Leeds Community Healthcare NHS Trust

Information Governance Policy and Framework	
Author (s)	Narissa Leyland – Head of Information Governance & Data Protection Officer
Corporate Lead	**Leeds Community Healthcare NHS Trust** Executive Director of Finance and Resources
Document Version	3.0
Document Status	Approved
Date approved by Clinical and Corporate Policies Group (CCPG)	5th November 2018
Date ratified by SMT	28th November 2018
Date issued	3rd November 2018
Review date	28th November 2021
Policy Number	PL301

Executive summary

The NHS is in a state of considerable change, with new legislation and guiding frameworks being implemented in 2018. To ensure this is undertaken effectively for all patients and staff, the Trust is implementing this policy, based on Department of Health (DH) guidelines and Data Protection (DP)-related law.

From 25 May 2018 the main piece of legislation is the EU General Data Protection Regulation (GDPR). This has been complemented with domestic legislation, which is the Data Protection Act 2018 (DPA).

This policy sets out the strategic IG agenda for Leeds Community Healthcare Trust. It relies strongly on a risk-based approach to the identification of Information Assets (IA) and ownership of such IAs by Information Asset Owners (IAO) through a robust Information Management (IM) programme.

Equality Analysis

Leeds Community Healthcare NHS Trust's vision is to provide the best possible care to every community. In support of the vision, with due regard to the Equality Act 2010 General Duty aims, Equality Analysis has been undertaken on this policy and any outcomes have been considered in the development of this policy.

Contents

1. Introduction

Information is a vital asset clinically and for the efficient management of services, resources and performance. It is therefore important that an appropriately robust policy framework is in place. Information Governance (IG) stipulates the way in which information, particularly in an NHS environment, how Personal Confidential Data (PCD) should be handled. IG also enables the Trust to ensure that all confidential information is dealt with legally, securely and efficiently, in order to deliver the best possible care to its patients.

2. Definitions

Personal Confidential Data is:

- Personal information about identifiable individuals, which should be kept private.
- The Data Protection (DP) legislation definition of personal and special categories of data, adapted to include those who have passed away (see next two paragraphs for definitions).
- Information 'given in confidence' and 'that which is owed a duty of confidence'.[1]

Under the new DP legislation **Personal Data is defined** as:

Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[2]

And **Special Categories of Personal Data is defined** as:
Racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union 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.[3]

3. Aims and Objectives

To ensure good practice across the Trust there are robust IG processes in place to support the successful local implementation of national legislation and guidance:

- An annual IG audit.
- Oversight by the healthcare regulator, the Care Quality Commission (CQC).
- A mandatory training and awareness programme.
- A staff Confidentiality Code of Conduct, distributed to all staff.
- A robust plan to communicate Confidentiality and DP to Data Subjects.
- An Information Asset Management (IAM) and Business Continuity (BC) programme.

[1] Independent Information Governance Oversight Panel (2013), *Information: To Share or Not to Share*, p.130.
[2] General Data Protection Regulation, Article 4(1).
[3] General Data Protection Regulation, Article 9(1).

- An Information Risk Management (IRM) programme.
- Data Protection Impact Assessments (DPIA) for new projects and proposals.
- Robust Information Security (IS), Cyber Security and User Access Controls.
- Safe Haven processes to ensure data is safely transmitted and received.
- Systematic Records Management processes.
- Robust IG clauses in third party contracts.
- Clarity on the legalities of processing data and the use of consent.
- Robust Information Sharing processes.
- Assurance on the transfer of PCD (Personal Confidential Data) outside the UK.
- Data Quality Assurance.
- Subject Access Requests (SAR), allowing subjects to view and check their information.
- Clarity on the disclosure of information to the police.
- Robust processes for the reporting and analysis of information-related incidents.

4. Responsibilities

All staff employed by Leeds Community Healthcare NHS Trust must work in concordance with the Leeds Safeguarding Multi-agency Policies and Procedures and local guidelines in relation to any safeguarding concerns they have for service users and the public with who they are in contact.

Everyone within the Trust has a level of IG responsibility:

The Trust Board: The Board is ultimately responsible for ensuring the IG function is addressed.

Chief Executive: The individual with overall accountability for IG within the Trust is the Accountable Officer, the Chief Executive. The role provides assurance, through a Statement of Internal Controls, that all risks to the organisation, including those relating to information, are effectively managed and mitigated.

Senior Information Risk Owner: The (SIRO) is the Director of Finance and Resources with overall responsibility for the organisation's Information Risk Management. The SIRO also leads and implements the IG risk assessment and advises the Board on the effectiveness of Information Risk Management (IRM) across the organisation.

Caldicott Guardian: The Caldicott Guardian is the Medical Director, this is an advisory role and has responsibility for protecting the confidentiality of patient information and ensuring it is shared appropriately and securely. The Caldicott Guardian is supported by the Trust's IG Team.

Head of Information Governance & Data Protection Officer: The Head of Information Governance & Data Protection Officer has the leadership function for IG, maintaining the confidence of patients, staff and the public, through advice and guidance on the creation of robust and effective mechanisms and assurance processes to protect and appropriately handle PCD. This includes ensuring that the Trust is fully compliant with all IG-related legislation and that the Trust meets statutory and mandatory obligations for IG through development of strategy and implementation of IG policies and procedures.

Information Security Manager: A role held by the Head of Information Technology, it provides advice on all aspects of Information Security (IS). Their assessment of IS risks, threats and advice on controls contributes significantly to the effectiveness of the Trust's information security. The role holder is required to hold a formal IS qualification.

Information Asset Owners (IAOs): The SIRO is supported by IAOs. The role of an IAO is to understand what information is held, how it is used, who has access and why for information systems under their responsibility. Consequently they can understand and address risks to the IAs they own and to provide assurance to the SIRO on their security and use, including the creation of System Level Security Policies. The IG Team support the IAOs in fulfilling their role.

Information Governance Group (IGG): IGG has representatives from across the Trust and is responsible for overseeing the implementation of the Information Governance Policy and Framework also the annual IG assessment. The Group also reviews and approves IG-related documentation. The Group reports to the Audit Committee and through that to the Trust Board. IGG has a key function to monitor and review IG incident trends and guide overarching remedial action to those trends.

Directors, Managers and Supervisors: All managers have a responsibility to promote this policy and enable good IG practice within their areas. They must promote that national and local IG standards are upheld within their department and advising all staff of their IS, confidentiality and data quality responsibilities and supporting planned evaluation / audit of IG tasks, and implementing necessary actions. They also have a responsibility to liaise with the IG Team where necessary regarding issue and/or incidents of concern.

All staff: Staff have responsibility to abide by their legal, professional ethical and contractual responsibilities for IG related issues, regardless of their position, and whether directly employed or not. They must also comply with the most up-to-date version of this policy and other Trust IG policies / procedures, and undertake annual IG mandatory training.

5. Overarching Legislation and Principles

A range of components fall under IG as it overlaps Clinical Governance and is a subset of Corporate Governance. The National Data Guardian Review on Data Security, Consent and Opt-outs[4] outlines the National Data Security Standards, which the Trust must adopt. Local implementation of the National Data Security Standards is supported by compliance with the Data Security and Protection Toolkit (DSPT), which replaces the IG Toolkit in April 2018.

In its management of PCD, the Trust complies with Data Protection Act 2018 and Caldicott Principles. Under the new law, PCD must be processed in line with six principles:

[4] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/535024/data-security-review.PDF

1. Fairly, lawfully and transparently.
2. For specified purposes.
3. Using the minimum amount necessary.
4. Accurately.
5. For only as long as it is needed.
6. Securely

Individuals (Data Subjects) also have rights under the new legislation to:

1. **Information about how their information is being processed.** The Trust addresses this by ensuring a layered approach to informing data subjects how their information is used, including posters, pamphlets and service-level leaflets.

2. **Access to their personal information.**

3. **Rectification when information is wrong.** Any request for rectification will be assessed on a case by case basis using the precedent of the Trust's developing experience of the new legislation, along with relevant case law.

4. **Be forgotten, when it is appropriate.** In healthcare, information needs to be retained for care and medicolegal purposes, rendering this right largely exempt. Any request to be forgotten will be assessed on a case by case basis using the precedent of the Trust's developing experience of the new legislation, along with relevant case law.

5. **Restrict processing.** Data Subjects may request that the Trust hold only sufficient Personal Data about them, but not process it any further. Any request for restriction of processing will be assessed on a case by case basis using the precedent of the Trust's developing experience of the new legislation, along with relevant case law.

6. **Data portability.** This allows Data Subjects to obtain and reuse their information across different services. In healthcare there are not expected to be many requests, as much information is available as a SAR. Any request for portability of data will be assessed on a case by case basis using the precedent of the Trust's developing experience of the new legislation, along with relevant case law.

7. **Object to processing.** This allows the Data Subject to object if they do not believe the use of their information is legitimate. Any request to object will be assessed on a case by case basis using the precedent of the Trust's developing experience of the new legislation, along with relevant case law.

8. **Appropriate decision-making.** The Trust is required to demonstrate that it has a lawful basis to carry out profiling and / or automated decision-making. This is undertaken by an annual organisation-wide assessment, led by the IG Team.

All requests from Data Subjects to exercise their rights must normally be responded to within 1 month (30 days) unless there are extenuating circumstances, in which case there are some rights to extension under the legislation.
In the NHS, the Caldicott Principles are equally as important; when using PCD:

1. Justify the purpose(s).
2. Don't use it unless it is absolutely necessary.
3. Use the minimum necessary.
4. Access should be on a strict need to know basis.
5. Everyone with access to it should be aware of their responsibilities.
6. Comply with the law.
7. The duty to share information can be as important as the duty to protect patient confidentiality.

6. Effective Information Governance Management

To ensure good practice across the Trust there are robust IG processes in place:

a) Annual Information Governance Audit

From April 2018 the Trust's IG compliance will be measured via an annual self-assessment process of compliance against standards set out in the Data Security & Protection Toolkit (DSPT). The Trust will utilise the tool to assess its IG practice in broadly the same manner as its IG Toolkit (IGT), DSPT predecessor, to assess its compliance against national security standards.

b) Care Quality Commission Oversight

CQC, as outlined in *Safe Data, Safe Care* (2016),[5] have powers to inspect the Trust's IG as part of its inspection process. To this end the Trust must ensure that robust IG practices are in place. CQC specifically requires that Medical Records are accurate, fit for purpose, held securely and confidentially.

c) Mandatory Training and Awareness

Fundamental to the success of delivering a robust IG agenda across the Trust is the development of an IG-aware culture. Training is provided to all staff to promote this ethos. In practical terms, since IGT v13, this means 95% of all staff must be adequately trained.

In addition to formal IG training, a layered approach to awareness is employed, acknowledging a broader understanding of training to encapsulate raising awareness.[6]

Some roles, such as SIRO, Caldicott Guardian, and IAOs are required to undertake regular training to remain current in their role.

All decisions on the need for training will be documented in a Training Needs Analysis, which must be ratified by the Information Governance Group (IGG).

[5] Care Quality Commission (2016), *Safe Data, Safe Care*.

[6] Among others these include Global emails, articles in Trust newsletters, bespoke advice; IG Team attendance at departmental meetings; Community Talk articles and the Information Governance Staff Handbook.

d) Confidentiality Code of Conduct

All staff must be aware of their individual responsibilities for the maintenance of confidentiality, Data Protection, Information Security management and data quality. They are given the tools for this through attending annual mandatory IG training, and all staff receiving a Confidentiality Code of Conduct. All new staff are issued the latter during the Trust Corporate induction, and all staff are annually directed to it via the Information Governance Staff Handbook.

It is made clear in both of these documents that failure to maintain confidentiality may lead to disciplinary action, including dismissal.

e) Data Protection & Information Security

The IG Team jointly maintain an Improvement Plan with the IT Team. This includes actions to ensure that patients and the public are adequately informed about confidentiality and the way their information is used and shared, their rights as Data Subjects, in particular how they may access their Personal Data and how they may exercise those rights.

f) Information Risk Management (IRM)

The Trust is committed to making the best use of the information it holds to provide efficient healthcare and services to its patients and the local health economy, while ensuring that adequate safeguards are in place to keep information secure and to protect Data Subjects' right to privacy.

The Trust recognises that information handling represents a significant corporate risk in that failures to protect information properly or use it appropriately can have a damaging impact on its reputation. Furthermore, failure to protect information adequately can attract the attention of the Information Commissioner's Office (ICO), which regulates DP and has access to a range of sanctions including significant fines.

IRM complements the Trust's risk management approach. As part of this, information risks are clearly recognised and the appropriate controls implemented through a Board-approved risk management policy and procedure.

Information risk is intrinsic in all administrative and business activities and all staff must continuously manage it. The Trust recognises that the aim of IRM is not to eliminate risk, but to provide the structural means to manage it, by balancing its treatments with anticipated benefits that maybe derived.

The Trust acknowledges that IRM is an essential element of broader IG and IS arrangements and is an integral part of good management practice; it should not be seen as an additional requirement.

g) Records Management

The Trust is committed to a systematic and planned approach to the management of records within the organisation, from their creation to their ultimate disposal. The Trust ensures it controls the quality and quantity of the information that it generates,

can maintain that information in an effective manner, and can dispose of the information efficiently and securely when it is no longer required.

Medical Records are managed in accordance with the Records Management Code of Practice for Health and Social Care, as set out in the Trust's Records Management Policy and managed by the IG Team. To ensure that the Trust maintains the highest standards in the quality of its Medical Records an annual audit of clinical records is undertaken.

h) Information Governance, Information Security and Cyber Security Incidents

The IG Team must be informed immediately of all IG, IS and Cyber Security incidents. These include, but are not limited to, NHS Digital's classifications:

- Lost in transit
- Lost or stolen hardware
- Lost or stolen paperwork
- Disclosed in error
- Uploaded to website in error
- Non-secure disposal – hardware
- Non-secure disposal – paperwork
- Technical security failing (Inc. hacking)
- Unauthorised access/disclosure

IG incident reporting is undertaken on the Trust's Datix incident reporting application.

On receiving notification of a potential Data Security and Protection Incidents, the IG Team must inform the DPO, SIRO, Caldicott Guardian, a senior Manager within the respective Directorate as soon as practicably possible to seek advice and guidance, as appropriate.

The decision to report externally to the ICO is made in line with NHS Digital's Guide to the notification of Data Security and Protection Incidents, with the ultimate decision being the DPO's with advice of colleagues in the previous paragraph.

Any reports are made by the IG Team, having taken advice from the DPO, SIRO, Caldicott Guardian and / or a senior Manager within the respective Department.

7. Monitoring Compliance and Effectiveness

Explain how you will monitor compliance with, and effectiveness of, the policy, this may include auditing. Give clarity on who is leading with what and how actions will be implemented.

Minimum requirement to be monitored / audited	Process for monitoring / audit	Lead for the monitoring/audit process	Frequency of monitoring / auditing	Lead for reviewing results	Lead for developing / reviewing action plan	Lead for monitoring action plan
Compliance with the Data Security & Protection Toolkit	Reporting to the IG Group	Head of Information Governance & Data Protection Officer	Quarterly	Director of Finance and Resources	Head of Information Governance & Data Protection Officer	IG Group
Annual Information Governance Audit	Reporting to the Audit Committee	Head of Information Governance & Data Protection Officer	Annually	Director of Finance and Resources	Head of Information Governance & Data Protection Officer	IG Group

8. Training needs

All staff must adhere to the IG training requirements set out in the Trust's Mandatory and Statutory Training Policy.

9. Approval and Ratification process

The policy has been approved by the IG Group, Audit Committee and ratified by SMT on behalf of the Board.

10. Dissemination and Implementation

Dissemination of this policy will be via the Clinical and Corporate Policy Group/Work force policies to services and made available to staff via the IG intranet page.

11. Review arrangements

This policy will be reviewed in three years by the author or sooner if there is a local or national requirement then ratified by the Audit Committee.

12. Associated documents

Key IG Policies
The policies / procedures in place to support the IG Framework are:-

Confidentiality Code of Conduct
Records Management Policy
FOI Procedure
Data Protection Policy
Information Rights and Subject Access Request Procedure
Information Handling Policy
Network Security Policy

13. References

General Data Protection Regulation
Data Protection Act (2018)
Access to Health Records Act (1990)
Computer Misuse Act (1990)
Environmental Information Regulations (2004)
Freedom of Information Act (2000)
Health and Social Care Act (2012)
Health and Social Care (Safety and Quality) Act (2015)
Human Rights Act (1998)
Privacy and Electronic Communications Regulations (2003)
A Manual for Caldicott Guardians (2017)
Common Law Duty of Confidentiality
Care Quality Commission, Safe Data, Safe Care (2016)

Department of Health, Confidentiality: NHS Code of Practice (2003)
Informaiton Governance Alliance, Records Management Code of Practice for Health and Social Care (2016)
Department of Health, Information Security Management Code of Practice (2007)
Department of Health, Information: To Share or Not to Share (2013) (Caldicott 2)
Department of Health, Report on the Review of Patient-Identifiable Information (1997) (The Caldicott Report)
National Data Guardian for Helath and Care - Review of Data Security, Consent and Opt-Outs (2016)
NHS Digital, Code of Practice on Confidential Information (2014)

Policy Consultation Responses

Complete this template when receiving comments at various draft stages of the Policy.

Responder (including job titles and organisation)	Version, Comment and Date	Response from Author

Policy Consultation Process

Title of Document	Information Governance Policy and Framework
Author (s)	Narissa Leyland – Head of IG& DPO
New / Revised Document	Revised
Lists of persons involved in developing the policy	Narissa Leyland
List of persons involved in the consultation process	IG Group members Clinical Leads

Appendix: 2 – Authors Guide for writing/Review and Approval of Procedural Documents

	Title of new/reviewed Document	Yes/No/ Unsure	Comments
1.	**TITLE**		
	Is the title clear and unambiguous?	**Yes**	
	Is it clear whether the document is a guideline, policy, protocol or standard?	**Yes**	
2.	**RATIONALE**		
	Are there defined reasons for document development?	**Yes**	
3.	**REVIEW PROCESS**		
	Is the method described in brief?	**Yes**	
	Are individuals involved in the development identified?	**Yes**	
	Has a rational attempt been made to ensure the relevant expertise has been used?	**Yes**	
	Is there evidence of a consultation with stakeholders and users?	**Yes**	
4.	**CONTENT**		
	Is the objective of the document clear?	**Yes**	
	Is the target population clear and unambiguous?	**Yes**	
	Are the intended outcomes described?	**Yes**	
	Are the statements clear and unambiguous?	**Yes**	
5.	**EVIDENCE BASE**		
	Is the type of evidence to support the document identified explicitly?	Yes	
	Are key references cited?	Yes	
	Are the references cited in full?	Yes	
	Are all supporting documents referenced?	Yes	
6.	**APPROVAL**		
	Has the named Director had sight of the document?	Yes	IG Group approved the policy
	Does the document identify which committee/ group will approve it?	Yes	
	If applicable have the joint Human Resources/staff side committee (or equivalent) approved the document?	n/a	
7.	**DISSEMINATION and IMPLEMENTATION**		
	Is there an outline/plan to identify how this will be done?		
	Does the plan include the necessary training/support to ensure compliance?	Yes	
8.	**DOCUMENT CONTROL**		
	Does the document identify where it will be		

	held?		
	Have archiving arrangements for superseded documents being addressed?		
9.	**PROCESS to MONITOR COMPLIANCE and EFFECTIVENESS**		
	Are there measurable standards or KPI's to support the monitoring compliance with and effectiveness of the document?	Yes	
	Is there a plan to review or audit compliance with the document?	Yes	
10.	**REVIEW DATE**		
	Is the review date identified?	Yes	
	Is the frequency identified? Recommend every 2/3 years or sooner if required.	Yes	
	Is this an acceptable time frame?	Yes	
11.	**OVERALLRESPONIBLITY for the DOCUMENT**		
	Is it clear who will be responsible for co-ordinating the dissemination, implementation and review of the document?	Yes	
12.	**FORMAT and CONTENT**		
	Arial font	Yes	
	Font size 12	Yes	
	Trust Logo on front page	Yes	
	Title of policy on front page	Yes	
	Policy control page completed		
	Is this a review of an existing document, if so have all changes/amendments been recorded in the table provided	No	This has been a complete re-write and unsure how this should be documented
	Footer of each page details: name of policy, author and date of publication	Yes	
	Numbered sequentially	Yes	
	Appendices present (where required)		
	Impact assessment carried out	Yes	
	Glossary included as appropriate	Yes	
	Proof read the document	Yes	

Author			
If you are satisfied and want to approve this document please sign and date it			
NAME	Narissa Leyland	**DATE**	16-10-2018
SIGNATURE			
FINAL APPROVAL			