NHS
Lincolnshire
Integrated Care Board

Data Protection and Confidentiality Policy

ICB document reference:	**ICB IG 002**
Name of originator/author:	NHS AGEM CSU
Date of approval:	March 2024
Name of responsible Committee:	Executive Committee/Audit & Risk Committee
Responsible Director/ICB Officer:	Julie Ellis-Fenwick, Head of Corporate Governance
Category:	Information Governance
EIA undertaken:	
Date issued:	March 2024
Review date:	March 2027
Target audience:	All staff
Distributed via:	Email, Website, Intranet and Board Portal

Document Control Sheet

Document Title	Confidentiality and Data Protection Policy
Version	0.6
Status	Draft
Authors	NHS AGEM CSU
Date	21/02/2024

Document history			
Version	**Date**	**Author**	**Comments**
0.1	06/11/20	NHS AGEM CSU/Optum Health Systems Support IG Services	Updated document based on predecessor Lincolnshire ICB documentation & taking account of the Data Protection Act 2018 and GDPR.
0.2	21/12/20	NHS AGEM CSU/Optum Health Systems Support IG Services	Updated to reflect governance/approval arrangements
0.3	09/02/20	NHS AGEM CSU	Minor changes following feedback from ICB
0.4	05/10/20	NHS AGEM CSU	Minor amendments to terminology and minor re-formatting. Reference added for the requirement to conduct a DPIA to the DPIA policy.
0.5	27/06/2022	NHS AGEM CSU	Policy review and rebrand for the transition of the CCG to an ICB. Updated linked guidance.
0.6	21/02/2024	NHS AGEM CSU	Minor wording changes, relevant guidance updates

1. INTRODUCTION

This Policy applies to NHS Lincolnshire ICB.

The ICB has a legal obligation to comply with all appropriate legislation in respect of data, information and information security. It also has a duty to comply with guidance issued by the Department of Health (DH), the Information Commissioner's Office (ICO), other advisory groups to the NHS and guidance issued by professional bodies.

All legislation relevant to an individual's right of confidence and the ways in which that can be achieved and maintained, are paramount to the ICB. Penalties could be imposed upon the ICB, and/or ICB employees for non-compliance with relevant legislation and NHS guidance.

2. PURPOSE

This policy details how the ICB meets its legal obligations and NHS requirements concerning confidentiality and information security standards. The requirements are primarily based upon the key piece of legislation, the Data Protection Act 2018 which incorporates the General Data Protection Regulations; however, other relevant legislation and appropriate guidance is also relevant.

3. SCOPE

This policy applies to all employees (permanent, seconded, contractors, management and clinical trainees, apprentices, temporary staff and volunteers) of the ICB. Third Parties with whom the ICB may agree information sharing protocols will be governed by the associated information sharing agreements and will be made aware of this policy.

4. DEFINITIONS

Data Controller:
The person or organisation that collects personal data and decides on how to use, store or distribute that data

Data Processor:
Any person or organisation (other than an employee of the data controller) that processes personal data on behalf of the data controller

Data Subject:
Any living individual who is the subject of the personal data

Personal Confidential Data:
Data that relates to a living individual that can identify the individual from this data or other information in the possession of the data controller (for example name address, postcode or NHS Number).

Sensitive Personal Data or Special Category Data:
Data that relates to a living individual that includes racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, physical or mental health condition, sex life, criminal proceedings or convictions

Right of Subject Access:
Data Subjects have the right to access and be given details of any information held about them that:

- consists of information relating to the physical or mental health or condition of an individual and
- has been made by or on behalf of a health professional in connection with the care of that individual

- for ICB staff, this includes the Personnel and Occupational Health record

Where data has been obtained from NHS England via a Data Service for Commissioners Regional Office (DSCRO) advice must be sought from them prior to release to ensure compliance with the terms of any Data Sharing Contract that may be in force.

Under the Data Protection Act 2018, the following are the rights of Data Subjects:

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.

Further information regarding these rights can be found here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

Please note that under the derivations applicable to the UK, the right to erasure (the right to be forgotten) is not applicable to health (NHS) data, and that the normal principles of retention are in place as per the NHS guidance: Records Management Code of Practice - NHS Transformation Directorate (nhsx.nhs.uk)

5. DUTIES AND RESPONSIBILITIES

The ICB has a legal duty to comply with the Data Protection Act 2018. The Accountable Officer is responsible for ensuring that the responsibility for data protection is allocated appropriately within the ICB and that the role is supported.

The ICB is responsible for the implementation of this policy and for ensuring:

- All staff dealing with personal confidential data are aware of the need for compliance with the Act and associated provisions
- All staff are aware of the requirements of the common law duty of confidence as set out in the NHS Code of Practice on Confidentiality 2003
- There is compliance with guidance issued by the Department of Health and by the Information Commissioner
- The processing of personal data is in compliance with the Act
- There is notification to the Information Commissioner of processing of personal data and that this notification is accurate and up to date
- The appointment of a Data Protection Officer, and the allocation of responsibility for Information Risk Management to a senior Director
- There is a scheduled regular review of this policy

Information Asset Owners are responsible for understanding and addressing information governance risks relevant to the “information assets” that they own.

Information Asset Owners in the ICB are responsible for ensuring that this policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance.

All staff must adhere to ICB policies and procedures relating to the processing of personal information.

All staff members are responsible for maintaining compliance with the Data Protection Act principles and for reporting non-compliance through the ICB incident reporting process.

6. PROCESS

6.1. Legislation

The legislation listed below also refers to issues of security and confidentiality of personal data. A more detailed description of the legislation is provided in Appendix 2:

- Access to Health Records Act 1990
- Access to Medical Reports Act 1988
- Data Protection Act 2018
- The UK General Data Protection Regulation
- Computer Misuse Act 1990
- Crime and Disorder Act 1998
- Freedom of Information Act 2000
- Health and Social Care Act 2012
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000

6.2. NHS and related guidance

The following are the main publications referring to security and confidentiality of personal identifiable information:

- Health and Social Care Information Centre: Guide to Confidentiality 2013
- Caldicott Reviews and updates
- Information Commissioner's Office Codes of Practice
- Records Management: NHS Code of Practice 2016

Further guidance on compliance requirements for the ICB can be found in the Data Security and Protection Toolkit Help (dsptoolkit.nhs.uk)

6.3. Overview of the Data Protection Act 2018 that incorporates the General Data Protection Regulations.

The GDPR harmonises data protection legislation across Europe and have been incorporated into UK law in the Data Protection Act 2018.

The Data Protection Act 2018 sets out specific rights of individuals and affirms that organisations must proactively assure themselves as to the use of, transfers of, and legal basis for processing of all the information they hold. Further, where new uses or processes for information are introduced, these must be subject to a Data Protection Impact Assessment, and in certain circumstances, approval must be obtained by the supervisory authority (for this ICB that is the Information Commissioner) before that processing may commence.

This legislation applies to all person identifiable information held in manual files, computer databases, videos and other automated media, about living individuals. The legislation requires that information should only be disclosed on a need to know basis. Printouts and paper records must be treated carefully and disposed of in a secure manner, and staff must not disclose information outside their duties and responsibilities. Any unauthorised disclosure of information by a member of staff may result in disciplinary action.

The Act requires the ICB to register its information held manually and on computers and other automated equipment with the Information Commissioner's Office, identifying the purposes for holding the data, how it is used and to whom it may be disclosed. Failure to register, an incorrect registration or an outdated registration, are criminal offences, which may lead to prosecution of the ICB. ICB notification is maintained and reviewed annually.

Under the Data Protection Act 2018 an individual can request access to their personal information, regardless of the media in which this information may be held / retained. The ICB has a Subject Access Policy for managing these requests.

Appendix 1 provides an overview of NHS and related guidance.

6.4. Data Protection Principles

These are that information must be

a) processed lawfully, fairly and in a transparent manner in relation to individuals

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required in order to safeguard the rights and freedoms of individuals

f) 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.

For each of the above, the Data Controller (the ICB) is responsible for, and must be able to demonstrate, compliance with the principles.

6.5. What is Personal Data

Personal data is information that relates to an identified or identifiable person who could be identified, directly or indirectly based on the information.

Personal data includes an identifier like:

- a name
- an identification number, for example a National Insurance or passport number
- location data, for example a home address or mobile phone GPS data
- an online identifier, for example your IP or email address.

Sensitive personal data is also covered as special categories of personal data. The special categories specifically include:

- genetic data relating to the inherited or acquired genetic characteristics which give unique information about a person's physiology or the health of that natural person
- biometric data for the purpose of uniquely identifying a natural person, including facial images and fingerprints
- data concerning health which reveals information about your health status, including both physical and mental health and the provision of health care services
- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- sex life or sexual orientation.

6.6. Staff Issues

Staff contracts of employment are produced and monitored by the ICB Human Resources function, provided under a Service Level Agreement with AGEM CSU. All contracts of employment include Information Governance clauses, including information governance and data protection responsibilities.

A breach of the Data Protection requirements could result in a member of staff facing disciplinary action. All staff must adhere to ICB policies and procedures relating to the processing of personal information.

6.7. Disclosure of personal confidential data

There are Acts of Parliament that govern the disclosure/sharing of personal identifiable information. Some make it a legal requirement to disclose information whilst others state when information cannot be disclosed. Some examples include:

Legislation to restrict disclosure

- Human Fertilisation and Embryology (Disclosure of Information) Act 1992
- Venereal Diseases Act 1917 and Venereal Diseases Regulations of 1974 and 1992
- Abortion Act 1967
- The Adoption Act 1976

Legislation requiring disclosure

- Public Health (Control of Diseases) Act 1984 & Public Health (Infectious Diseases) Regulations 1985
- Education Act 1944 (for immunizations and vaccinations to NHS ICBs from schools)
- Births and Deaths Act 1984
- Police and Criminal Evidence Act 1984

Whilst there is a public expectation of appropriate sharing of information between organisations providing health care services to them and with other organisations providing related services, the public rightly expect that their personal data will be properly protected. When sharing personal information, ICB staff must ensure that the Principles of the Data Protection Act 2018, the Human Rights Act 1998, the Caldicott Review Principles, and the Common Law Duty of Confidentiality are upheld. Information sharing protocols provide the basis for facilitating the exchange of information between organisation

Please contact the agem.lincs.ig@nhs.net for further advice relating to any form of disclosure of personal information e.g. disclosure to the police, the media etc.

6.8. Keeping patients informed

It is an ICB requirement that patients are advised how their information is to be used before they are asked to provide it, or as soon as is possible (Health and Social Care Information Centre: Guide to Confidentiality 2013). Specific information must be given to patients about the use of their personal information, particularly if for uses other than the provision of healthcare.

.

6.9. Data Protection contractual clauses

The ICB is responsible for obtaining appropriate contractual assurance in respect of

compliance with Information Governance requirements from all bodies that have access to the ICB's information or conduct any form of information processing on its behalf. This is particularly important where the information is about identifiable individuals as this is a legal requirement. The assurance sought from each organisation can be in the form of their self-assessment under the Data Security and Protection Toolkit.

All contractors or support organisations (including non-clinical staff) with access to personal data, that the ICB is data controller for, must be identified and appropriate clauses for inclusion in contracts must be used. In general, the ICBs contracts are based upon the national NHS contract.

6.10. Data Protection Impact Assessments

Data Protection Impact Assessments (DPIAs) are a tool required under the Data Protection Act 2018 to build required compliance for data protection into projects and processes. The ICB has a Data Protection Impact Assessment Policy for understanding how and when to complete a Data Protection Impact Assessment.

DPIAs are intended to build in "privacy by design" and are intended to prevent privacy related problems from arising, by:

- Considering the impact on privacy at the project start
- Identifying ways of minimising any adverse impact
- Building this into projects and processes as they develop

The requirement for Data Protection Impact Assessments to be completed in the ICB will be through the formal Business Case and Project Management Office processes and will be considered where any project or proposal will:

- Introduce a new or additional piece of Information Technology that will relate to the management of Personal Confidential Data (PCD)
- Introduce a new process that requires the use of PCD where it had previously been conducted anonymously
- Involve a change in how the ICB will handle either large amounts of PCD about an individual, or Patient Identifiable Data about a large number of individuals

7. TRAINING REQUIREMENTS

The ICB Director of Finance and Contracting (in the role of Senior Information Risk Owner), and the Head of Corporate Governance (in the role of Deputy Senior Information Risk Owner), have responsibility for maintaining training and awareness of confidentiality and information security issues for all staff. The ICB Director of Nursing and Quality, in the role of Caldicott Guardian is also able to provide advice on the sharing of, and access to, PCD.

Information Governance training is mandatory for all staff and all new starters must undertake IG training, as part of their induction training.

All staff members are required to undertake Data Security Awareness Level 1 training. The agreed method is through the e-learning module available through the Electronic Staff Record.

8. REFERENCES AND ASSOCIATED DOCUMENTATION

The Data Protection Act 2018

https://www.gov.uk/government/collections/data-protection-act-2018

The General Data Protection Regulation:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

The Freedom of Information Act 2000
http://www.opsi.gov.uk/Acts/acts2000/ukpga_20000036_en_1

The Human Rights Act 1998
http://www.opsi.gov.uk/ACTS/acts1998/ukpga_19980042_en_1

Access to Health Records Act 1990
http://www.opsi.gov.uk/acts/acts1990/ukpga_19900023_en_1

Caldicott Reviews

Caldicott review: information governance in the health and care system - GOV.UK (www.gov.uk)

9. MONITORING COMPLIANCE WITH, AND THE EFFECTIVENESS OF, PROCEDURAL DOCUMENTS

Compliance with this policy will be monitored through the ICB's Information Governance Management Framework, through regular reports to the Director of Finance and Contracting in the role of Senior Information Risk Owner, and to Audit and Risk Committee. Relevant requirements include in the report are:

- Compliance with Subject Access Request requirements
- Compliance with the Data Security and Protection Toolkit assertion requirements
- Caldicott Log & Information Governance incident reporting
- Reporting on Data Protection Impact Assessments and Information Sharing Agreements

10 EQUALITY STATEMENT

The ICB aims to design and implement policy documents that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others. This policy takes into account the provisions of the Equality Act 2010 and advances equal opportunities for all. This document has been assessed to ensure that no one receives less favorable treatment on the protected characteristics of their age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex (gender) or sexual orientation. In carrying out its functions, NHS Lincolnshire ICB must have due regard to the different needs of different protected equality groups in their area, while ensuring Human Rights are respected.

This applies to all the activities for which the ICB is responsible, including policy development, review and implementation.

11 APPENDICES

Appendix 1: Overview of legislation

The GDPR

The Data Protection Act 2018 incorporates the General Data Protection Regulations into UK law. The GDPR is a legal framework that sets guidelines for the collection and processing of personal information of individuals within the European Union. GDPR seeks to harmonise data protection legislation across the EU. Further information about the regulations can be found here: https://ico.org.uk/for-organisations/guide-to-the-general-

data- protection-regulation-gdpr/

The Access to Health Records 1990
This Act gives patient's representatives right of access to their manually held health records, in respect of information recorded on or after 1 November 1991. This Act is only applicable for access to deceased persons' records. All other requests for access to information to living individuals are provided under the access provisions of the Data Protection Act 2018.

Access to Medical Reports Act 1988
This Act allows those who have had a medical report produced for the purposes of employment and/or insurance to obtain a copy of the content of the report prior to it being disclosed to any potential employer and/or prospective insurance company.

Human Rights Act 1998
This Act became law on 2 October 2000. It binds public authorities including Health Authorities, ICBs, and individual doctors treating NHS patients to respect and protect an individual's human rights. This includes an individual's right to privacy (under Article 8) and a service user's right to expect confidentiality of their information at all times.

Article 8 of the Act provides that 'everyone has the right to respect for his private and family life, his home and his correspondence'. However, this article also states 'there shall be no interference by a public authority with the exercise of this right except as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention or detection of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others'.

Each organisation must act in a way consistent with these requirements. It must take an individual's rights into account when sharing personal information about them.

Freedom of Information Act 2000
This Act came into force on 1 January 2005. This act gives individuals right of access to corporate information held by the ICB such as policies, reports, minutes of meetings. The ICB has a Freedom of Information Policy and a nominated officer to deal with requests and queries.

Regulation of Investigatory Powers Act 2000
This Act combines rules relating to access to protected electronic information as well as revising the 'Interception of Communications Act 1985'. The Act aims to modernise the legal regulation of interception of communications in the light of the Human Rights laws and rapidly changing technology.

Crime and Disorder Act 1998
This Act introduces measures to reduce crime and disorder, including the introduction of local crime partnerships around local authority boundaries to formulate and implement strategies for reducing crime and disorder in that local area.

The Act allows disclosure of person identifiable information to the Police, Local Authorities, Probation Service, or the Health Service but only if the purposes are defined within the Crime and Disorder Act. The Act does not impose a legal requirement to disclose/exchange person identifiable information and responsibility for disclosure rests with the organisation holding the information. There should be a Crime and Disorder Protocol governing the disclosure/exchange and use of personal information within a local authority boundary agreed and signed by all involved agencies and organisations.

The Computer Misuse Act 1990

This Act makes it a criminal offence to access any part of a computer system, programs and/or data that a user is not entitled to access. Each organisation will issue individual users an individual user ID and password which will only be known by the individual they relate to and must not be divulged / misused by other staff. This is to protect the employee from the likelihood of their inadvertently contravening this Act.

Each organisation will adhere to the requirements of the Computer Misuse Act 1990 by ensuring staff are made aware of their responsibilities regarding the misuse of computers for personal gain or other fraudulent activities. Any member of staff found to have contravened this Act will be considered to have committed a disciplinary offence and be dealt with accordingly.

The Justice and Coroners Act
This Act amended the Data Protection Act to strengthen the Information Commissioner's inspection powers.

Appendix 2: Overview of NHS Guidance

HSCIC: Guide to Confidentiality 2013
This code of practice provides detailed guidance for NHS bodies concerning confidentiality and patient's consent to use their personal confidential information. It details the required practice the NHS must follow concerning security, identifying the main legal responsibilities for an organisation and details employee's responsibilities

Employee Code of Practice
Guidance produced by the Information Commissioner detailing the data protection requirements that relate to staff / employee and other individual's information

The Caldicott Principles
These provide guidance relating to sharing of patient identifiable information and promotes the appointment of a senior health professional to oversee the implementation of the guidance.

Records Management: NHS Code of Practice 2021
Provides guidance to improve the management of NHS records, explains the requirements to select records for permanent preservation, lists suggested minimum requirements for records retention and applies to all information, regardless of the media, applicable to all personnel within the NHS such as patients, employees, volunteers etc. Aids compliance with the Data Protection and Freedom of Information Acts