Lincolnshire Community Health Services NHS Trust

Information Risk Policy

(Information Assets and Data Privacy Impact Assessments)

Reference No:	P_IG_30
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 the Trust
Distributed via:	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				
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.

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 policy 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 the policy of the Trust 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 their safe use
- Information that can be used to identify a person including confidential information about that person, business information and confidential business 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 treatment of personal information is very important to the successful delivery of health care 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 must inform everyone's approach as to how they perform their daily tasks, regardless of seniority.
- Managers must not just acknowledge that information is valuable and risks must be mitigated. They must portray through their 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 for themselves including knowing the limits of their competence and when to defer to others for guidance.
- All staff Personal Development Plans should include competencies on information handling.
- The board must encourage all staff to question instructions that seem inappropriate on information risk grounds and must encourage reporting on instances of inappropriate behaviour.

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

- The balance between level of risk, tolerance of risk and the effort being 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 reasonably 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' aspect and 'Do' aspect must to be supported by 'Check' and 'Act'. This will ensure that required controls have been implemented adequately and that action plans are in place to address shortfalls.

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

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

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

Roles & Responsibilities

Trust Board
The 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 Trust's Accounting Officer is the CE who has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level.

Caldicott Guardian (CG)
The CG is the person with overall responsibility for protecting the confidentiality of Personal Confidential Data (PCD). The CG plays a key role in ensuring that the Trust and partner organisations abide by the highest level of standards for handling PCD.

They are responsible for ensuring that their Trust adheres to the Caldicott Principles and to feedback any IG issues to the appropriate board.

Senior Information Risk Officer (SIRO)
The SIRO is 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 IG culture, across the Trust and with its business partners;
- Make corporate decisions on the viability of presented information risks
- Owning the Trust's overall information risk policy and risk assessment process, testing its outcome and ensuring that it is used.
- Advising the chief executive on the information risk aspects of their statement on internal control.

Information Governance (IG)
IG is responsible for providing support and guidance to staff with regard to the management of their Information Asset (IA).

This is done by;
- Promoting awareness by organising training, awareness 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

Information Asset Owners (IAO)
The IAO provides a common, consistent and unambiguous understanding of what information they hold, how important it is, how sensitive it is, how accurate it is, how reliant

they are on it, and who's responsible for it. The IAO is expected to understand the overall business goals of the Trust and how the IA they own contribute to and affect these goals.

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 Privacy 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;
- Put procedures, controls and BCP in place to ensure the integrity and availability

Information Asset Administrators (IAA)
IAA are staff who understand and are familiar with the IA within their area. If an IAA has been appointed they are responsible for;

- 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 that information is securely destroyed when there is no further requirement for it;
- Ensuring that local information handling constraints (e.g. limits on who can have 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
Need 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 staff or patient/client's records, electronic databases or methods of communication containing PCD 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 PCD 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 PCD is kept safe and secure at all times and in line with the Records Management Code of Practice for Health and Social Care 2016;
- Be aware that personal and sensitive information should not be published on the Trust's 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.

PCD must not be taken home or kept at home unless authorised or stored 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.

Information Asset Register (IAR)

All IA of the Trust should be identified and have a nominated IAO. Accountability for assets helps to ensure that appropriate protection is maintained and any risks to data loss minimised.

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.

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 or not 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 have an effect on 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 (DH), 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 policy 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 an organisation's 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 are 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
All BCPs are to be completed by the IAO and signed off for approval.

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

Training
IG training is mandatory for all staff on induction and on an annual basis. The IG Lead will work with line managers to ensure that additional training is available, as appropriate to support staff.

IAO/IAA training is available and compulsory and this is to be completed annually and will align to IG Training.

IG 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 as a set of IG requirements. It is required to carry out self-assessments of its compliance against the IG requirements on an annual basis.

A key element of the toolkit is

- To ensure that all IA that hold, or are, 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.

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		
Date:		June 2018		