Data Protection Policy	
Author (s)	Narissa Leyland, Data Protection Officer, LCH (former) Simon Boycott, Head of Development and Governance
Corporate Lead	Jim Barwick
Document Version	1.1
Document Status	FINAL
Date approved by Quality Committee	5th July 2022
Date issued	5th July 2022
Review date	July 2023

Executive summary

The Leeds GP Confederation is committed to ensuring the privacy of individuals are respected and that all personal data processed is handled appropriately and in accordance with the requirements of the General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA2018) and all other data protection laws collectively known in this policy document as (Data Protection Legislation).

The Confederation has a legal obligation to comply with all appropriate legislation and guidance when processing personal data about patients, employees and other individuals.

Contents

1. Introduction 4
2. Aims and Objectives ..... **Error! Bookmark not defined.**
3. Definitions 5
4. Responsibilities 6
5. GDPR Principles 8
6. Accountability 10
7. Lawful basis for processing 10
8. Consent 12
9. Individuals Rights 12
10. Data Processors and Contracts 13
11. Documentation 13
12. Data Protection by Design and Default 14
13. Data Privacy Impact Assessment (DPIA) 14
13. Data Protection Officer 14
14. Personal Data Breaches 15
15. International Transfers 15
16. Monitoring Compliance and Effectiveness 16
17. Training needs 17
18. Approval and Ratification process 17
19. Dissemination and Implementation 17
20. Review arrangements 17
21. Associated documents 17
22. References 17

1. Introduction

This policy is to set out the Confederations' commitment in how the organisation will comply with current Data Protection Legislation.

The Confederation will, through appropriate management, and strict application of criteria and controls:

- observe fully conditions regarding the fair and lawful collection and use of information;
- meet its legal obligations to specify the purposes for which information is used;
- collect and process appropriate information to the extent that it is needed to fulfil operational needs or to comply with legal requirements;
- ensure the quality of information used;
- apply strict checks to determine the length of time information is held;
- ensure that the rights of people about whom information is held can be fully exercised under the Data Protection Act 2018;
- take appropriate technical and organisational security measures to safeguard personal information;
- ensure that personal information is not transferred abroad without suitable safeguards.

2. Scope

This policy must be followed by all staff who work for or on behalf of the Confederation including those on temporary or honorary contracts, secondments, volunteers, students and any staff working on an individual contractor basis or who are employees for an organisation contracted to provide services.

The policy is applicable to all areas of the organisation and covers all aspects of information 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.
- 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.

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.

3. Definitions

Data Protection Legislation refers to both the General Data Protection Regulations (2018) and the Data Protection Act 2018 where the following definitions apply.

Personal Data means 'any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier'.

Special Category Data consists of personal data relating to:

- ethnic origin,
- physical and mental health (including, for example, details of the reasons for an individual's sick leave),
- sexual preference,
- genetics
- biometrics (where used for ID purposes)
- religion or belief,
- political opinion
- Trade Union membership

Greater protections are required when processing this data.

Processing means obtaining, recording, holding or adding to the information or data or carrying out any operation or set of operations on the information or data.

Data Subject "Data subject" means an individual who is the subject of the personal data.

Data Controller means a person who or organisations which (either alone or jointly or in common with other persons/organisations) determines the purposes for which, and the manner in which, any personal data is processed. In this case, this means the Confederation or nominated individuals acting on behalf of and with the authority of the Confederation.

Data Processor means any person (other than a member of staff) or organisation that processes data on behalf of the Confederation.

4. Responsibilities

Chief Executive

The individual with overall accountability for Information Governance within the Confederation 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, on a day-to- day basis will be delegated to the Head of Development and Governance.

Senior Information Risk Owner (SIRO)

The Confederation has appointed the Chief Executive as the Senior Information Risk Owner (SIRO).

The SIRO is responsible for:

- Taking overall ownership of the Confederation's information risk management approach.
- Acting as champion for information risk on the Board and provide written advice to the Accounting Officer on the content of the Confederation's statement of internal control in regard to information risk.
- Implementing and lead the NHS information governance risk assessment and management processes.
- Advising the Board on the effectiveness of information risk management across the Confederation.

Data Protection Officer

This role is defined under the EU General Data Protection Regulation (GDPR) 2018. The regulation specifies the minimum duties or "tasks" to be performed by the DPO.

- To inform and advise the Confederation, and their employees, of their obligations under the Regulation and other applicable laws and regulations.
- To monitor compliance with the Regulation and other applicable laws and regulations and with the relevant policies of the Confederation data controller, this includes assignment of responsibilities, awareness and training, and relevant audits.
- To advise on the data protection impact assessment (DPIA) and monitor its performance, if requested.
- To liaise with the Information Commissioner's Office as required under the GDPR (Article 39(1) (a-e).
- The DPO will be the contact point for the public as regards the Regulation.

Information Security Manager

The Head of Service in each of the Confederation's services acts as Information Security Manager.

The Information Security Manager is responsible for the day to day operational effectiveness of the Information Security Policy and its associated policies and processes of which the Data Protection Policy is one.

- Lead on the provision of guidance to individuals in the organisation on all matters concerning information security, compliance with policies, setting standards and ensuring best practice.
- Provide a central point of contact for information security.
- Ensure the operational effectiveness of security controls and processes.
- Ensure that staff are aware of their responsibilities and accountability for information security.
- Be accountable to the SIRO and other bodies for Information Security across the Confederation.
- Monitor potential and actual security breaches with appropriate expert security resource.

In carrying out these tasks the Information Security Manager will work closely with the Confederation Head of Governance.

Caldicott Guardian

The Confederation has appointed the Medical Director as the Caldicott Guardian.

The Caldicott Guardian is responsible for ensuring the confidentiality of patient confidential data and ensuring it is shared appropriately and securely.

Managers

Managers within every business area are responsible for implementing and ensuring compliance with data protection procedures. This includes the requirement to take all reasonable steps to ensure compliance by third parties. Managers must always contact the Data Protection Officer if:

- they are unsure of the lawful basis which they are relying on to process personal data;
- they need to rely on consent for processing personal data;
- they need to prepare privacy notices or other transparency information they are unsure about the retention period;
- they are unsure on what basis to transfer personal data outside the European Economic Area (EEA);
- they are engaging in a significant new, or change in, processing activity which is likely to require a Data Protection Impact Assessment;
- they plan to use personal data for purposes other than those for which it was originally collected;
- they plan to carry out activities involving automated processing including profiling or automated decision-making;

- they need help with any contracts or other areas in relation to sharing personal data with third parties (including our contractors);
- they plan to share data with another organisation or person in a way which is new or could affect data subjects' rights.

All Staff

Everyone working for The Leeds GP Confederation or on behalf of The Leeds GP Confederation is responsible for ensuring that they understand and follow this policy and other procedures relating to the processing and use of personal data and support The Leeds GP Confederation in complying with data protection legislation, including undertaking Information Governance training on an annual basis.

5. GDPR Principles

The GDPR sets out the main principles for organisations when processing data. In accordance with Article 5 of the GDPR, the Confederation must ensure that personal data is:

5.1 Lawfulness, Transparency and Fairness

Lawfulness

To process personal data and special category data lawfully, the Confederation must identify a legal basis for each data processing activity.

An annual data mapping exercise is undertaken across the Confederation which identifies all inbound and outbound flows of information and an appropriate condition under Article 6 and Article 9 of the GDPR is identified and documented.

Transparency and Fairness

General information about how we process personal data as a controller (referred to as "fair processing information") will be available on our website through privacy notices and other public-facing material.

5.2 Purpose Limitation

The Confederation has clearly identified and documented the purposes for processing and included details of these purposes in our privacy information which we make available to both patients and our staff. All purposes are reviewed on an annual basis.

5.3 Data Minimisation

The Confederation will only collect personal data required for specified purposes and ensure information we hold is periodically reviewed and removed when it is no longer required.

5.4 Accuracy

The Confederation will take reasonable steps to ensure the accuracy of personal data and will carefully consider any challenges to the accuracy of information. This will be achieved by ensuring:

- appropriate processes are in place to check the accuracy of data;
- any mistakes are clearly identified as a mistake;
- all records will identify any matters of opinion, and where appropriate whose opinion it is and any relevant changes to the underlying facts;
- any challenges to the accuracy of personal data will be carefully considered when complying with an individual's right to rectification;

5.5 Storage limitation

We will ensure that personal data is not kept in an identifiable form for longer than is necessary. Due to our function as a public authority, the Confederation retains some personal data for long periods of time.

Details of all of our retention and disposal periods are set out in our Records Management Policy.

5.6 Appropriate Security

A key principle of the GDPR and Data Protection Act 2018 is that personal data must be processed securely by means of 'appropriate technical and organisational measures' – this is the 'security principle'. This will be achieved by ensuring:

- A Network security policy is in place and implemented across the Confederation.
- Additional policies and controls are in place to enforce them.
- Information security risk shall be adequately managed and risk assessments on IT systems and business processes shall be performed where appropriate.
- The requirements for confidentiality, integrity and availability for the personal data we process are understood.
- Appropriate information security controls are implemented to protect all IT facilities, technologies and services used to access, process and store the Confederation information.
- Encryption and/or pseudonymisation are in place where it is appropriate to do so.
- Access to personal data can be restored in the event of any incidents, such as by establishing an appropriate backup process.
- Regular testing is conducted and reviews of our measures to ensure they remain effective, and act on the results of those tests where they highlight areas for improvement.
- Measures are implemented that adhere to an approved code of conduct or certification mechanism when necessary.
- All relevant information security requirements of the Confederation shall be covered in agreements with any data processors, third-party partners or suppliers, and compliance against these is monitored.

6. Accountability

The Confederation is **responsible** for complying with the GDPR and DPA18 and must be able to **demonstrate** compliance by evidencing the steps taken to comply. This will be achieved by ensuring:

- we take responsibility for complying with the GDPR and DPA 2018, at the highest management level and throughout our organisation;
- we keep evidence of the steps we take to comply with the GDPR and DPA 2018;
- appropriate technical and organisational measures are in place, which will be achieved by;
    - adopting and implementing data protection policies;
    - taking a 'data protection by design and default' approach - putting appropriate data protection measures in place throughout the entire lifecycle of our processing operations;
    - putting written contracts in place with organisations that process personal data on our behalf;
    - maintaining documentation of our processing activities;
    - implementing appropriate security measures;
    - recording and, where necessary, reporting personal data breaches;
    - carrying out Data Protection Impact Assessments (DPIA) for uses of Personal Data that are likely to result in high risk to individuals' interests;
    - appointing a data protection officer;
    - adhering to relevant codes of conduct and signing up to certification schemes (where possible);
    - We review and update our accountability measures at appropriate intervals.

7. Lawful basis for processing

The Confederation must determine the lawful basis for processing before starting any collection of personal data. The lawful basis for processing are set out in Article 6 of the GDPR and at least one of these must apply whenever Personal Data is processed:

(a) Consent: the individual has given clear consent to process their Personal Data for a specific purpose.

(b) Contract: the processing is necessary for a contract with the individual, or because they have asked the Confederation to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for the Confederation's legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply when the Confederation is processing data to perform its official functions).

In order to process **Special Categories Data**, the Confederation must also ensure that one of the following applies:

(a) The data subject has given explicit consent to the processing of those personal data for one or more specified purposes;

(b) Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection;

(c) Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) Processing relates to personal data which are manifestly made public by the data subject;

(e) Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(f) Processing is necessary for reasons of substantial public interest, on the basis of EU or UK law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(g) Necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional;

(h) Necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.

These conditions must be read alongside the Data Protection Act 2018, which adds more specific conditions and safeguards:

- Schedule 1 Part 1 contains specific conditions for the various employment, health and research purposes under Articles 9(2), (b), (g), (i) and (j).

- Schedule 1 Part 2 contains specific 'substantial public interest' conditions for Article 9(2)(h).

The Confederation annually reviews the purposes of our processing activities, and selects and documents the most appropriate lawful basis for each activity to demonstrate compliance. This information is included in our privacy notices for both staff and patients.

8. Consent

Where relying on consent as the legal basis for lawful sharing of personal information, ensure the quality of consent meets new requirements and that:

- consent is active, and does not rely on silence, inactivity or pre-ticked boxes;
- consent to processing is distinguishable, clear, and is not *"bundled"* with other written agreements or declarations;
- data subjects are informed that they have the right to withdraw
- there are simple methods for withdrawing consent, including methods using the same medium used to obtain consent in the first place;
- separate consents are obtained for distinct processing operations; and
- consent is not relied on where there is a clear imbalance between the data subject and the controller (especially if the controller is a public authority).

9. Individuals Rights

The Confederation will respect individuals' rights when processing personal data. These are enshrined in the legislation as follows:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

The rights above depend upon the lawful basis for processing. For example, the right to erasure only applies where the lawful basis for processing is consent. Where public task, legitimate interests, contractual basis or a legal requirement are used as the basis for processing, the right of rectification, restriction and the right to object are also limited to ensuring that the data is accurate before it can be processed.

The right to be informed is, however, a key right and applies in all circumstances (see Transparency and Fairness, section 5.1). The Confederation has an Individuals Rights and Subject Access Request Procedure in place to support.

10. Data Processors and Contracts

Where it uses a data processor, the Confederation is still responsible for data protection and liable for any data transferred.

The Confederation is also liable for the Data Processor's compliance with the legislation and must only appoint processors who can provide sufficient guarantees that the requirements of the legislation will be met and the rights of data subjects protected. It must, therefore, ensure that there is an appropriate written contract with the data processor. The contract is important so that both parties understand their responsibilities and liabilities.

Contracts will set out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subject, and the obligations and rights of the controller and which must, as a minimum set out the following:

- only act on the written instructions of the Confederation;
- ensure that people processing the data are subject to a duty of confidence;
- take appropriate measures to ensure the security of processing;
- only engage sub-processors with the prior consent of the Confederation and under a written contract;
- assist the Confederation in providing subject access and allowing data subjects to exercise their rights under the GDPR;
- assist the Confederation in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- delete or return all personal data to the controller as requested at the end of the contract;
- submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a Member State.

The Confederation will apply the approach set out in the Procurement Policy Note (PPN03/17) Changes to Data Protection Legislation & General Data Protection Regulation, published by Crown Commercial Service.

11. Documentation

The Confederation is required to maintain a record of its processing activities, covering areas such as processing purposes, data sharing and retention.

A Data Mapping review of all data processing activities across the Confederation will be undertaken on an annual basis facilitated by the Quality, Performance and Finance Committee. The review will identify all inbound and outbound flows of personal identifiable information from each department and Business Unit, the purposes of the flow, what type of personal data is involved, who it is shared with, the lawful basis and whether an information sharing agreement has been established.

12. Data Protection by Design and Default

The Confederation will ensure that privacy and data protection issues are considered at the design phase of any new system, service, product or process and that appropriate technical and organisational measures to implement the data protection principles and safeguard individual rights are in place. This will involve but not limited to;

- Only using Data Processors that provide sufficient guarantees of their technical and organisational measures for data protection by design.
- Anticipating risks and privacy-invasive events before they occur, and take steps to prevent harm to individuals.
- Making data protection an essential component of the core functionality of our processing systems and services.

13. Data Privacy Impact Assessment (DPIA)

The GDPR introduces a new obligation to carry out a DPIA before carrying out types of processing likely to result in high risk to individuals' interests.

The Confederation will consider if a full DPIA is necessary if the processing of personal data involves:

- evaluation or scoring (including profiling and predicting)
- automated decision making
- systematic monitoring of data subjects, including in a publicly accessible area
- sensitive data (special categories of data as defined in Article 9 and data regarding criminal offences)
- data being processed on a large scale
- matched or combined datasets
- vulnerable individuals
- transferring data outside the European Union
- innovative technical or organisational solutions
- preventing data subjects from exercising a right or using a service or a contract

As a minimum, a DPIA will include;

- A description of the envisaged processing operations and the purposes of the processing;
- An assessment of :
    (i) the need for and proportionality of the processing and
    (ii) the risks to data subjects (as viewed from the perspective of data subjects) arising; and
- A list of the measures envisaged to mitigate those risks and ensure compliance with the GDPR.

13. Data Protection Officer

The GDPR introduces a duty to appoint a Data Protection Officer (DPO) if you are a public authority or body, or if you carry out certain types of processing activities.

The Confederation's DPO is Simon Boycott, who can be contacted via email simon.boycott@nhs.net or phone: 0113 221 7387

Or at the following address:
The Leeds GP Confederation
Stockdale House
Victoria Road
Leeds
LS6 1PF

14. Personal Data Breaches

It is a legal obligation to notify personal data breaches of the GDPR under Article 33 within 72 hours, to the ICO, unless it is unlikely to result in a risk to the rights and freedoms of individuals. Article 34 also makes it a legal obligation to communicate the breach to those affected without undue delay when it is likely to result in a high risk to individual's rights and freedoms. It is also a contractual requirement of the standard NHS contract to notify incidents in accordance with this guidance. By notification, this may be an initial summary with very little detail known at the outset but a fuller report that might follow. There is no expectation that a full investigation will be carried out within 72 hours.

The Confederations documents all data breaches even if they don't need to be reported to the Information Commissioner.

The *'Guide to the Notification of Data Security and Protection Incidents'* must be followed when a data breach has been detected. The guidance applies to all organisations operating in the health and social care sector. This guidance has been incorporated into the Personal Data Breach Management Procedure, which is aligned to the Incident & Serious Incident Policy.

15. International Transfers

Current data protection laws impose restrictions on the transfer of personal data outside the European Union, to third countries or international organisations. These restrictions are in place to ensure that the level of protection of individuals afforded by the GDPR is not undermined.

16. Monitoring Compliance and Effectiveness

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 Corporate Committee	Head of Governance / Data Protection Officer	Quarterly	Chair of Corporate Committee	Corporate Committee	Corporate Committee
Annual Information Governance Audit	Reporting to the Corporate Committee	Head of Governance / Data Protection Officer	Annually	Chair of Corporate Committee	Corporate Committee	Corporate Committee

17. Training needs

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

18. Approval and Ratification process

The policy has been approved by the Corporate Committee on behalf of the Confederation Executive.

19. Dissemination and Implementation

Dissemination of this policy will be via the Confederation Website.

20. 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 Corporate Committee.

21. Associated documents

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

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

22. References

General Data Protection Regulation 2018
Data Protection Act 2018
Human Rights Act 1998
Privacy and Electronic Communications Regulations 2003

A Manual for Caldicott Guardians (2017)
Department of Health, Confidentiality: NHS Code of Practice (2003)
Department of Health, Information: To Share or Not to Share (2013) (Caldicott 2)
Report on the Review of Patient-Identifiable Information (1997) (The Caldicott Report)
NHS Digital, Code of Practice on Confidential Information (2014)