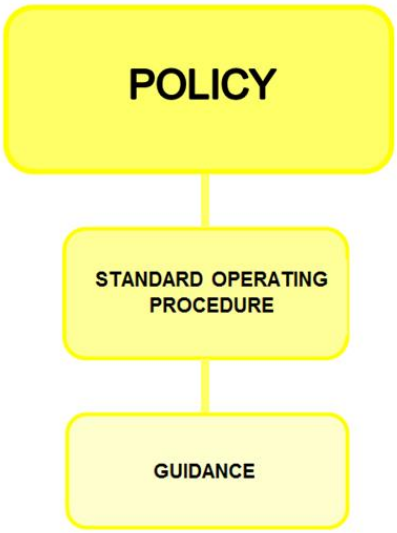
Health Records Security & Confidentiality Policy

UNIQUE POLICY REFERENCE	IM&T004
APPROVAL DATE	October 2017
REVIEW DATE	October 2019
POLICY AUTHOR	Health Records Lead
ACCOUNTABLE DIRECTOR	Senior Information Risk Owner (SIRO) / Chief Finance Officer
APPROVED BY	Chief Finance Officer & Senior Information Risk Owner

TRUST GOVERNANCE STRUCTURE
POLICY LINKED TO *Corporate Governance & Compliance Sub Committee*



POLICY VERSION CONTROL

This record shall detail all previous versions of the Policy, including versions that have been known by other names and the date of when a new version was created.

Previous Versions (Title)	Date Reviewed	Why was a new version created?
Health Records Service Security & Confidentiality Policy IM&T 004	*July 2016*	*Review date reached. Changes made to comply with new corporate policy standards.*

1. TRUST POLICY STATEMENT

This Policy identifies the Key Principles that must be applied by everyone who has access to or uses Service Users Information whilst carrying out their duties.

A Health Record is a critical information asset used every day by Health Professionals and support staff. The security and confidentiality of this information asset is vital in enabling us to deliver high quality services.

Service Users, their carers and families expect that information given to us during the course of receiving treatment or advice will remain confidential and will only be used and shared appropriately.

Health Record

A Health Record contains both personal identifiable data (PID) and sensitive data and therefore the information contained within a Health Record, either paper or electronic format is confidential and is subject to legislation under the Data Protection Act 1998 (DPA) soon to be superseded by the General Data Protection Regulation (GDPR) 2018 . The Trust will comply with the Principles of the Data Protection Act 1998 and General Data Protection Regulations (GDPR) 2018 in managing its Health Records.

Data Protection Act 1998 and General Data Protection Regulation 2018

The DPA and GDPR provides a framework that governs the processing of information that identifies living individuals – personal data in Data Protection terms. Processing includes holding, obtaining, recording, using and disclosing information and the Act applies to all forms of media, including paper and images.

Information Commissioners Office

The Information Commissioners Office (ICO) is the UK's independent regulatory authority that upholds information rights in the public interest. They ensure that organisations are compliant with relevant legislation such as the DPA 1998, GDPR 2018 Freedom of Information Act 2000 and the Environmental Information Regulations 2004.

Codes of Practice and Professional Codes

The NHS Code of Practice: Confidentiality also describes the required practice for all staff who work within or under contract to NHS organisations concerning confidentiality.

All Health Professionals and Allied Health Professionals also have a duty to comply with confidentiality guidelines described in their own Professional/Ethical Codes of Practice.

2. APPLICATION

This Policy relates to the confidentiality and security of health records.

It applies to all sensitive data and PID relating to Service Users, held in any format and includes:

- Paper held Health Records,
- Electronic patient records (EPR) e.g. eCR, RiO, EMIS, SystmOne NCRS and Windip,
- Bed boards
- Emails
- Verbal communication e.g. Face to face conversations, telephone conversations
- Administrative documents e.g. Bed state lists, Allocation lists
- Letters & other correspondence
- Text messages and social media such as Whatsapp

(This list is not exhaustive and only provides examples of where PID and sensitive data may be gathered from)

This Policy and associated documents applies to:

- all employees of LCFT,
- all agency and contracted staff
- All staff of partner organisations
- All volunteers

that process or have access to PID or Sensitive Data regarding Service Users whilst carrying out their required duties.

3. IMPLEMENTATION

Chief Executive Officer (CEO)
The CEO has overall Trust accountability for this Policy and provides assurance to the Trust Board of statutory and regulatory compliance.

Caldicott Guardian (CG)
The CG is the senior person responsible for protecting the confidentiality and security of service users information and ensuring that information sharing is safe, secure and appropriate. Serious breaches will be reported to the CG and recorded on the CG log.

Senior Information Risk Owner (SIRO)
The SIRO is accountable for Information Risk Strategy and seeks assurance in respect of compliance with this Policy and procedure.

Information Governance, Assurance and Compliance Lead
The IG Lead is responsible for ensuring that the organisation meets its statutory and corporate responsibilities and engenders public confidence in the handling of personal and corporate information.

Health Records Lead
The Health Records Lead is responsible for writing and promoting the use of this Policy and associated documents across all areas of the Trust. They will offer guidance and support to Information Asset Owners and Managers on implementation and compliance.

Information Asset Owners (IAO) and Information Asset Administrators (IAA)
IAO and IAA's will also support the SIRO in the overall Information risk management function and ensure the use and protection of the Corporate asset. This will be achieved by maintaining an Information Asset register which is reviewed as a minimum annually. Data Flow Mapping must also be undertaken

Staff must refer to the Standard Operating Procedure for Health Records Security & Confidentiality for support on how to comply with this policy.

Other policies and documents to be read in conjunction with this Policy are:

- Information Governance Policy
- Health Records Management Policy
- Access to Health Records Policy
- IM&T Security Policy
- NHS Code of Practice: Confidentiality
- Sharing information with External agencies policy

Line Managers
Line Managers are expected to monitor compliance with this policy through staff Supervision and one to one and Team meetings. They will also ensure that the principles of this policy and associated documents are embedded into local processes.

All other staff
All staff who handle or use service users Health Records or Personal Identifiable Data must familiarise themselves with the content of this policy and associated procedures. Staff should seek advice from Line Managers in relation to compliance or understanding of this Policy.

4. COMPLIANCE

The duty of confidentiality arises out of the Common Law Duty of Confidentiality, professional obligations, and also staff employment contracts (including those for contractors). Breach of confidence, inappropriate use of health records or abuse of computer systems may lead to disciplinary measures, bring into question professional

registration and possibly result in legal proceedings. Staff should ensure that they are aware of the requirements and standards of behaviour that apply.

Voluntary staff who are not employees, and students are also under obligations of confidentiality, and must sign an agreement indicating their understanding when helping within the NHS.

Annual audits will be facilitated by the Health Records Team and IG Team in conjunction with IAO's/IAA's to monitor compliance with the Policy.
All outcomes and recommendations and subsequent action plans will be submitted to the Corporate Records & Information Governance Group (CRIG) for review, advice and guidance.

The IAO and IAA roles will document, understand and monitor;

- What information assets are held and for what purpose
- How information is created, amended or added to overtime e.g. access to the correct version
- Who has access to the information and why
- Understand and address the risk to the asset, providing assurance to senior management

Over all compliance with this policy will be reported through the Corporate Governance and Compliance Sub-committee.

Staff also need to be made aware that ad-hoc confidentiality audits are carried out by the Trust to identify access that does not meet the expected legitimate relationship rule. Any records access that does not meet such criteria will be investigated and if it is determined that access was not lawful then disciplinary action may be taken by the Trust.

5. COMMUNICATION

This Policy and associated documents will be made available via the Policies & procedures page on Trustnet. It will also be linked to the Health Records page and the Information Governance page on Trustnet.

All new staff will receive information regarding Health Records Security & Confidentiality Policy at Trust Induction.

The Policy and associated documents will be published in the Trust weekly bulletin – The Pulse.

Meta-compliance will be used to distribute the Policy electronically to all staff who access a computer and the Policy will also be made available on individuals My Compliance Portal.

Managers must ensure that staff who do not have access to a PC/mobile device are able to view this Policy and associated documents by other means.

6. MONITORING INTEGRITY OF THE SYSTEM

Updates or changes in legislation or regulation may affect this Policy. Any changes or updates will be agreed through the Clinical Records and Information Governance Group (CRIG).

All incidents and near misses relating to the security and confidentiality of service user records must be reported on the Trusts Datix system.

Any proposals for changes to the Policy will be carried out with the agreement of the Clinical Records & IG Group which is chaired by the Deputy Caldicott Guardian/Chief Clinical Information Officer.