Lincolnshire Community Health Services NHS Trust

Data Protection Policy

(Safe Haven and Information Sharing)

Reference No:	P_IG_26
Version:	1
Ratified by:	LCHS Trust Board
Date ratified:	14 August 2018
Name of originator/author:	Kaz Scott, Information Governance Lead
Name of approving committee/responsible individual:	Information Governance Management Assurance Group
Date issued:	August 2018
Review date:	August 2020
Target audience:	All staff and third party contractors employed by LCHS
Distributed via:	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				
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 General Data Protection Regulation 2016 and the Data Protection Act 2018) which is the key piece of legislation covering security and confidentiality of Personal Confidential Information (PCD).

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
- All 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.

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 (DH), 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 personal information.

Legislation

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

- Data Protection Legislation
- 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 or confidentiality of Personal Confidential Data (PCD):

- Confidentiality: NHS Code of Practice
- Records Management Code of Practice for Health and Social Care 2016
- 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)

Roles and Responsibilities

Chief Executive (CE)

The CE has ultimate responsibility for security and patient confidentiality at Trust level.

Caldicott Guardian (CG)

The CG has responsibility for safeguarding the confidentiality of patient information and enabling appropriate information-sharing.

Data Protection Officer (DPO)

The responsibility is primarily to provide technical expertise on data protection and confidentiality issues.

Information Governance Management Assurance Group (IGMAG)
The IGMAG are responsible for coordinating improvements in data protection, confidentiality and information security and over-seeing integrated Trust policies, and reviewing procedures and risk issues and for bringing 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 that staff attend training on an annual basis, implement any necessary and reasonable changes required and ensure that any personal data held is up to date and accurate.

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

All staff are responsible for any records or data they create and what they do 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 this information.

Disclosure of Information & Information in Transit
It is important that information about identifiable individuals (such as the general public, patients and/or staff) should only be disclosed on a strict 'need to know basis'.

Some disclosures of information may occur because there is a statutory requirement upon the Trust to disclose e.g. with a Court Order because other legislation requires disclosure (for staff to the tax office and if a patient has a communicable disease e.g. Tuberculosis).

If PCD need to be transported in any portable media such as: disc, USB memory stick or manual paper records, even more stringent measures should be employed to ensure that the data remains secure to maintain strict security and confidentiality of this information. Encryption of data in transit or scanning of paper records sent through secure e-mail.

In the event that any member of staff wishes to process personal information outside of the United Kingdom, IG must be consulted prior to any agreement to transfer or process information.

Training
This is carried out through formal awareness and training.

- IG 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 established and maintained in order to ensure that staff awareness is refreshed and updated as necessary

All staff will be made aware of what could be classed as an information security incident or breach of confidentiality. They will be made aware of 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 Workforce Services 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.

Subject Access Request (SAR)
DP legislation allows an individual who is the subject of personal information processed by the Trust to access their information. In the event that an individual wishes to have a copy of their information under the subject access provision of the legislation a request must be made in writing to the Access to Information Team.

The Trust is obliged to respond to requests within 21 working days and comply within one calendar month of a request being made for access to records containing PCD. Failure to do so is a breach of the legislation and could lead to a complaint to the ICO. If it is anticipated that a request will take longer than the statutory timescale, the Trust will inform the applicant giving an explanation of the delay and agree a new deadline.

Data Subject Rights
Under the legislation, data subjects (patients and staff) have enhanced rights. These include:

- Whether or not personal data concerning the data subject are being processed, and, where that is the case, access to the personal data and the following information:
- The purposes of the processing
- The categories of the personal data
- The recipients of the personal which is to be disclosed
- How long the data will be processed by the trust
- The right to request to rectify or erase any data held by the trust
- The right to be told if any automated decision making is taking place, including profiling
- The right to restrict the processing of the personal data
- The right to data portability
- The right to access any personal data held by the trust
- The right to be told is any personal has been affected on the occasion of a data breach/loss

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 that a request for disclosure is made referencing any of these Acts the Trust DPO must be notified prior to any information being released.

- 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 safe haven procedures to maintain the privacy and confidentiality of the personal information 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 personal information to a Trust department, they should be confident that they are being sent to a location which ensures the security of the data.

A number of Acts and guidance dictates the need for safe haven arrangements to be set in place, 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
- A definition of the term 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.

Definitions

Safe Haven
The term safe haven is a location situated on Trust premises where arrangements and procedures are in place to ensure Personal Confidential Data (PCD) can be held, received and communicated securely. In a Trust they are the point from where PCD is controlled.

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

PCD
This relates to information about a person which would enable that person's identity to be established by one means or another.

This might be fairly explicit such as an unusual surname or isolated postcode or bits of different information which if taken together could allow the person to be identified.

All information that relates to an attribute of an individual should be considered as potentially capable of identifying them to a greater or lesser extent. This includes the nationally recognised NHS number.
Special Category Data

This is information where loss, misdirection or loss of integrity could impact adversely on individuals, the organisation or on the wider community.

This is wider than, but includes, data defined as sensitive under the legislation.

beliefs, or trade union Personal data revealing racial or ethnic origin, political opinions, religious or philosophical membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation

Information / Data Flow / Information 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, fax, 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 sharing data. The protocol will show that all signatory agencies are committed to maintaining agreed standards on handling information and will publish a list of senior signatories. It should be underpinned by information sharing agreements between the organisations who are actually sharing the information.

Information Sharing / Confidentiality 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

- Any area sending/receiving PCD should consider the physical security arrangements i.e. a room that is locked or accessible via a coded key pad known only to authorised staff, or swipe card controlled. This should be the first step in the aim to create safe haven conditions
- The office or workspace should be sited that only authorised staff can enter i.e. not an area which is readily accessible to any member of staff in the same building, or any visitors
- If sited on the ground floor, any windows should have locks on them
- The room should conform to health and safety requirements in terms of fire, safety from flood, theft or environmental damage
- Paper records containing PCD must be stored in locked cabinets / rooms, where possible
- Computerised information should not be left on view or accessible to unauthorised staff and the screen 'locked' or logged/switched off when not in use
- Confidential information should not be removed from a safe haven unless absolutely necessary

Fax Machines
Fax machines must only be used to transfer PCD where it is **absolutely** necessary to do so and the use of secure e-mail to communicate confidential information is recommended.

- Faxing must be limited
- Fax is sent to a safe location where only staff that have a legitimate right to view
- Use a Fax Header Sheet with confidentiality clause / disclaimer
- Ensure Fax number is correct, use Pre-programmed numbers
- Maintain an up-to-date list
- Telephone recipient before & after
- Confidential faxes are not left lying around for unauthorised staff to see

Communication by Post
Transit envelopes must not be used for when PCD 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 sensitive records must be placed face down in public areas and not left unsupervised
- In-coming mail should be opened away from public areas
- Outgoing mail should be sealed securely in robust envelopes and to be opened by addressee only (if the information is particularly sensitive or intended for a particular individual). Where possible use tamper-evident envelopes or tape/seals.
- Confirm the name, department and full address of the recipient before sending any information out, and ask the recipient to confirm receipt
- Paper Records can be tracked to allow auditing and movement of them

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

- Confidential Information must be stored securely and restricted as appropriate.
- Regular house-keeping of files, ensuring only the minimum amount of data is retained
- Any new database/system created / introduced that contain PCD must be registered as an Information Asset and comply with DP legislation and Caldicott principles

Phone:
- Information should not usually be provided over the telephone as the identity of the caller cannot always be verified
- Always confirm the name, job title, department, and organisation of the person requesting the information
- Confirm the reason for the information request
- Take a contact number i.e. main switchboard (never a direct line or mobile telephone number unless known to you)
- Call them back (always call the switchboard) to confirm the details, if necessary
- Check whether the information can be provided; if in doubt tell the enquirer that you will call them back
- Provide the information only to the person, who requested it, do not leave messages

Other Transportation Arrangements
- PCD should only be taken off site when absolutely necessary
- Information must be transported in a sealed container (where possible)
- Never leave PCD unattended
- 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 containing PCD 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 clinical information onto a whiteboard, the information should be abbreviated or symbolised so only health professionals can understand the information not other members of staff that may come into the department.

The use of PCD in patient areas should be carefully considered and a risk assessment undertaken by an appropriate manager.

Sharing Information with other Organisations
Information must only be shared if:

- You have patient consent or
- If a law says you have to or
- It's in the public interest
- Direct Care purposes

Employees of the Trust authorised to disclose information to other organisations outside the NHS must seek assurance that these organisations have a designated Safe Haven point for receiving personal information.

The Trust must be assured that these 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/confidentiality agreements must be put in place with organisations 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.

NHSLA 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	IG Lead	Annual	IG Lead / IGMAG	IG Lead / IGMAG	IG Lead / IGMAG

Equality Analysis

A.	Briefly give an outline of the key objectives of the policy; what it's intended outcome is and who the intended beneficiaries are expected to be	To provide clear and effective management and accountability structures, governance processes, documented policies and procedures, a comprehensive IG training programme and adequate resources to manage and embed IG throughout the Trust.		
B.	Does the policy have an impact on patients, carers or staff, or the wider community that we have links with? **Please give details**	All Staff and Service Users		
C.	Is there is any evidence that the policy\service relates to an area with known inequalities? **Please give details**	No		
D.	Will/Does the implementation of the policy\service result in different impacts for protected characteristics?	No		
		Yes	No	
	Disability		X	
	Sexual Orientation		X	
	Sex		X	
	Gender Reassignment		X	
	Race		X	
	Marriage/Civil Partnership		X	
	Maternity/Pregnancy		X	
	Age		X	
	Religion or Belief		X	
	Carers		X	
	If you have answered 'Yes' to any of the questions then you are required to carry out a full Equality Analysis which should be approved by the Equality and Human Rights Lead – please go to section 2			
The above named policy has been considered and does not require a full equality analysis				
Equality Analysis Carried out by:		Kaz Scott, IG Lead		
Date:		May 2018		