Liverpool University Hospitals
NHS Foundation Trust

Confidentiality Code of Conduct

Protecting and using patient, staff and Trust corporate information

An information leaflet for staff

Introduction - Duty of Confidentiality

The Trust and its staff must take all reasonable care to protect the electronic and physical security of personal confidential data from accidental loss, damage or destruction and from unauthorised or accidental disclosure.

All NHS staff are bound by the terms and conditions of the Confidentiality NHS Code of Practice (2003), which gives clear guidance on the security and disclosure of patient information.

All NHS staff have a duty of confidence under common law when obtaining, accessing, using, storing or disposing (processing) of personal and confidential information.

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.

All staff should be aware that it is a condition of their contract with the Trust that under no circumstances should information of a confidential nature be discussed with, or passed on to any unauthorised person at any time, either during the course of their work or outside the working environment, whilst contracted by the Trust or after the contract has terminated.

Staff are authorised to access personal/confidential data on a need to know basis in order for them to perform their duties. Accessing data that is not needed to carry out your duties or providing data to someone who is not authorised to receive it is a breach of confidentiality which could result in disciplinary action.

Statute law imposes legal obligations regarding the confidentiality of patient and staff data, whether it is held manually or electronically.

The Trust is committed to enabling those working with information to have an effective understanding of their obligations regarding confidentiality and information security. This document describes those responsibilities and provides guidelines in order to ensure that confidentiality and information security is maintained.

Data Protection Legislation

The Data Protection Act 2018 (DPA 2018) and the UK General Data Protection Regulations (UK-GDPR) legislate how personal information is used.

The Principles:

Information should be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Accurate and where necessary, kept up to date
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
- Processed in a manner that ensures appropriate security if the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction of damage, using appropriate technical or organisational measures

The Trust's Data Protection Officer (DPO) is the Associate Director of Corporate Affairs/Company Secretary.

Common Law Duty of Confidence

Information given or received in confidence, obtained for one purpose, must not be disclosed or used for another purpose without the consent of the provider of the information.

Article 8 - Human Rights Act 1998

Everyone has the right to respect for private and family life, your home and correspondence. It is unlawful for a public authority to act in a way that is incompatible with a Convention right.

The Care Record Guarantee

The Care Record Guarantee sets out the rules that govern how patient information is used in the NHS and the control the patient can have over this. It looks at an individual's rights of access to their own information, how information will be shared and how decisions on sharing information will be made.

The Caldicott Principles

The Information Governance Review (March 2013) built on the previous Caldicott Report to look at the balance between safeguarding patients' sensitive information and encouraging responsible information sharing.

Good information sharing is essential for providing safe and effective care. There are also important uses of information for purposes other than individual care, which contribute to the overall delivery of health and social care or serve wider public interests.

The Principles:

- Justify the purpose(s) for using confidential information
- Only use confidential information only when it is necessary
- Only use the minimum that is required
- Access to confidential information should be on a strict need-to-know basis
- Comply with the law
- The duty to share information for individual care is as important as the duty to protect patient confidentiality
- Inform patients and service users about how their confidential information is used

The Trust's Caldicott Guardian is the Medical Director who has delegated executive responsibility for ensuring patient confidentiality is maintained at all times.

This Trust is committed to delivering patient, staff and corporate confidentiality as is required by law, ethics and policy. Protecting data about patients and staff requires us to think carefully about which items are identifiable, whether using these items is absolutely necessary and if so whether it is secure.

What is Personal Identifiable Data (PID)?

Personal identifiable Data (PID) is information relating to a natural living person who:

- can be identified or who are identifiable, directly from the information in question; or
- can be indirectly identified from that information in combination with other information.

Personal data includes:

- Person's name, address, post code, date of birth, contact details, next of kin, gender, occupation, NHS number, National Insurance number and local identifiable codes (hospital number)
- Pictures, photographs, videos, audio-recordings or other images of individuals, email and IP addresses.

Special Category Data includes:

- Racial or ethnic origin, ethnicity, religious or philosophical beliefs, sexual orientation, trade union membership, political opinions, genetic or biometric data concerning health.

Staff Responsibility

You are responsible for your decision to provide information. If you are unsure about whether to disclose personal data, consult your Line Manager and/or if necessary, obtain advice from the Trust's Data Protection Officer.

Please ensure

- You are aware of the requirements for confidentiality and that you comply with this on a daily basis
- When personal, confidential information (including photos, videos and audio recordings) is in your possession, it is kept safe and secure at all times
- You report any suspected breaches of confidentiality including any improper or misleading use of data; whether accidental or deliberate immediately to the Data Protection Officer, your line manager and on Datix
- All work related passwords should adhere to our password best practice and are kept confidential, safe and secure at all times and not used externally in your personal life
- You never knowingly misuse information or allow others to do so. Breach of confidentiality is a serious issue and failure to the guidance within Data Protection and Cyber Security Policies may result in disciplinary action
- You complete mandatory Data Security Awareness Training on an annual basis. You have an obligation as part of the core skills training programme
- You never access your own record. It is your right to access your own records (paper or electronic), however this must be formally requested access via the Subject Access Request department
- You never access a friend's/acquaintance/relatives record. You must have a legitimate clinical or other professional reason to access any record. Just because someone gives you their consent to access their record does not mean you can legitimately access it, unless access is required and necessary for the performance of your duties
- You understand regular audits are carried out to monitor employees' access to records and you may be asked to justify your actions

How you can help with security and confidentiality of data

- Never use someone else's password or smartcard to gain access to information held on any Trust electronic devices
- Always lock the screen when leaving a device unattended
- Patient data must be kept secure and never left unattended and available for an unauthorised person to view
- Envelopes containing confidential data must be securely sealed, labelled 'Confidential' and clearly addressed to the correct contact
- Be aware of the environment. Ensure you are in an appropriate venue when discussing confidential data i.e. not the cafeteria, the lift, or public transport
- Faxing is not secure. Personal confidential data should only be faxed where there is no alternative and immediate receipt is necessary for clinical purposes. 'Safe Haven' procedures should be followed
- Do not hold paper or electronic records for longer than necessary. Always lock the office when left unattended
- Never divulge personal, confidential or corporate data to anyone without having a legitimate reason to do so and only when you are sure of who they are, and what they intend to use the data for
- Do not remove paper records out of the Trust. They contain identifiable personal confidential data. This includes ward hand over notes
- Sending letters to patients. Ensure care is taken when addressing and inserting correspondence into envelopes

Electronic Transfer of Data

- Personal identifiable data (PID) must be removed, or minimised, in emails and where possible, substitute data with an pseudonymised unique identifier such as the NHS/Hospital number
- Do not transfer electronic files that include PID without sufficient security (encryption) and only transfer what is needed. *Guidance on how to encrypt emails can be found on the Trust Intranet or from the Cyber Security Team*
- All emails to and from NHS.net to Trust email addresses are automatically encrypted, as those, to NHS Digital. *The list continues too expand and can be confirmed by the Cyber Security Team. If you are unsure, encryption can be manually carried out and guidance is available on the Intranet or via Cyber Security, or IG*
- **Subject line** - Please ensure you do not include any PID in the 'subject' field as this is not secure
- **Distribution/Group contact lists** - Please ensure your lists do not include personal email addresses (such as hotmail.co.uk)
- **Reply to all** - Please ensure when sending 'reply all' email that only those email addresses that should receive the communication do so, and that they receive only what is needed
- Any PID being transferred using mobile data storage as disks, CDs, or USB pens must be encrypted, and a strong password used that is not attached to the medium
- It is your responsibility to ensure the safekeeping of any USB storage device. *Guidance on how to encrypt USB devices can be requested from the Cyber Security Team.*

Working from home

If you have an agreement to work from home, you must ensure the following are considered and remember that there is personal liability under the Data Protection Act 2018, UK-GDPR, and your contract of employment for breach of these requirements:

- All staff must ensure that they have authority from their Head of Service, Service Manager to take records home and to ensure they only take the minimum that is necessary
- Any Personal Identifiable Data (PID) must be transported in a suitably robust, lockable bag/case (not plastic wallets, or loose in diaries). PID in any electronic format must not be taken off site unless it has been encrypted to the correct standard
- Records, equipment or information must be kept secure and not visible during transport or carried on you personally whilst travelling
- Under no circumstances should any Trust documents, diaries or personal data or IT equipment be left unattended in a vehicle for other than a short time and never left overnight.
- While at home you have a personal responsibility to ensure the records and IT equipment are kept secure and confidential. This means that other members of your family and/or your friends/ colleagues must not have access to the content. You must not let anyone have access to the records, unless authorised.
- You must report any loss or theft of IT equipment (laptops etc.) immediately via IT **Service Desk** on (Royal - 0151 706 5499 or Aintree - 0151 529 3423) and on **Datix** quoting the IT reference.
- PID should ideally not be downloaded and stored on personal devices but if unavoidable the device should be securely configured and protected, and the data promptly deleted.
- When undertaking meetings or phone calls be conscious of the ability of other people to eavesdrop potentially sensitive discussions
- If authorised to use personal devices for remote working purposes ensure robust anti-virus, don't store any data on the personal device and ensure any suspicious activity on the device is reported
- If you are working off site, please be mindful of your surroundings, such as cameras, other people and the risks associated with the use of public wi-fi.

Informing people

The Trust has a legal duty in accordance with DPA 2018 and UK-GDPR to keep all personal information secure and respect confidentiality when personal information is held in confidence.

Patients and service users (data subjects) have the right to know what information we hold about them, what it is used for and who it will be shared with. Patients and service users will not expect health care professionals to look at their health record unless you are involved in their care.

Whenever possible, you should inform patients and service users that you are accessing and using their information and the reason for doing so.

There are specific techniques that you should use.

Explain	Clearly explain to people how you will use their information and point them to additional information if they ask for it. For example, on the Trust's website, in a leaflet or on a poster.
Give a choice	Give people a choice about how their information is used and tell them whether that choice will affect the services offered to them. For example, it may not be possible to provide some services without being able to access their information.
Meet expectations	Only use personal information in ways that people would reasonably expect

Privacy notices

A range of **Privacy Notices** have been produced to inform the following categories of data subjects:

- Patients
- Employees
- FT Membership
- Children (under 13)
- Easy Read

Whilst the privacy notices will no longer be reproduced in paper format or sent out with appointment letters, they are available to view and print via the Trust website and intranet pages.

All staffing providing care and managing patients from clinical, clerical and managerial roles should familiarise themselves with how to locate and print out the **privacy notices** in order to assist with requests for printed versions made by patients and service users.

You can find out more about Information Rights from the Data Protection Office via:

The Trust website - **Information Rights**
Email: **DPO@liverpoolft.nhs.uk**
Telephone: 0151 529 8878/6562 and a member of the team will be able to assist

Patients have the right to access their own data held within their health record, but they should apply for this is writing via the Subject Access Department

Email: **SAR@liverpoolft.nhs.uk**
Telephone Aintree: 0151 529 2023
Telephone Royal: 0151 706 2681

Trust policies

To access Trust policies on Data Protection and Cyber Security please refer to **Document Management System** (DMS).

April 2022
Data Protection Office
T: 0151 529 8878