Lincolnshire Community Health Services NHS Trust

Information Risk Policy

(Information Assets and Data Protection Impact Assessments)

Reference No:	P_IG_30
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 the Trust
Distributed via:	LCHS website

Lincolnshire Community Health Services NHS Trust

Information Risk Policy

Version Control Sheet

Version	Section/Para/ Appendix	Version/Description of Amendments	Date	Author/Amended by
1		Amalgamation of policies P_IG_12, 14, content previously ratified and further content update to reflect GDPR.	June 2018	Kaz Scott
2		Full Review UK GDPR	March 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

Information Risk Policy

Contents

Lincolnshire Community Health Services NHS Trust

Information Risk Policy

Policy Statement

Background	The Trust aspires to the highest standards of corporate behaviour and clinical competence, in order to ensure that safe, fair and equitable procedures are applied to all organisational transactions, including relationships with patients, public, staff, stakeholders and the use of public resources. In order to provide clear and consistent guidance, the Trust will develop documents to fulfil all statutory, organisational and best practice requirements.
Statement	This document sets out the approach to information risk.
Responsibilities	This document applies to: All full-time and part-time employees of the Trust, and to non-executive directors, contracted third parties (including agency staff), locums, students and trainees, seconded and other staff on temporary placements and staff of partner organisations with approved access; Other individuals and agencies who may gain access to data, such as volunteers, visiting professionals or researchers, and companies providing ICT Services to the Trust.
Training	Training will be facilitated via Trust induction and mandatory annual training updates for all staff.
Dissemination	The 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

INFORMATION RISK
The Trust aspires to the highest standards of corporate behaviour and clinical competence, in order to ensure that safe, fair and equitable procedures are applied to all organisational transactions, including relationships with patients, public, staff, stakeholders and the use of public resources. In order to provide clear and consistent guidance, the organisation will develop documents to fulfil all statutory, organisational and best practice requirements.

Purpose and scope
The purpose of this is to establish employee responsibility and the rules of conduct for all members of staff regarding information risk management. This applies to all staff in the Trust whether operating directly or providing services to other organisations under a service level agreement (SLA) or joint agreement.

It is Trust policy to ensure that:

- Information is protected against unauthorised access and confidentiality is assured
- Integrity of information is maintained, available and delivered to the right person
- Regulatory requirements and legislation are met
- Information technology systems are used in a manner that ensures safe use
- Information that can be used to identify a person including confidential information, business information and commercially sensitive information is restricted to authorised users only
- Business Continuity Plans (BCP) are produced, maintained and tested
- Information security training is available to all staff

The lawful and correct handing of personal information is very important to the successful delivery of health services and to maintaining confidence in the Trust as a whole.

Procedure – Information Risk Principles
Creating an information handling culture

- It is the responsibility of the Trust Board to create an information handling culture. This must permeate throughout and inform all how to perform daily tasks, regardless of seniority.
- Managers must not just acknowledge that information is valuable, and risks must be mitigated. This must portray through decisions and actions, the importance of handling information.
- All staff should know good information handling is part of their job.
- Senior staff will understand they are bound by the same rules as junior staff. They must not override, for reasons of convenience, risk controls.
- All staff should be able to answer general questions about information protection and make sensible information risk decisions themselves including knowing the limits of their competence and when to defer to others for guidance.
- All staff Development Plans should include competencies on information handling.
- Staff should be encouraged to question instructions that seem inappropriate on information risk grounds and to report instances of inappropriate behaviour.

Information Risk Management Programme
This will be aligned to the Trust's business plan to support individual objectives and ensure they are adequately resourced. The Programme will cover:

- The balance between level of risk, tolerance and the effort used to manage the risk,
- Identification of gaps between the current and target risk positions
- Progress being made against agreed information risk priorities
- The effectiveness of the risk management controls including successes and failures

Risk Mitigation
Risk mitigation must:

- Be commensurate with the level of the risk – it does not need to remove the risk
- Be kept simple so it is manageable and can be communicated to staff
- Include monitoring and reporting on the ongoing level of information failures and security breaches so the effectiveness being achieved can be assessed

Risks must be assessed in terms of general level of harm that could be caused if information were to fail or be compromised.

Mitigation should take the form of a wide range of controls directed at reducing the likelihood of an information failure and reducing the amount of harm a failure could cause. Controls covering both will reduce the likelihood of failure and reduce the amount of harm and will enhance overall mitigation.

Plan - Do - Check - Act
A risk-based approach means there will always be some level of risk that will be tolerated. Controls must be applied under constraints of:

- Expertise, Cost. Effort and Practicability

The 'Plan' and 'Do' aspect must to be supported by 'Check' and 'Act'. This will ensure the required controls have been implemented adequately and action plans are in place to address shortfalls.

Monitoring and further mitigation
The Trust is required to monitor protection failures and deal with incidents to contain the harm they cause. Analysis of incidents will support in understanding the real level of risk being experienced in adjusting the controls in place.

The dynamic nature of evolving information use and technology requires regular re-evaluation of risk and controls to ensure these do not develop or constrain operational effectiveness or exceed risk tolerance levels.

The Trust Board will ensure it understands and accepts the aggregate information risk position to ensure the information protection obligations are being fulfilled.

Roles & Responsibilities

Trust Board
Has overall responsibility for setting the strategic context in which organisational process documents are developed, and for establishing a scheme of governance for the formal review and approval of such documents.

Chief Executive (CE)
The Accounting Officer (AO) is the CE who has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level which are handled in a similar manner to other risks such as financial, legal and reputational risks.

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

Senior Information Risk Officer (SIRO)
An executive Board member with allocated lead responsibility for the Trust's information risks and provides a focus for the management of information risk at Board level.

Responsibilities include:

- To provide a focal point for the resolution and/or discussion of information risk issue;
- Ensuring the Trust has a plan to achieve and monitor the right culture, across the Trust and with its business partners;
- Make corporate decisions on the viability of presented information risks
- Owning the overall information risk policy and risk assessment process, testing its outcome and ensuring that it is used.
- Advising the CE on the information risk aspects of their statement on internal control.

Data Protection Officer (DPO)
Provide specialist advice to the risk owners, enabling them to understand their obligations and risk profile fully so they can make well informed decisions about how best to treat any privacy risks. The risks are usually attached to the corporate objectives or stakeholder expectations

Data Protection and Compliance Team
Under the direction of the DPO to support for effective management, accountability, compliance and assurance for all aspects of IG/DP. The key tasks include:

- Responsibility for delivering a high-quality specialist service to the Trust
- To provide strategic direction, planning and guidance to ensure compliance with legislation and the national agenda
- Ensure work practices are evaluated and supported through the development of appropriate policy and procedures across the Trust

This is done by;
- Promoting awareness by organising training, campaigns and providing written procedures/guidance that are widely disseminated and available to staff;
- Co-ordinate with the notifications and investigation of such breaches of confidentiality or data loss with the ICO
- Develop and maintain the Information Asset Register (IAR) working with IAOs and IAAs to help mitigate risk

Data Protection Impact Assessment (DPIA)
A process to help identify and minimise the data protection risks of a project which must be undertaken for processing that is likely to result in a high risk to individuals.

Information Asset Register (IAR)
All Information Assets should be identified and have a nominated Information Asset Owner (IAO). Accountability for assets helps to ensure that appropriate protection is maintained and any risks to data loss minimised whilst identifying data flows of processing activities.

Any new processes that are introduced should be identified by the IAO in order to ensure that any impacts to information security, confidentiality or integrity are identified prior to implementation and initiation of any new system

Information Asset Owners (IAO)
Their role is to understand what information is held, what is added and what is removed, how information is moved, who has access and why. They are able to understand and address risks to the information assets they 'own' and to provide assurance to the SIRO.

The IAO will therefore document, understand and monitor:

- Lead and foster a culture that values, protects and uses information for public good;
- Know what information the asset holds, what information is transferred in / out of it;
- Know who has access and why, and ensure that their use of the asset is monitored;
- Understand and address risks to the asset, provide assurance to the SIRO
- Any new IA have a completed Data Protection Impact Assessment (DPIA)

Any changes to an IA are documented and follow the correct change control;

- Review their IA on an annual basis at a minimum and put procedures, controls and BCP in place to ensure the integrity and availability

Information Asset Administrators (IAA)
IAA work with an IAO. They ensure that policies and procedures are followed, recognise actual or potential security incidents; consult their IAO on incident management.

- The general data quality of their IA and report areas of concern to the IAO;
- Ensuring that personal information is not unlawfully exploited;
- Recognising potential or actual security incidents and consulting the IAO;
- Under the direction of their IAO, ensuring information is securely destroyed when there is no further requirement for it;
- Ensuring that local information handling constraints (e.g. limits on who has access to the assets) are applied, referring any difficulties to the relevant IAO;
- Reporting to the relevant IAO on current state of local information handling;

All Staff
To be aware that confidentiality and security of information includes all information relating to the Health and Care Community, its patients, service users, carers and employees.

Such information may relate to personal data of staff or patient records, electronic databases or methods of communication containing Personally identifiable Information (PII) including mobile devices.
Staff will be expected to

- Read and comply with the Confidentiality: Staff Code of Practice which forms part of their contract of employment;
- Adhere to the Data Protection Policy and any associated procedures/guidelines;
- Attend all mandatory training and awareness programmes;
- Ensure that all PII is accurate, relevant, up-to-date and used appropriately on both electronic and manual records and devices;
- Share information on a 'need to know' basis only
- Ensure that all PII is always safe and secure and in line with the Records Management Code of Practice 2020;
- Be aware personal and sensitive information should not be published on the website.
- Ensure any incidents and or events are reported that could have an impact on the IA; this can be done through the incident reporting procedure.

PII must not be taken home or kept at home unless authorised. Do not store on home PC's as these can be easily compromised putting all the information at risk. If an employee is found to have made an unauthorised disclosure they may face disciplinary action, which could lead to dismissal and legal action.

Information Governance Management Assurance Group (IGMAG)
The IGMAG will receive regular IG reports on a quarterly basis, which will include information on data protection/confidentiality, information risk, security and sharing as a matter of routine, including details of any breaches of confidentiality or data loss.

Training/Support
Support and guidance in relation to information risk management and conducting a DPIA to fulfil the obligations set out will follow the Trust DPIA process.

INFORMATION ASSETS AND DATA PRIVACY IMPACT ASSESSMENT (DPIA)
An IA can be defined as an operating system, infrastructure, business application, off-the-shelf product, user-developed applications, records and information. It will have recognisable and manageable value, risk, content and lifecycles and can range from a basic Excel spread sheet or database to a national system. Within the Trust there are hundreds of such systems, both electronic and paper that hold information relating to service users and staff.

To assess whether you have an IA the following questions should be asked:

- Does the information have value/use to the Trust?
- Will it cost money to reacquire?
- Would there be legal, reputational or financial repercussions if you couldn't produce it on request?
- Would it influence operational efficiency if you could not access it easily?
- Would there be consequences of not having it?

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

The ICO may, in certain circumstances service a monetary penalty notice on an organisation 2% - 4% of the annual turnover.

Statement/Objective
The Trust has a commitment to ensure that IA are managed in accordance with all relevant regulations and guidance. This process supports the implementation, identification and management for all IA within The Trust.

A DPIA should be carried out whenever a new process or information asset is likely to involve a new use or significantly change the way in which personal data is handled. Numbers of DPIAs received will be reported quarterly in the Assurance Reports presented at IGMAG.

Business Continuity (BC)
BC is a core component of corporate risk management and emergency planning. Its purpose is to counteract or minimise interruptions to Trust business activities from the effects of major failures or disruption to its IA (e.g. data, data processing facilities and communications).

Approved BCPs must be in place for all critical IA and all staff aware of their roles and responsibilities. IAO's have implemented approved procedures and controls for their information assets and have effectively informed all relevant staff.

BCPs, and system specific procedures and control measures are regularly reviewed, and where necessary tested, to assess their ability to meet their business objectives
Transfer of Data outside the UK

Transfers of personal data to countries outside the EU are only permitted where the adequacy conditions laid down in UK GDPR are met.

Training
IAO/IAA training is available, and the Data Protection and Compliance (DP&C) will work with line managers to ensure that additional training is available, as appropriate to support staff.

DP&C will work with the CG, SIRO, IAO/IAA and the Communications Team to maintain continued awareness of confidentiality and security issues to both staff and the individual through Team Brief, newsletters, leaflets, posters, web services, etc.

Compliance
The Trust must demonstrate compliance with the Data Security and Protection Toolkit (DSPT) which draws together the legal rules and central guidance and presents them in one place. It is required to carry out self-assessments of its compliance against the National Data Guardian's (NDG) 10 data security standards on an annual basis.

A key element of the toolkit is

- To ensure that all IA that hold personal data are protected by appropriate organisational and technical measures

Monitoring Compliance
This is through audit, monitoring and review through the number and type of incidents.

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	Information Risk Management Policy		
Date form completed	Mar 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: