard Trust Confidentiality form on their first day or as soon as possible following receipt of their domain logon details. A copy of the form can be downloaded from the Trust's intranet.

Staff must meet the standards in this code. Much of what is required builds on existing good practice. Clearly staff may sometimes be prevented from meeting these standards where appropriate systems and processes are not yet in place. In these circumstances the test must be whether you have been working within the spirit of this code and are making reasonable effort to comply.

Blatant non-compliance with this code of conduct by any person working for the Trust may result in disciplinary action being taken in accordance with the Trust's disciplinary procedure, and may lead to dismissal for gross misconduct.

To obtain a copy of the disciplinary procedures please discuss with your manager or the Human Resources department, or visit the Trust's intranet.

19. Possible breaches or risk of breach

If you think there are processes or procedures in place that put patient confidentiality at risk e.g. receiving confidential letters not marked private etc, then you should report this to your manager.

The Trust also encourages you to report if you are aware or suspect that another member of staff, whether from the Trust or another organisation, is breaching this code and abusing patient or staff confidentiality.

If you do not feel able to approach your manager, then you should discuss this with the Caldicott Guardian or consider using the Trust's whistle-blowing procedures.

20. Amendments

This code will be amended as necessary to reflect the Trusts development of policies and procedures and the changing needs of the NHS. Staff will be informed of any changes through the Trust's intranet and where necessary by individual or group emails.

21. Equality Analysis

An Equality Analysis has been undertaken. See Appendix C.

22. Process for Monitoring Compliance and Effectiveness

See Appendix A – Monitoring Table.

The security and integrity of information confidentiality processes within the Trust will be monitored by the Information Governance Group who will escalate any areas of concern to the Performance and Finance Committee.

23. Standards/Key Performance Indicators

Standards for this code have been drawn from the NHS Confidentiality Code of Practice, GMC Guidance, and the requirements of the Information Governance Toolkit.

The primary performance indicator for compliance with this Code is staff awareness of and compliance with confidentiality requirements, as measured by Datix incident reports.

24. References

NHS Confidentiality Code of Practice - 3rd edition. November 2003

GMC Guidance 'Confidentiality: Protecting and Providing Information'. April 2004

National Data Guardian for health and care – Review of Data Security, Consent and Opt-Outs Dame Fiona Caldicott June 2016

25. Associated Documents

This code of conduct relates closely to the following documents and Trusts policies for:

Safe Haven Procedure

Release of Information Procedure

NHS Code of Confidentiality Nov. 2003

Data Protection Act 1998

Information Security Policy

Professional Codes of Practice

Common Law Duty of Confidence

Employment Contract – Confidentiality Clause

Caldicott2

National Data Guardian for health and care – Review of Data Security, Consent and Opt-Outs.

Appendix A – Summary Confidentiality Code of Conduct for Employees

1. Introduction

- 1.1 All employees (including contractors and volunteers) working in the NHS are bound by a legal duty of confidentiality to protect personal and commercially sensitive information they may come into contact with during the course of their work.
- 1.2 A duty of confidentiality is written into Trust employment contracts and is a legal requirement under various UK laws. It is also included in the codes of practice of many professional bodies.
- 1.3 The duty of confidentiality means that everyone is obliged to keep any personal identifiable information (such as patient and employee records) strictly confidential.
- 1.4 For the purposes of this Code, sensitive non-personal identifiable information should be treated with the same degree of care. For example, **commercially sensitive information or operationally critical information should be protected.**
- 1.5 The principle behind the Code of Conduct is that no employee shall breach their legal duty of confidentiality or allow others to do so, or attempt to override any of the Trust's security systems or controls, which may result in a breach of confidentiality.
- 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. Confidentiality of Information

- 2.1 All employees are responsible for maintaining the confidentiality of information they come into contact with during their employment with the Trust.
- 2.2 Employees can be held personally liable for unauthorised data loss under the terms of the Data Protection Act 1998 and the Criminal Justice and Immigration Act 2008. The Information Commissioner has the power to impose considerable fines on both the Trust and the individual if personal data is improperly disclosed.

3. What is a Duty of Confidence?

- 3.1 A **duty of confidence** arises when one person discloses information to another in circumstances where it is reasonable to expect that the information will be held in confidence. For example, a communication between a patient and a paramedic, between a manager and an employee and commercially sensitive information discussed in contract negotiations and tender documents constitute a duty of confidence.
- 3.2 Respecting the duty of confidence is a legal obligation that is derived from case law, and a requirement established within professional codes of conduct. It is also included within the Trust employment contract as a specific requirement.

- 3.3 A breach of the duty of confidence is likely to constitute gross misconduct and will result in disciplinary action against the staff members concerned.

4. Abuse of Privilege

- 4.1 It is strictly forbidden for employees to look at any information relating to their own family, friends or acquaintances unless they have a legitimate reason for doing so (e.g. they are directly involved in their care as a patient). Any action of this kind will be viewed as a breach of confidentiality, and may result in disciplinary action.
- 4.2 Anyone who has concerns about this issue should discuss them with their line manager.

5. Non-Compliance

- 5.1 Non-compliance with the terms of this Code of Conduct by any person 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.

Appendix B – Monitoring Table

| What | Who | How | Frequency | Evidence | Reporting arrangements | Acting on recommendations | Change in practice and lessons to be shared |
|------------------------------------|---|-----------------------------|--------------------------|--|---|--|---|
| Datix incident data | IG Team | Reports to IGG | Bi-monthly updates | Formal written reports on information/ confidentiality related incidents | <p>Review by Information Governance Group</p> <p>Incident reports will be discussed and required actions and timescales agreed</p> <p>Decisions of the group will be formally recorded in minutes</p> | Compliance and Standards Lead with support from Caldicott Guardian and IGG members | Review of staff awareness of confidentiality requirements with changes to staff training and awareness initiatives, as necessary |
| Confidentiality awareness training | <p>Information Governance Team</p> <p>Learning and Development Unit</p> | Training completion reports | Monthly reports from LDU | Formal written reports | <p>Review by Information Governance Group</p> <p>Ongoing monitoring by the Learning and Development Manager</p> <p>Formal training reports will be discussed at IGG and required actions and timescales agreed</p> <p>Decisions of the group will be formally recorded in minutes</p> | <p>Compliance and Standards Lead</p> <p>Learning and Development Manager</p> | <p>Action taken to ensure that all staff have completed either introductory information governance induction training or annual IG refresher training.</p> <p>All IG training includes instruction on confidentiality best practice and staff obligations</p> |

Appendix C – Equality Analysis

Title: Confidentiality Code of Conduct

What are the intended outcomes of this work? *Include outline of objectives and function aims*

The purpose of this policy is to assist staff in making what are often difficult decisions on whether a breach of patient confidentiality can be justified in the public interest

Who will be affected? *e.g. staff, patients, service users, general population etc*

All staff, third party contractors, patients, service users and general population

Evidence *The Government's commitment to transparency requires public bodies to be open about the information on which they base their decisions and the results.*¹

What evidence have you considered? *List the main sources of data, research and other sources of evidence (including full references) reviewed to determine impact on each equality group (protected characteristic). This can include national research, surveys, reports, research interviews, focus groups, pilot activity evaluations etc. If there are gaps in evidence, state what you will do to close them in the Action Plan on the last page of this template.*

Disability

The policy can be made available in different formats if required.

Gender

No evidence found to highlight any differences/ allowances required

Race

The policy can be made available in different formats if required.

Age

The policy can be made available in different formats if required.

Gender reassignment (including transgender)

No evidence found to highlight any differences/ allowances required

¹ [EEAS Being Open Policy](#)

Sexual orientation

No evidence found to highlight any differences/ allowances required

Religion or belief

No evidence found to highlight any differences/ allowances required

Pregnancy and maternity

No evidence found to highlight any differences/ allowances required

Carers

No evidence found to highlight any differences/ allowances required

Other identified groups

No evidence found to highlight any differences/ allowances required

Engagement and involvement

Was this work subject to the requirements for public engagement/consultation?

How have you engaged stakeholders in gathering evidence or testing the evidence available?

How have you engaged stakeholders in testing the policy/strategy or programme proposals?

For each engagement activity, please state who was involved, how and when they were engaged, and the key outputs:

Summary of Analysis

No evidence to suggest that there is any potential differential impact for any of the protected characteristics.

Eliminate discrimination, harassment and victimisation

No evidence to suggest that there is any potential differential impact for any of the protected characteristics.

Advance equality of opportunity

No evidence to suggest that there is any potential differential impact for any of the protected characteristics.

Promote good relations between groups

No evidence to suggest that there is any potential differential impact for any of the protected characteristics.

What is the overall impact?

No evidence to suggest that there is any potential differential impact for any of the protected characteristics.

Addressing the impact on equalities

No actions required

Action planning for improvement *Please give an outline of the key actions based on any gaps, challenges and opportunities you have identified. Actions to improve the policy/programmes need to be summarised (An action plan template is appended for specific action planning). Include here any general action to address specific equality issues and data gaps that need to be addressed through consultation or further research.*

Please give an outline of your next steps based on the challenges and opportunities you have identified. *Include here any or all of the following, based on your assessment*

- *Plans already under way or in development to address the **challenges** and **priorities** identified.*
- *Arrangements for continued engagement of stakeholders.*
- *Arrangements for continued monitoring and evaluating the policy for its impact on different groups as the policy is implemented (or pilot activity progresses)*
- *Arrangements for embedding findings of the assessment within the wider system*
- *Arrangements for publishing the assessment and ensuring relevant colleagues are informed of the results*
- *Arrangements for making information accessible to staff, patients, service users and the public*
- *Arrangements to make sure the assessment contributes to reviews of EEAS strategic equality objectives.*

For the record

Name of person who carried out this assessment:

Gail Butler (Corporate Records Manager)

Date assessment completed:

21st October 2016

Name of responsible Director:

Sandy Brown (Director of Nursing and Clinical Quality)

Date assessment was signed: 8th December 2016

A handwritten signature in black ink, appearing to read 'A. Brown', is written in the bottom section of the form.