Lincolnshire Community Health Services NHS Trust

Data Protection Policy

(Safe Haven and Information Sharing)

Reference No:	P_IG_26
Version:	2
Ratified by:	LCHS Trust Board
Date ratified:	11 May 2021
Name of author:	Data Protection Officer
Name of responsible committee:	Information Governance Management Assurance Group
Date approved by responsible committee:	21 April 2021
Date issued:	May 2021
Review date:	May 2023
Target audience:	All staff and third-party contractors employed by LCHS
Distributed via:	LCHS Website

Lincolnshire Community Health Services NHS Trust

Data Protection Policy

Version Control Sheet

Version	Section/Para/ Appendix	Version/Description of Amendments	Date	Author/Amended by
1		Amalgamation of policies P_IG_15, 17, content previously ratified and further content update to reflect GDPR.	June 2018	Kaz Scott
2		Full Review UK GDPR	Jan 2021	Kaz Lindfield-Scott
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				

Lincolnshire Community Health Services NHS Trust

Data Protection Policy

Contents

Lincolnshire Community Health Services NHS Trust

Data Protection Policy

Policy Statement

Background	The Trust is required to meet its legal obligations and NHS requirements concerning confidentiality and information security standards. The requirements within the Policy are primarily based upon the Data Protection incorporating the UK General Data Protection Regulation and the Data Protection Act 2018) which is the key piece of legislation covering security and confidentiality of Personally Identifiable Information (PII). The policy is split into sections and details specific procedures for achievement of the policy standards.
Statement	This policy covers records held and processed by the Trust which is responsible for its own records under the terms of the Act and it has submitted a notification as a Controller to the Information Commissioner.
Responsibilities	This Policy will apply to: • All staff including any temporary staff • Information or systems used and managed by the Trust; • Any individual using or requires access to information 'owned' by the Trust
Training	Facilitated via Trust Induction and Mandatory Annual Training updates
Dissemination	This policy will be published on the Trust Website.
Equality Statement	As part of our on-going commitment to promoting equality, valuing diversity and protecting human rights, Lincolnshire Community Health Services NHS Trust is committed to eliminating discrimination against any individual (individual means employees, patients, services users and carers) on the grounds of gender, gender reassignment, disability, age, race, ethnicity, sexual orientation, socio-economic status, language, religion or beliefs, marriage or civil partnerships, pregnancy and maternity, appearance, nationality or culture

DATA PROTECTION
The Trust has a legal obligation to comply with all appropriate legislation in respect of data, information and data security. It also has a duty to comply with guidance issued by the Department of Health and Social Care (DHSC), the Information Commissioner Office (ICO), other advisory groups to the NHS and guidance issued by professional bodies.

Penalties could be imposed upon the Trust and/or employees for non-compliance with relevant legislation and NHS guidance.

Aim
This Trust will meet its legal obligations and NHS requirements concerning confidentiality and information security standards. The requirements are based on the Data Protection (DP) legislation as this is the key piece of legislation covering security and confidentiality of PII.

Legislation
For the purpose of this Policy other relevant legislation may be referenced.

- Data Protection Act 2018 and UK GDPR
- Access to Health Records Act 1990
- Human Rights Act 1998
- Freedom of Information Act 2000
- Crime and Disorder Act 1998
- Computer Misuse Act 1990
- Police and Justice Act 2006
- Health & Social Care Act 2012

The following are the main publications referring to security and confidentiality of PII:

- Confidentiality: NHS Code of Practice
- Records Management Code of Practice 2020
- Information Security Management: NHS Code of Practice
- Employee Code of Practice (Information Commissioner)
- Guide to Confidentiality in Health and Social Care
- Information: Review of Data Security, Consent and Opt-Outs (Caldicott 3)
- National Data Guardian for Health and Care Review of Data Security, Consent and Opt-Outs
- Confidentiality: NHS Code of Practice - supplementary guidance: public interest disclosures
- Seven Data Protection Principles

Roles and Responsibilities

Chief Executive (CE)
Ultimate responsibility for security and confidentiality at Trust level.

Caldicott Guardian (CG)
Responsibility for safeguarding the confidentiality of patient information and enabling appropriate information-sharing.

Data Protection Officer (DPO)
To ensure the processing of personal data is in compliance with the applicable UK Data Protection Regulation and act as a contact point for data subjects and the Information Commissioner's Office (ICO).

Information Governance Management Assurance Group (IGMAG)
The IGMAG are responsible for coordinating improvements in data protection, confidentiality, information security and cyber security and over-seeing integrated Trust policies and reviewing procedures and risk issues and raising IG concerns to the Trust Board.

Managers
Directors and senior managers are responsible for ensuring that all staff comply with the policies and procedures and staff attend training on an annual basis, implement any necessary and reasonable changes required and ensure that any PII held is up to date and accurate.

All Staff
All staff, whether permanent, temporary or contracted are responsible for ensuring they are aware of the requirements incumbent upon them and for ensuring they comply with these on a day to day basis.

All staff are responsible for any records or data they create and with information they use.

Security & Confidentiality
All information relating to identifiable individuals and any information that may be deemed sensitive, must be kept secure at all times. The Trust shall ensure there are adequate policies and procedures in place to protect against unauthorised processing of information and against accidental loss, destruction and damage to the information.

Disclosure of Information & Information in Transit
It is important that information about identifiable individuals should only be disclosed on a strict legitimate 'need to know basis'.

Some disclosures may occur because there is a statutory requirement to disclose e.g. with a Court Order because other legislation requires disclosure under UK GDPR.

Portable media such as: disc, USB memory stick should be encrypted, or manual paper records scanned and sent by secure-mail or encrypted envelope.

If a member of staff wishes to process PII outside of the United Kingdom, the DPO must be consulted prior to any agreement to transfer or process information.

Training
This is carried out through formal awareness and training.

- Training on Data Confidentiality, Security and Compliance requirements under the Data Protection legislation shall be included in the staff induction process
- An ongoing awareness programme shall be maintained to ensure that staff awareness is refreshed and updated as necessary

All staff will be made aware of what could be classed as a Data Security Breach and the process to follow so that incidents can be identified, reported, monitored and investigated.

Contracts of Employment
Staff contracts of employment are produced and monitored by the Human Resources Team.

- Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a confidentiality clause.

Disciplinary
A breach of the DP principles could result in a member of staff facing disciplinary action. A copy of the Disciplinary Policy is available on the website.

Data Subject Access Request (DSAR)
Legislation allows an individual (Data Subject) a right of access to data processed by the Trust and is obliged to respond within one complete month. An extension of a further sixty days may be applied in exceptional circumstances where the request is likely to take longer than the statutory timescale. The Trust will inform the requester explaining the delay and agree a new deadline.

Failure to do so is a breach of the legislation and could lead to a complaint to the ICO.

Data Subject Rights
Under the UK GDPR, data subjects have enhanced rights.

These include:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

Disclosure of Personal Information
There are Acts of Parliament that govern the disclosure of personal information. Some of these Acts make it a legal requirement to disclose and others that state that information cannot be disclosed.

In the event a request for disclosure is made referencing any of these Acts the DPO may require notification prior to any information release.

- Professional bodies (e.g. NMC, GMC, CIPFA, CIMA) often release guidelines and advice for their own disciplines. These guidelines should not conflict with this policy or legislative requirements.

SAFE HAVEN AND INFORMATION SHARING
All NHS organisations require haven procedures to maintain the privacy and confidentiality of the PII held. The implementation of these procedures facilitates compliance with the legal requirements placed upon the Trust.

Where departments within the Trust, other NHS Trusts or other agencies want to send PII to a Trust department, they should be confident that they are being sent to a location which ensures the security of the data.

Several Acts and guidance dictate the need for 'Safe Haven' arrangements, they include:

Confidentiality: NHS Code of Practice: Annex A1 Protect Patient Information *"Care must be taken, particularly with confidential clinical information, to ensure that the means of transferring from one location to another are secure as they can be"*

Scope
This provides:

- The legislation and guidance which dictates the need for a safe haven
- When a Safe Haven is required and requirements and procedures to implement
- Rules for different kinds of safe haven

The processes described in this policy must be followed by all Trust staff, unless exceptional circumstances arise, which may have an impact on direct patient care.

This may include formal action in line with the Disciplinary process for Trust employees; and other action in relation to other workers, which may result in the termination of an assignment, placement, secondment or honorary arrangement. Non-compliance may also lead to criminal action being taken.

Safe Haven
The term is a location where arrangements and procedures are in place to ensure PII can be held, received and communicated securely.

However, any department sending, receiving, holding or communicating PII, should provide safe haven conditions by following the guidelines set out within this policy.

Personally Identifiable Information (PII)
Personal Identifiable Information is any data that can be used to clearly identify an individual. And **GDPR** also references sensitive personal data.

Special Category Data
Personal data revealing **racial or ethnic origin**; **political opinions**, **religious or philosophical beliefs, trade union membership**; **genetic data**; **biometric data** (where used for identification purposes, **data concerning health**, **a person's sex life; and sexual orientation**.

Data Flow Mapping
This is the process of documenting the flow of information from one physical location to another and the method by which it "flows". Data flows may be by: E mail, post/courier, text or portable electronic or removable media.

Anonymised Information
Anonymised data is data that is has been rendered unidentifiable in such a way that the natural person cannot be identified from that data.

Inter-Agency Information Sharing Protocol
The protocol is the high-level document setting out the general reasons and principles for information sharing. It shows that all signatory agencies are committed to maintaining agreed standards on handling information. It should be underpinned by information sharing agreements between the organisations who are actually sharing the information.

Data Sharing Agreement
The agreement is a more detailed document, the intention of which is to spell out how the organisations involved will operate the approach to information sharing.

Safe Havens - Location/Security Arrangements

- Sending/receiving PII, consideration should be given to the physical security arrangements i.e. locked room or accessible via a keycode, only known to authorised staff, or swipe card controlled.
- The office or workspace area should only be accessible to authorised members of staff in the same building.
- Windows should have locks and the room should conform to health and safety requirements in terms of fire, safety from flood, theft or environmental damage.
- Paper records containing PII must be stored in locked cabinets / rooms, where possible.
- Digital information should not be left on view or accessible to unauthorised staff and the screen 'locked' or logged/switched off when not in use.

Fax Machines
These must only be used for Business Continuity Planning (BCP) where it is **necessary**; e.g. Major Incident or Pandemic when the infrastructure to use other secure means of communication is affected.

Communication by Post
Transit envelopes must not be used for when PII is sent. Internal post can be sent safely on the Internal Courier as the vehicle is emptied each day therefore mitigating the loss of any post.

- All confidential information must be placed face down and not left unsupervised
- Mail should be opened away from public areas
- Outgoing post should be securely sealed securely in robust envelopes and clearly addressed to the department address or addressee only. Where possible use tamper-evident envelopes or tape/seals.
- Paper Records can be tracked to allow auditing and movement of them or scanned and sent electronically by secure e-mail or encrypted envelope

Information should be stored on the Trust's network and **not** on local computer hard drives i.e. 'C' drive (usually 'my documents') due to potential failure.

- PII and Commercially Sensitive must be stored securely and restricted as appropriate.
- Regular housekeeping of files to ensure only the minimum amount is retained.
- Any new system created / introduced or changes in data flow must undertake a Data Protection Impact Assessment (DPIA) and registered as an Information Asset to comply with DP legislation and Caldicott principles.

Phone:

- Information should not usually be provided over the telephone unless the identity of the caller can be verified
- Confirm the reason for the information request, take a contact number or switchboard, check whether the information can be provided; if in doubt, call the enquirer back and provide to the person requesting it

Transportation Arrangements

- PII should only be taken off site when absolutely necessary and transported in a sealed container (where possible)
- Never leave unattended and ensure all information is returned back to site as soon as possible, and records are updated

Displaying Personal Information (for example on white-boards)

Boards must be sited in areas that are **not** accessible by the public, e.g. staff offices. These rooms should be clearly marked 'staff only' and windows obscured appropriately.

If it is absolutely necessary to put information onto a whiteboard, it should be abbreviated or symbolised so only health professionals or staff can understand it. These areas should be carefully considered with a risk assessment undertaken by an appropriate manager.

Sharing Information with other Organisations

- You have consent or
- If a law says you have to or
- It's in the public interest
- Direct Care purposes
- Department for Health and Social Care in response to a Pandemic e.g. COPI

The Trust must be assured that organisations are able to comply with the safe haven ethos and meet certain legislative and related guidance requirements:

- DP legislation
- Common Law Duty of Confidentiality
- Confidentiality: NHS Code of Practice

Information sharing agreements must be put in place where personal information is to be shared. All flows of information coming in and going out of the department should be risk assessed as appropriate.

Monitoring

The Trust will monitor and audit its practices for compliance and will:

- Identify areas of operation that are covered by the Trust's policies and identify which procedures and/or guidance should comply to the policy;
- Set and maintain standards by implementing new procedures, including obtaining feedback where the procedures do not match the desired levels of performance.

NHSR Monitoring

Minimum requirement to be monitored	**Process for monitoring e.g. audit**	**Responsible individuals/ group/ committee**	**Frequency of monitoring /audit**	**Responsible individuals/ group/ committee (multidisciplinary) for review of results**	**Responsible individuals/ group/ committee for development of action plan**	**Responsible individuals/ group/ committee for monitoring of action plan**
DSPT Standards	Review / Audit / Reports	DPO	Annual	DPO / IGMAG	DPO / IGMAG	DPO / IGMAG

Equality Impact Analysis Screening Form

Title of activity	Data Protection Policy		
Date form completed	Jan 2021	Name of lead for this activity	Kaz Lindfield-Scott

Analysis undertaken by:		
Name(s)	Job role	Department
Kaz Lindfield-Scott	Data Protection Officer	Data Protection and Compliance

What is the aim or objective of this activity?	To provide effective management and accountability governance structures, processes, policies and procedures and a comprehensive IG/DP training adequately resourced to manage and embed IG and DP throughout the Trust.
Who will this activity impact on? *E.g. staff, patients, carers, visitors etc.*	All Staff and Service Users

Potential impacts on different equality groups:

Equality Group	Potential for **positive** impact	**Neutral** Impact	Potential for **negative** impact	Please provide details of how you believe there is a potential positive, negative or neutral impact (and what evidence you have gathered)
Age	☐	☒	☐	
Disability	☐	☒	☐	
Gender reassignment	☐	☒	☐	
Marriage & civil partnerships	☐	☒	☐	
Pregnancy & maternity	☐	☒	☐	
Race	☐	☒	☐	
Religion or belief	☐	☒	☐	
Sex	☐	☒	☐	
Sexual Orientation	☐	☒	☐	
Additional Impacts	☐	☒	☐	

If you have ticked one of the above equality groups please complete the following:

Level of impact

	Yes	No
Could this impact be considered direct or indirect discrimination?	☐	☒
If yes, how will you address this?		

	High	Medium	Low
What level do you consider the potential negative impact would be?	☐	☐	☐

If the negative impact is high, a full equality impact analysis will be required.

Action Plan

How could you minimise or remove any negative impacts identified, even if this is rated low?
How will you monitor this impact or planned actions?
Future review date: