NHS
Leeds
Clinical Commissioning Group

CONFIDENTIALITY AND DATA PROTECTION POLICY

Version:	1.5
Ratified by:	Audit Committee
Date ratified:	21 April 2021
Name & Title of originator/author:	Karen Rowe, Information Governance Manager
Name of responsible committee/individual:	IG/BI/IT Committee
Date issued:	April 2021
Review date:	April 2023
Target audience:	All staff

Executive Summary

This policy aims to clarify the principles that govern the use of personal information and to ensure that practices are understood and adhered to and applies to all employees of NHS Leeds Clinical Commissioning Group (CCG), staff who work for, or on behalf, of the CCG including those on temporary or honorary contracts, secondments, volunteers, pool staff, Governing Body members, students and any staff working on an individual contractor basis or who are employees for an organisation contracted to provide services to the CCG, (referred to as staff / /employees from this point on).

All Staff have a common law duty of confidentiality to patients and a duty to support professional ethical standards of confidentiality. This applies to **all types of information** whether held on paper or electronically and whether passed in written form or orally. All person identifiable information should be accessed, stored and disposed of securely.

This policy aims to ensure that:

- there are nominated persons responsible for data protection
- everyone that handles personal / confidential information:
  a) understand their responsibility for following good data protection practice
  b) is appropriately trained to do so
- anyone who receives or wants to make an enquiry about accessing personal information knows what to do.

The CCG is committed to the delivery of a first class confidential service. This means ensuring that all person identifiable information is processed fairly, lawfully and as transparently as possible so that our patients and staff:

- Understand the reasons for processing personal information
- Give their consent (where applicable) for the disclosure and use of their personal information
- Gain trust in the way we handle information held about them

We may occasionally be required to collect and use certain types of personal information to comply with the requirements of the law. No matter how it is collected, recorded and used, e.g. on a computer or on paper, this personal information must be dealt with appropriately to ensure compliance with the UK General Data Protection Regulation (GDPR) and that Data Protection Act 2018 (DPA18)

The lawful and proper treatment of personal information is extremely important to the success of our business and in order to maintain the confidence of our service users and employees.

Equality Statement

This policy applies to all employees, Governing Body members and members of Leeds Clinical Commissioning Group irrespective of age, race, colour, religion, disability, nationality, ethnic origin, gender, sexual orientation or marital status, domestic circumstances, social and employment status, HIV status, gender reassignment, political affiliation or trade union membership.

A full Equality Impact Assessment is not considered to be necessary as this policy will not have a detrimental impact on a particular group.

Contents

1 Introduction

NHS Leeds Clinical Commissioning Group (CCG) recognises the importance of reliable information, both in terms of the clinical management of individual patients and the efficient management of services and resources. The CCG also recognise the duty of confidentiality owed to patients, families, staff and business partners with regard to all the ways in which they process, store, share and dispose of information.

Confidentiality and data protection legislation and guidance provide a framework for the management of all data from which individuals can be identified. It is essential that all staff and contractors of the CCG are fully aware of their personal responsibilities for information which they may come into contact with.

2 Purpose

The purpose of this policy is to ensure that all staff understand their responsibilities in regard to any information they come into contact with in the course of their work and to provide assurance to the Governing Body that the CCG has in place, the processes, rules and guidelines to ensure such information is dealt with legally, efficiently and effectively.

The CCG will establish, implement and maintain procedures linked to this policy to ensure compliance with the requirements of the UK General Data Protection Regulations and the Data Protection Act 2018 and other associated and related legislation and guidance, contractual responsibilities and to support the assurance standards of the Data Security and Protection Toolkit.

This policy supports the CCG in its role as commissioner of health services and will assist in the safe sharing of information with partner and agencies.

3 Scope

This policy must be followed by all staff who work for, or on behalf, of the CCG including those on temporary or honorary contracts, secondments, volunteers, pool staff, Governing Body members, students and any staff working on an individual contractor basis or who are employees for an organisation contracted to provide services to the CCG. The policy is applicable to all areas of the organisation and adherence should be included in all contracts for outsourced or shared services. There are no exclusions.

This policy covers:

All aspects of information within the organisation, including (but not limited to):

- Patient/Client/Service User information
- Personnel/Staff information
- Organisational and business sensitive information
- Structured and unstructured record systems - paper and electronic
- Photographic images, digital, text or video recordings including CCTV
- All information systems purchased, developed and managed by/or on behalf of, the organisation

- CCG information held on paper, mobile storage devices, computers, laptops, tablets, mobile phones and cameras

The processing of all types of information, including (but not limited to):

- Organisation, adoption or alteration of information
- Retrieval, consultation, storage/retention or use of information
- Disclosure, dissemination or otherwise making available information for clinical, operational or legal reasons
- Alignment, combination/linkage, blocking, erasing or destruction of information

Confidentiality and data protection within an independent contractor's (such as GPs and Dentists) premises is the responsibility of the data controller (owner/partners). However, the CCG is committed to supporting independent contractors in their management of information risk and will provide advice, share best practice and provide assistance where appropriate.

The CCG recognise the changes introduced to information management as a result of the Health and Social Care Act 2012 and Health and Social Care (Safety and Quality) Act 2015 and will work with national bodies and partners to ensure the continuing safe use of information to support services and clinical care.

Failure to adhere to this policy may result in disciplinary action and where necessary referral to the appropriate regulatory bodies including the police and professional bodies.

4 Accountabilities and Responsibilities

There are a number of key information governance roles and bodies that the CCG needs to have in place as part of its Information Governance Framework, these are:

- Governing Body
- Audit Committee
- Data Protection Officer
- Senior Information Risk Owner
- Caldicott Guardian
- Qualified Cyber Professional
- Information Asset Owner
- Heads of Service

The accountability and responsibility are set out in more detail in the Information Governance Strategy Policy and Management Framework which must be read in conjunction with this policy.

5 Definition of Terms

5.1 Personal data

Personal data refers to all items of information in any format from which an individual might be identified or which could be combined with other available

information to identify an individual and is information which has a duty of confidence. This may include (but is not limited to):

- Name
- Date of Birth
- Post code
- Address
- National Insurance Number
- Photographs, digital images etc.
- NHS or Hospital/Practice Number
- Date of Death
- Passport Number
- Online identifiers and location data (such as MAC, IP addresses and mobile device IDs)
- Pseudonymised data

5.2 Special categories of personal data

Categories of information are classified as special categories of personal data and require additional safeguards when sharing or disclosing this information in line with guidance and legislation. This includes (but is not limited to):

- Concerning health, sex life or sexual orientation
- Racial or ethnic origins
- Trade union membership
- Political opinions
- Religious or philosophical beliefs
- Genetic data
- Biometric data

5.3 Direct Patient Care

The CCG adheres to national guidance in relation to using Personal Confidential Data for commissioning purposes and recognises that such data can only flow where a clear legal basis enables this.

5.4 Legal basis for processing identifiable data

A Data Protection Impact Assessment (DPIA) is required in order to demonstrate a legal basis for processing identifiable data. (see 6.11)

If a legal basis has been established in the first instance for processing identifiable data and the data is to be used for another purpose, explicit consent is required.

Explicit consent is described in GDPR as any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, through a statement or clear affirmative action, signifies agreement to the processing of their personal data.

An overview of these considerations is provided within the CCG's Privacy Notice.

5.5 Objections and Opt Out

Where patient identifiable information is being processed for purposes other than direct care, there is an obligation to respect opt outs that have already been presented.

The National Data Opt Out programme was introduced in May 2018, enabling patients to opt out from the use of their data for research or planning purposes.

This programme is explained within the CCG's right to be informed/privacy notice and further information is available from the NHS Digital national data opt out website

5.6 Corporate Information

Corporate information includes:

- Governing Body and meeting papers and minutes
- Tendering and contracting information
- Financial and statistical information
- Project and planning information

Corporate information may be accessible through the Freedom of Information Act 2000 either from the CCG responding to a request for information or through making information accessible via the CCG's Publication Scheme. The information may be exempt from release, where there is a duty of confidence or the data is commercially sensitive. Additionally, other exemptions of the Act could restrict release of certain corporate information.

6 Ensuring Information is Secure and Confidential

6.1 General Principles

- The CCG regards all identifiable personal information relating to patients as confidential and assurance of compliance with the legal and regulatory framework will be provided through the IG strategy and management framework.
- The CCG regard all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise.
- The CCG has a Privacy notice which informs individuals of their rights under Data Protection legislation.
- The CCG will establish and maintain policies and procedures to ensure compliance with the General Data Protection Regulation, Data Protection Act 2018, Human Rights Act 1998, the Common Law Duty of Confidentiality, Privacy and Electronic Communications Regulations, the Freedom of Information Act 2000, and Environmental Information Regulations and other related legislation and guidance.
- Awareness and understanding of all staff, with regard to responsibilities, will be routinely needs assessed and appropriate training and awareness provided in addition to the annual mandatory Data Security Awareness training.
- Risk assessment, in conjunction with overall priority planning of organisational activity will be undertaken to determine appropriate,

effective and affordable confidentiality and data protection controls are in place.
- Where any disclosure of person identifiable data is made there a must be a legal basis for doing so.

6.2 Using and Disclosing Confidential Patient Information for Direct Healthcare

For direct care, the legal basis for disclosing information is identified in the CCG's privacy notice which outlines what information will be shared, the purpose of this, who the data will be shared with, how long data will be retained, the rights of the data subject (including opt-outs) and what security measures are in place to protect confidentiality.

If not for direct care then explicit consent or some other legal basis must be present to enable sharing.

6.3 Using and Disclosing Confidential Staff Information

Processing of personal data where the information sharing is needed for direct communications related to their role, salary payment and pension arrangements, is lawful. Staff should be made aware that disclosures may need to be made for legal reasons, to professional regulatory bodies and in response to certain categories of freedom of information requested where the public interest in disclosure is deemed to override confidentiality considerations.

Using staff information for other purposes must be subject to explicit consent being granted unless another legal basis permits this.

6.4 Using and Disclosing Corporate and Business Information

All staff should consider all information which they come into contact with through the course of their work as confidential and its usage and any disclosure should be in line with agreed duties and for authorised work purposes.

6.5 Information Security

Rules and guidance on information security are set out in:

- The Information Security Policy - sets rules, guidance and good practice on ensuring security of information in the workplace, on areas such as portable devices, email, paper and electronic systems.
- The Records Management and Information Lifecycle Policy – includes sections on transfer, storage and archive of records.

6.6 Sharing Confidential Information Without Consent

It may sometimes be necessary to share confidential information without consent or where the individual has explicitly refused consent. There must be a legal basis for doing so (e.g. to safeguard a child) or a court order must be in place. In deciding on any disclosure, certain considerations and steps need

to be taken, therefore please refer any requests to the Caldicott Guardian / IG lead.

6.7 Confidentiality and Conversations

Where during the course of your work you have conversations relating to confidential matters which may involve discussing (or disclosing information about) individuals such as staff members or patients you must ensure:

- that such discussions take place where they cannot be overheard.
- that you do not give out confidential information over the phone - unless you are certain as to the identity of the caller and they have a legal basis to receive such information (e.g. you may need to speak with another team member on the phone who is based at another location).
- that you do not discuss confidential work matters in public places or at social occasions.
- when leaving a message on an answer phone, ensure that you have consent to do so.

6.8 Records Management

The CCG has a Records Management Policy which should be followed for all aspects of record creation, sharing, storage, retention and destruction of records.

6.9 Information Sharing

The organisation will ensure that information sharing takes place within a structured and documented process and in line with the Information Commissioner's Code of Conduct and in accordance with the Health and Social Care Act 2012 and Health and Social Care (Safety and Quality) Act 2015.

Any local Information Sharing Protocols that the CCG have signed up to need to be followed at all times.

6.10 Information Confidentiality Breaches

All actual, potential or suspected incidents involving breaches of confidentiality or security / cyber-related must be reported on Datix following the CCG Incident Reporting procedure.

All incidents involving patient data breaches are notified, via Datix, to the Caldicott Guardian, Data Protection Officer (DPO), SIRO and the IG team.

The DPO, together with the SIRO will consider whether serious breaches of confidentiality or those involving large numbers of individuals need to be reported to the Information Commissioner's Office. Reportable breaches should be determined and presented within 72 hours of being identified.

What should be reported?
Misuse of personal data and security incidents must be reported so that steps can be taken to rectify the problem and to ensure that the same problem does not occur again. The following list gives some examples of breaches which should be reported:

- Sharing of passwords and/or smartcards.
- Unauthorised access to the computer systems either by staff or a third party.
- Unauthorised access to personal confidential personal information where the member of staff does not have a need to know.
- Disclosure of personal data to a third party where there is no justification and you have concerns that it is not in accordance with the data protection principles and NHS Code of Confidentiality.
- Sending data in a way that breaches confidentiality.
- Leaving confidential information lying around in a public area e.g. photocopier.
- Theft or loss of patient-identifiable information.
- Disposal of confidential information in a way that breaches confidentiality i.e. disposing of patient records and or content in an ordinary waste paper bin
- Processing identifiable information without an appropriate Information Asset and associated data flow being identified and recorded in the organisations register.

6.11 Data Protection Impact Assessment

All new projects, processes and systems (including software and hardware) which are introduced that include person identifiable data, must meet confidentiality and data protection requirements. To enable the organisation to address the privacy concerns and risks a Data Protection Impact Assessment (DPIA) must be completed and approved by the IG team/DPO. A DPIA will assist to:

- Identify privacy risks to individuals
- Protect the CCG's reputation
- Ensure person identifiable data is being processed safely
- Foresee problems and negotiate solutions
- Identify all Information Assets and corresponding data flows.

7 Confidentiality Guidance and Legislation

For personal and confidential Information held by the CCG there will be appropriate measures to ensure confidentiality and security, underpinning the principles of Caldicott, NHS Digital Guidance, ICO and professional Codes of Practice, legislation and common law.

Lawfulness, fairness and transparency	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the individual.
Purpose limitation	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
Data minimisation	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
Accuracy	Personal data shall be accurate and, where necessary, kept up to date.
Storage limitation	Personal data shall be kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the personal data is processed.
Integrity and confidentiality	Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
Accountability	There are appropriate measures in place to demonstrate compliance with the above

It is important to note that the Regulation specifies that:

- organisations are accountable for how they handle personal data and need to develop and maintain adequate policies, procedures, processes and systems to fulfil this role.
- data processors can be held liable for breaches.
- all actual information breaches must be reported to the ICO within 72 hours of becoming known.
- there is a maximum penalty for breach of the Regulation of £17.5 million.
- a DPIA is completed for any project where personal data will be processed or it is otherwise anticipated to have a high privacy risk.

- Privacy notices must transparently explain how personal data is used and the rights of the data subject.
- data subjects have the right to erasure, data portability, review of automated decision making and profiling, to request their personal data are removed when an organisation is retaining them beyond a reasonable or defined time period.
- subject access requests must be completed within a month and provided free of charge (unless a request is “manifestly unfounded or excessive”).
- organisations must keep a record of processing activities.
- appointment of a Data Protection Officer.

7.1 Individual rights

The GDPR provides individuals with key rights to control and influence how data about them is used. These general rights are captured below although it is important to note that they are not absolute (they change depending on the legal basis for processing being used) – advice must be sought from the IG team if staff are unclear what action is required.

The right to be informed	The CCG must provide information about how it uses information about individuals. Staff must be aware of the privacy notice(s) in place to support this.
The right to access	Individuals may ask for access or copies of the information held about them by the CCG. Staff should be aware of the CCG Subject Access Request and Access to Health Records procedure, which supports this.
The right to rectification	Individuals can challenge the accuracy of personal data held about them, and ask for it to be corrected or deleted if there are factual errors or omissions. Staff must consider such corrections.
The right to erasure	Individuals can request their data be deleted and in some (not relating to health or social care purposes) circumstances, the CCG will need to respect this. Staff should seek advice from the IG team if they receive such a request.
The right to restrict processing	Individuals can limit the way the CCG uses personal data if they are concerned about the accuracy of the data or how it is being used. Staff should seek advice from the IG team if they receive such a request.
The right to data portability	Individuals have the right to obtain their personal data from the CCG an accessible and machine-readable format. Staff should seek advice from the IG team if

	they receive such a request.
The right to object	Individuals may object to the processing of their personal data by the CCG. Staff should seek advice from the IG team if they receive such a request.
Rights in relation to automated decision making	Individuals can ask that automated decisions and profiling without any human involvement do not happen. Staff should seek advice from the IG team if they receive such a request.

More information about the rights that GDPR provides individuals can be found at https://ico.org.uk/your-data-matters/

It is important to note the CCG only has one month to review and respond to any of the above requests.

7.2 Data Protection Act 2018

The Data Protection Act 2018 (DPA18) controls how personal information is used by organisations, businesses or the government and is the UK's implementation of the GDPR.

In summary the DPA18:

- Implements GDPR standards across all general data processing.
- Provides clarity on the definitions used in the GDPR in the UK context.
- Ensures that sensitive health, social care and education data can continue to be processed while making sure that confidentiality in health and safeguarding situations is maintained.
- Provides appropriate restrictions to rights to access and delete data to allow certain processing currently undertaken to continue where there is a strong public policy justification, including for national security purposes.
- Sets the age from which parental consent is not needed to process data online at age 13, supported by a new age-appropriate design code enforced by the Information Commissioner.

7.3 Human Rights Act 1998

Article 8 of the Human Rights Act 1998 established a right to respect for private and family life, home and correspondence. This reinforces the duty to protect privacy of individuals and preserve the confidentiality of their health and social care records.

7.4 Common Law Duty of Confidentiality

All Staff have a common law duty of confidentiality to all patient, client or staff information and a duty to support professional ethical standards of confidentiality. This applies to all types of information whether held on paper or electronically and whether passed in written form or orally and must not normally be disclosed without the individual's consent.

There are three circumstances where disclosure of confidential information is lawful:

- where the individual to whom the information relates has consented.
- where disclosure is necessary to safeguard the individual, or others, or is in the public interest.
- where there is a legal duty to do so, for example a court order.

Any decision to disclose without consent must be fully documented and agreed by the Caldicott Guardian.

7.5 Information Commissioner's Office Codes of Practice

The CCG processes data that is covered in the following Codes of Practice published by the Information Commissioner's Office (ICO):

- Data sharing
- Subject access
- Closed Circuit Television
- Privacy Notices
- Employment Practices
- Anonymisation
- Personal Information Online

7.6 NHS Digital Guidance

NHS Digital is responsible for facilitating the management and sharing of data across the NHS to support both operational and other functions such as planning, research and assessments.

7.7 NHS Act 2006

Section 251 of the NHS Act 2006 allows the Common Law Duty of Confidentiality to be set aside by the Secretary of State for Health in specific circumstances where anonymised information is not sufficient and where patient consent is not practicable.

7.8 Computer Misuse Act 1990

This Act makes it illegal to access data or computer programs without authorisation and establishes three offences:

- Access data or programs held on computer without authorisation. For example, to view test results on a patient whose care you are not directly involved in or to obtain or view information about friends and relatives.
- Access data or programs held in a computer without authorisation with the intention of committing further offences, for example fraud or blackmail.
- Modify data or programs held on computer without authorisation.

7.9 Caldicott Principles

Following a review of how data was handled in the NHS, the Caldicott principles were developed. When deciding whether to use the information that will identify an individual the following principles should be followed:

1. **Justify the purpose(s)**
   Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented with continuing uses regularly reviewed, by an appropriate guardian.

2. **Don't use personal confidential data unless it is absolutely necessary**
   Personal Confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

3. **Use the minimum necessary personal confidential data**
   Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

4. **Access to personal confidential data should be on a strict need-to-know basis**
   Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

5. **Everyone with access to personal confidential data should be aware of their responsibilities**
   Action should be taken to ensure that those handling personal confidential data - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.

6. **Understand and comply with the law**
   Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

7. **The duty to share information can be as important as the duty to protect patient confidentiality**
   Health and Social Care professionals should have the confidence to share information in the best interests of their patients within the frameworks set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

The Caldicott Guardian has a strategic and operational role, which involves representing and championing confidentiality and information sharing requirements and issues at senior management level and, where appropriate, at a range of levels within the organisation's overall governance framework. A

detailed description of the Caldicott Function is given in the Information Governance Strategy.

8 Training

8.1 Mandatory Training

The CCG requires that all staff undergo Data Security Awareness training annually. All staff will receive this training in accordance with the IG Training Strategy.
Line managers must actively ensure that all staff undertake and complete the annual mandatory Data Security Awareness training.

8.2 Specialist Training

Additional training may be provided in specialist areas such as records management. The need for additional training should be identified with reference to the IG Training Strategy.

9 Implementation and Dissemination

Following ratification by the Audit Committee this policy will be disseminated to staff via the CCG's staff e-bulletin and extranet and will be available on the CCG Website.

This policy will be reviewed every two years or in line with changes to relevant legislation or national guidance.

10 Monitoring Compliance and Effectiveness

An assessment of compliance with requirements, within the Data Security and Protection Toolkit, will be undertaken each year. This includes confidentiality and data protection incidents that are reported. All associated risks resulting from the implementation of the Policy should be assessed and where necessary recorded on the appropriate risk register.

11 Advice and Guidance

An assessment of compliance with requirements, within the Data Security and Protection Toolkit, will be undertaken each year. This includes confidentiality and data protection incidents that are reported.

12 Associated Documents

This policy should be read in conjunction with:

- Information Governance Policy and Management Framework
- Records Management Policy
- Freedom of Information Act and Environmental Information Regulations Policy
- Information Security Policy
- Network Security Policy
- Mobile Working Policy
- Risk Management Policy
- Incident Reporting Policy
- Business Continuity Plan
- Disciplinary Policy

- Anti-Fraud Policy
- Anti-Bribery Policy
- Whistle Blowing Policy
- Internet and Social Media Policy
- Email Policy
- Acceptable Use Policy
- Password Management Policy
- Data Subject Information Rights Policy
- Data Security and Information Governance Training Strategy

All staff are bound by the codes of conduct produced by any professional regulatory body, by the policies and procedures of the organisation and by the terms of their employment contract.

Appendix A Policy Consultation Process:

Title of document	Confidentiality and Data Protection Policy
Author	Karen Rowe, Information Governance Manager
New / Revised document	Revised
Lists of persons involved in developing the policy List of persons involved in the consultation process:	Karen Rowe Information Governance/ Business Intelligence and IT Committee