East London NHS
NHS Foundation Trust

Confidentiality – What This Means in Practice

Guidance for staff

Document Ref IGL001

October 2015

Introduction

All employees of the Trust should be aware of their statutory, legal and professional responsibilities, Trust policies and best practice in respect of person identifiable information. This is called the Confidentiality Code of Conduct.

All employees are required to maintain the confidentiality of service user and other person identifiable information. Individuals must also ensure that anyone working for or on behalf of the Trust (all personnel, contracted employees, volunteers and agency staff) upholds their responsibilities in respect of confidentiality.

In this leaflet, any reference to personal, person identifiable or service user information applies generically to any individual, including service users, their carers or relatives, employees, prospective employees or contractors. This includes information that is recorded manually or held on computer and includes non-health information such as identification details, as well as clinical information, details of contacts and hospital/clinic/day centre attendances. The Trust has an Information Governance and IM&T Security Policy which sets out the standards required for maintaining proper confidentiality, integrity and access to the information we hold. This leaflet outlines these standards.

Accountability

An individual's rights to confidentiality are set out in Article 8 of the Human Rights Convention, the Caldicott Principles, the Data Protection Act and under common law.

All NHS Trusts are required to appoint a 'Caldicott Guardian' who is responsible for ensuring the protection of service users' confidentiality throughout the Trust in accordance with their legal rights. The Caldicott Guardian in this Trust is the Medical Director.

The Trust Board is ultimately responsible for ensuring that an individual's rights to confidentiality are met. It has established an Information Governance Steering Group to oversee this. The Caldicott Guardian chairs this group.

All individuals have a personal responsibility to respect the Data Protection Act and to maintain constant awareness of procedures regarding confidentiality. Failure to do so could result in disciplinary proceedings that ultimately might result in dismissal. Individuals also have an obligation to ensure that colleagues observe the Trust's policies, procedures and good practice advice.

Information governance policies and standards

Confidentiality is part of the information governance framework. The framework includes confidentiality, data protection, data quality and information security. The Trust takes its information governance responsibilities very seriously, and has a number of key information governance policies, procedures and best practice guidance leaflets to ensure information is handled appropriately, legally and to high standards.

Policies can be viewed on the intranet at:

http://elcmhtintranet/polices_procedures.html

Some policies are located with the Clinical policies whilst others are Information Management and Technology policies:

Clinical policies

Clinical Coding Policy

Health Record Keeping Policy

Information management and technology policies

Access to Health Records Policy

Clinical Records Management Procedures

De-duplication Procedure – Patient Records

Disposal of IM&T Equipment Policy

Freedom of Information Policy

IM&T Services Purchasing and Procurement Policy and Procedure

Information Governance and IM&T Security Policy

Network, Internet and Email Usage Policy

Mobile Phone Policy

Records Management Policy

North East London Information Sharing Protocol

P drive
There is also useful information on the Information Governance folder in the Induction folders on the P drive – (P:\Induction\Information Governance) including:

- Electronic copies of the slides used for Information Governance and Records Management induction and training sessions
- Useful reference material
- Information Governance standards
- Freedom of Information Act documents and the Trust's Publication Scheme

If you have difficulty finding this information, or require advice on any aspect of information governance please contact the Head of Information Governance on **020 7655 4131**

Training
Mandatory two hour training sessions on information governance and records management are provided to all new employed staff through the induction programme. These sessions are interactive, topical and include practical advice on personal responsibilities in respect of information governance and records management, the standards expected by the Trust, and a guide to the relevant policies and procedures.

All interim, Contract, Bank and agency staff must undertake this part of the induction programme

Regular information governance and records management training sessions are held for anyone who missed their induction session, would like to brush up on their knowledge or need advice. Please check the intranet for dates or contact the Learning & Development Facilitator on 020 7655 **4026** for details and to book a place.
Email: training.development@elft.nhs.uk

Guidance on best practice
Here are some simple rules that should be followed to ensure the Trust meets its obligations in respect of confidentiality and the safe handling of information.

The following list is not exhaustive and is a guide to best practice:

Safe handling and sharing of information.

Person identifiable information should not be communicated to anyone who is not authorised to receive it.
This refers to any information about an individual and includes information about service users, carers, staff, colleagues and prospective employees. This means person identifiable information should not be communicated to anyone who is not directly involved in the care of a service user, or is not responsible for a member of staff. It also includes organisations and agencies that do not have authorised access or a legitimate reason for the information to be shared.

- All person identifiable documents sent by post (internal and external) or carried by a staff member must be placed in sealed, fully addressed envelopes
- Correspondence with service users (including notification of appointments) must be marked 'Private and Confidential, Addressee Only'
- Faxes containing person identifiable information must not be left unattended and must be transmitted either to Safe haven numbers (i.e. 'secure' fax machines not publicly accessible) or to receiving machines where the recipient is known to be waiting. Confirmation of receipt must be requested
- Person identifiable discussions must not be held in public areas. In the rare circumstances where this cannot be avoided, then initials or similarly ambiguous references must be used when referring to a person
- Person identifiable information should not be disclosed over the phone without first checking the identity of the caller. If in doubt, phone back (to a switchboard number) or offer to write to the caller instead. Check with your line manager if in doubt
- Person identifiable information should not be disclosed over the phone in areas where the conversation can be heard by 'unauthorised' listeners
- Individuals must log out of systems or ensure the PC is locked (by using 'Ctrl / Alt / Del') before leaving a PC or terminal unattended
- PC screens must not be positioned to allow opportunist viewing
- Person identifiable information must not be sent by email unless the route is secure and the email and any attachment is encrypted

Access to electronic person identifiable information held by the Trust must be appropriately restricted.

This is equally applicable to information regarding service users, their relatives and carers, staff and prospective employees.

- Secure drives or systems must be used to store person identifiable information
- Passwords should be used to protect person identifiable information
- Network and system security passwords must never be disclosed or shared
- Individuals should never use someone else's password or smartcard to gain access to information
- Individuals must not attempt to gain access to any part of the system that their access privileges do not allow
- Information must not be extracted or downloaded from one electronic system to another without the explicit permission of the relevant System Owners
- Databases, spreadsheets or any other form of electronic record containing person identifiable, confidential or sensitive information require the approval of the Trust's Head of Information Governance.

The security of person identifiable paper records must be maintained.

- Person identifiable information must not be left unattended and must be securely stored when not in use in lockable filing cabinets or file rooms. Inactive files must be stored in locked areas
- Where used, tracer cards must be fully completed every time a file is removed to a different location, and signed back upon return
- Person identifiable information must be removed from unlocked desks overnight and stored in a secure (locked) drawer or area
- Original person identifiable records must not be forwarded to another hospital or Trust site. Copies should be placed in a sealed, fully addressed package and sent via Trust internal transport, registered post (special delivery) or approved courier
- Person identifiable information must not in any circumstances be sent unaccompanied in taxis
- Person identifiable information should be immediately removed from the photocopier. Only as many copies as necessary should be made
- Person identifiable papers for disposal should be shredded or separated from the general or recyclable waste in accordance with the local confidential waste policy

Service users should be informed how their information is used and shared.

- Only the minimum amount of data necessary should be processed (collected, held and used)
- All data should be accurate and up to date. Changes should be recorded in the notes
- Service users should be made aware of how information about them is used by the Trust by providing them with a copy of IGL007 Your records and You with Permission to Use & Share form.

Consent

Consent to use and share information must be clearly explained and proactively sought from service users. Before information can be shared (except in some exceptional circumstances) the service user must consent by signing the Trust's permission to share form which is part IGL007 Your records and permission to share form

- Consent to share is only valid if the service user has been made fully aware of what it means and how the data will be used
- Consent should be gained in writing and the consent form placed in the service user's notes
- Occasionally, consent may be given verbally. Verbal consent should be clearly recorded on the consent form. This must include the date of consent. However, every attempt should be made to seek written consent

- The right to withhold or withdraw consent must be fully explained, including the process for doing so

Carers and family

Carers or family members may ask for access to their charge's / relative's notes. In some circumstances (but not all), access may be granted.

- If the service user consents then the notes may be provided
- At times, service users may not wish for their carers and / or family to be involved in their treatment. This should be discussed with the service user, and the rights of both parties carefully balanced by the clinical team
- Carers or family may also wish to seek information or advice about their relative's illness and meetings. Provided the service user has given consent, meetings with the appropriate clinical teams may be arranged
- Carers can also ask for information on voluntary groups who can support them and offer advice on the illness and its treatment options.

Access to health records
Service users are entitled to view and receive copies of their clinical records. All such requests should be directed to the manager of the service where the service user has received care, and handled in accordance with the Trust's Access to Health Records Policy.

Information sharing

- All requests for sharing of information and disclosures of information must be recorded in the service user's notes
- Where the request is refused, the reason for refusal should also be recorded in the notes
- Where information is shared without the consent of the service user (for example in situations of emergency or high risk, or when there is a legal obligation to do so), the reason for disclosure must also be recorded

The Trust is committed to appropriately and sharing information with key health and social care agencies and is a signatory to a pan London Information Sharing Protocol. This also sets out the principles of good information sharing practice.

Confidentiality and research
Maintaining confidentiality also extends to service users or volunteers enrolled on a research programme. All research must be approved by both the Research Office and the Information Governance Manager. Project and Data Registration forms are available from the Research Office or by telephoning 020 7540 2322

Where access to medical records is required, the researcher must provide:

- Reasons for requesting access and the steps taken to maintain confidentiality
- Names and status of those access notes. Each must sign a declaration of confidentiality
- The specific period during which access will be required
- Confirmation that information will be anonymised
- Individual proof of consent where the researcher requires direct access to service users

Reporting security incidents
Any information security or confidentiality breach must be immediately reported on the Trust's Datix incident management system.

Confidentiality breaches include:

- Lost, mislaid or stolen paper record
- Lost, mislaid or stolen computers, phones, Blackberries, USB sticks etc
- Correspondence sent to the wrong service users, agencies etc or with transposed attachments for other service users
- Sharing of passwords

All confidentiality breaches are followed up by the Head of Information Governance. This may require a full data loss audit.

Advice
If there is any doubt about whether you should share information, speak to your Line Manager or Departmental Head who will be able to advise you.

Advice is also available from:
Records & Disclosure Manager **- 0207 655 4018** or recordsanddisclosure@elft.nhs.uk
Information Governance Manager - **0207 655 4131**or information.governance@elft.nhs.uk
Data Protection Officer (Associate Director of Assurance) – **0207 655 4110**
Caldicott Guardian (Medical Director) - EA **0207 655 4232**