NHS
Coventry and Warwickshire
Integrated Care Board

Data Protection and Confidentiality Policy

Reference Number:	IG/01
Version:	Version 1.2
Name of responsible Committee and date approved or recommended to Integrated Care Board:	Audit Committee 12 November 2024
Date approved by the Integrated Care Board (if applicable):	N/A
Next Review Date:	12 May 2027
Expiry Date:	12 November 2027
Name of author and title:	Kelly Huckvale, Senior Information Governance Manager, AGEM CSU
Name of reviewer and title:	Laura Whiteley, Governance and Corporate Affairs Manager, ICB
Department:	Governance (Information Governance)

VERSION HISTORY

Date	Version	Changes made to previous version	Consulting and Endorsing Stakeholders, Committees / Meetings / Forums etc.
Sept 2024	V1.2	General review and updates	Audit Committee

Contents

Acronym Glossary

CAG	Confidentiality Advisory Group
CSU	Commissioning Support Unit
CQC	Care Quality Commission
DH	Department of Health
DPA	Data Protection Act
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EEA	European Economic Area
GDPR	General Data Protection Regulations
IAO	Information Asset Owner
ICO	Information Commissioner's Office
IM&T	Information Management and Technology
SI	Serious Incident
SIRO	Senior Information Risk Owner
TNA	Training Needs Assessment

1. Introduction

1.1 Information is a vital asset and needs to be managed securely by NHS organisations, with effective arrangements put in place to ensure the confidentiality, security and quality of personal and other sensitive information and to ensure information is of the highest quality in terms of completeness, accuracy, relevance, accessibility and timeliness.

1.2 In order to operate efficiently, NHS Coventry and Warwickshire Integrated Care Board ("the ICB") collects and uses information about people with whom it works, including patients, public, employees (current, past and prospective), clients and customers, and suppliers. This personal information must be handled and managed appropriately, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means.

1.3 The obligation to keep personal information secure and to respect confidentiality stems from common law, data protection and human rights legislation and applies to all organisations. Staff working for and on behalf of the organisation must also meet these legal requirements and may be bound by professional obligations, employment contracts or other contractual measures. It is essential therefore, that organisations ensure their staff understand what they need to do to keep information safe and secure.

1.4 The Data Protection Act (DPA) 2018 governs how data is collected, stored, processed and shared. The Act requires every data controller who is processing personal information to notify unless they are exempt. Failure to notify is a criminal offence.

1.5 The Health and Social Care (Safety and Quality) Act 2015 and the Caldicott 2 report "Information: To Share or not to Share – The Information Governance Review (April 2013 have placed increased emphasis on the duty to share information between health and social care organisations for the purposes of direct care, by professionals with a legitimate relationship with the patient. ICBs do not have a statutory basis for accessing patient data without consent.

1.6 The six Caldicott Principles were developed in 1997 following a review of how patient information was handled across the NHS, chaired by Dame Fiona Caldicott. The Principles were extended to adult social care records in 2000.

1.7 The Caldicott2 Review Panel made a series of recommendations that were subsequently accepted by the Department of Health (DH) in a report titled "Information: To Share or not to Share - Government Response to the Caldicott Review (September 2013)"

1.8 A 7th Principle was added. Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

1.9 A further Caldicott Review was conducted in July 2016. The report that followed, titled "Review of Data Security, Consent and Opt-Outs", made a series of recommendations in relation to ownership and responsibility for data security, implementation of effective cyber security standards, improved public awareness of information sharing and a new consent / opt-out model to allow people to opt-out of their personal confidential data being used for purposes beyond their direct care.

1.10 An 8th principle was added following a further review in December 2020. "Inform patients and service users about how their confidential information is used."

1.11 The General Data Protection Regulations (GDPR) (Appendix B), adopted by EU Member States on 25th May 2018, include provisions that promote accountability, transparency and governance. While the principles of accountability and transparency have previously been implicit requirements of data protection law, the GDPR's emphasis elevates their significance. Organisations are therefore expected to put into place comprehensive but proportionate governance measures such as data protection impact assessments, privacy by design, a record of processing activities with a view to minimising the risk of breaches, having a validated record of its processing activities and upholding the protection of personal data.

2. Purpose

2.1 The aim of this policy is to ensure compliance with the Data Protection Act (DPA) 2018, the GDPR and Caldicott principles and enable the ICB to safeguard personal, sensitive information.

3. Scope

3.1 This policy applies to all ICB staff which for the purposes of this policy includes, but is not limited to Board Members, contractors, agency and temporary staff, student, honorary and volunteer staff.

3.2 The policy applies to both manual and electronic records.

3.3 This policy is applicable to all areas of the ICB and adherence should be included in all contracts for commissioned or collaboratively commissioned services, without exception.

4. The Data Protection Act 2018

4.1 The DPA 2018 principles under the GDPR are based upon good information handling. These give people specific rights in relation to their personal information and place certain obligations on those organisations that are responsible for processing it (Appendix A contains more detail in this respect).

The principles are:

- Principle (a) – lawfulness, fairness and transparency
- Principle (b) – purpose limitation
- Principle (c) – data minimisation
- Principle (d) – accuracy
- Principle (e) – storage limitation
- Principle (f) – integrity and confidentiality

4.2 Any person or organisation that uses personal information and determines the purpose and means of its processing is known as a **data controller**. The ICB is a data controller in its own right.

4.3 Each organisation is required to register its data holdings with the Information Commissioner annually, identifying the purposes for holding the data, how it is used and to whom it may be disclosed. All applications/databases (identified in the Information Asset Register) must be registered under the ICB's global registration.

4.4 The ICB also uses other organisations to process data on its behalf such as the Commissioning Support Unit (CSU), neighbouring ICBs and local authorities – these are known as **the data processors.**

4.5 The DPA 2018 imposes certain restrictions and obligations on the data controller in relation to that processing. The data controller remains responsible for ensuring its processing complies with the DPA but the data processor does have a shared liability in their own right, and processors as well as controllers may now be liable to pay damages or be subject to fines or other penalties.

4.6 If the data processor is located outside the European Economic Area (EEA), the data controller must ensure that any transfer of personal data to the processor complies with the eighth principle. The ICB maintains a Record of Processing Activities incorporating all information assets and maps all data transfers in accordance with the DPA. More information is provided in the ICB's Information Risk Policy.

5. The General Data Protection Regulations

5.1 The GDPR came into force on 25th May 2018, with the objective of providing individuals with increased control over use of their personal data, in relation to the following principles:

- **Easier access to personal data** by way of a reduction in the response timeframe for all subject access requests and the removal of all associated charges.
- **The right to be forgotten** without the need to seek a court order
- **The right to data portability** between organisations in relation to personal data implementation of "**data protection by design and default**" which mandates the completion of a Data Protection Impact Assessment (DPIA) with regard to all new or

significantly changed process, policies and projects which involve the use of person identifiable information.

- Increased **accountability** for all organisations that process personal data demonstrated by maintaining a Record of Processing Activities which includes the technical and organisational measures taken to secure data and justification for the processing.
- **Consent -** It has been acknowledged that it is not always practical or appropriate for health and social care organisations to seek consent for every instance of processing personal data. As "implied consent" is not recognised under GDPR (but is still relevant in relation to the common law of confidentiality), two clear Articles have been developed which provide health and social care organisations justification to process personal data in the absence of consent. However, in order to exercise these new Articles, the organisation must document their justification for processing in their Record of Processing Activity and Fair Processing Notice.

5.2 Article 5(2) of the GDPR requires that all data controllers shall be responsible for, and able to demonstrate compliance with the above principles and those referenced in Appendix B.

6. Data Subject Access

6.1 The individual who is the subject of personal data is the **Data Subject.**

6.2 The DPA 2018 also gives people a right to request a copy of the information held about them. This is known as a Subject Access Request.

6.3 An individual can request access to information regardless of the media in which it may be held.

6.4 The ICB's Subject Access Request Policy provides the ICB with a process for the management of requests for personal information under the DPA 2018 and GDPR (for living individuals) and under the Access to Health Records Act 1990 (for deceased individuals).

6.5 The ICB will ensure that the general public, staff, including volunteers, locums, temporary employees and patients are aware of why the NHS needs information about them, how this is used and to whom it may be disclosed. The ICB maintains a Fair Processing Notice on the respective websites and statements about data protection will be included on all forms requesting personal identifiable information.

7. Data Protection Legislation – Consent

7.1 Consent is one of several legal bases for processing personal data under Data Protection law. Where explicit consent is the most appropriate legal basis for

processing it should be formally recorded, according to existing processes i.e. Continuing Healthcare, Individual Funding Requests, Complaints etc. Where explicit consent is relied upon it must be:

- Fully informed
- Freely given
- Specific to the circumstances, and
- With positive indication from the data subject.

7.2 In most cases, those consenting must be able to withdraw their consent at any feasible point and must be given information at the time of consenting on how they are able to do so. Exceptions for this are where an individual has consented to a one-off activity that cannot be undone. This does not exempt an individual from requesting exercise of other rights however such as right to request personal data is deleted. Such instances are considered on case-by-case basis.

7.3 ***Common Law Duty of Confidentiality – Consent***

Under the Common Law Duty of Confidentiality, consent differs slightly from the consent described in GDPR:

- Implied consent will normally apply where data is being used and there is a reasonable expectation of the Subject or their representative, that their data would need to be used in that way, to carry out a mutually agreed or understood activity. For example, when a clinician refers a patient to another clinician as part of care of which the patient is already aware, and this is also explained to the patient. The patient does not object and so consent is implied. This type of consent will not usually be applicable to the purposes for which the ICB is processing personal data because it is not involved in direct patient care and there are limited circumstances in which it processes patient data.
- Explicit consent applies where an individual has agreed to the use of data for a specified purpose, after they have been fully informed. Consent under CLDC does not need to meet the requirements for consent set out in the GDPR.

7.4 ***The right to withdraw consent***

- Although not specified as an individual right in the UK GDPR, individuals do have the right to withdraw their consent for their data to be processed for any specified purpose. They can withdraw their consent at any time. Where possible, the ICB will make sure that the individual is able to withdraw their consent using the same method as when they gave it.
- If an individual withdraws their consent, the ICB must stop the processing of their data as soon as possible. Should such a request be received, the relevant service area should be contacted in the first instance. The relevant team should ensure that the ICB Data Protection Officer is made aware of the request, and make sure that the

request is recorded and support the ICB to acknowledge and then consider the request.

- The ICB does not have specific processes for recording consent or requests to withdraw consent as this will vary in each circumstance such a request is made and depending on how the data is held and for what purpose. Each request will be considered and acted upon on a case-by-case basis, with procedures in place within the team holding data to which this right may apply.

8. Data Protection and Confidentiality Work Programme

8.1 The ICB undertakes a Data Protection and Confidentiality Work plan under the auspices of the Caldicott work plan. This is overseen by the Clinical Quality and Governance Committee.

The key elements of the work programme are to:

- Ensure compliance with all aspects of the DPA 2018, GDPR and related provisions and provide reports to the Executive team
- Draft and/or maintain the currency of the Data Protection and Confidentiality policy
- Promote data protection awareness throughout the organisation by organising training and providing written procedures that are widely disseminated and available to all staff
- Co-ordinate the work of other staff with data protection responsibilities
- Work with the commissioning support unit, GPs and others involved in the commissioning process to ensure service users are provided with information on their rights under data protection legislation
- Monitor compliance with the DPA 2018 and associated legislation and the effectiveness of procedures through the use of compliance checks / audits and ensure appropriate action is taken where non-compliance is identified
- Maintain a Record of Processing Activities in accordance with Article 30 of the GDPR
- Assist with investigations into complaints about breaches of the Act.

9. Confidentiality and Caldicott

9.1 The legal framework underpinning disclosure of confidential information includes;

- NHS Codes of Practice on Confidentiality and Information Security Management,
- The Caldicott Principles
- The NHS Care Record Guarantee for England
- The NHS Constitution.

9.2 **Caldicott Principles**

- Justify the purpose(s) for using confidential information

- Do not use personal confidential data unless it is absolutely necessary
- Use the minimum necessary personal confidential data
- Access to personal confidential data should be on a strict need-to-know basis
- Everyone with access to personal confidential data should be aware of their responsibilities
- Understand and comply with the law
- Duty to share information can be as important as the duty to protect patient confidentiality; and
- Inform patients and service users about how their confidential information is used.

9.2.1 The ICB's staff are required to abide by this legal framework.

9.2.2 The ICB as commissioners will ensure providers also implement the Caldicott principles, through normal contracting mechanisms, particularly the newly added principle 7, i.e.

- For the purposes of **direct care**, relevant personal confidential data should be shared among the registered and regulated health and social care professionals (organisations) who have a **legitimate relationship** with the individual
- Sharing is effective and safe
- All contracts must prevent personal information from being used for purposes other than those contracted for and must also ensure that there is explicit consent, or some other lawful basis where required
- All health and care organisations clearly explain to patients and the public how the personal information they collect could be used in de-identified form for research, audit, public health and other purposes and their rights to dissent
- Individuals are asked for explicit consent for their confidential personal information to be shared for non-care purposes (e.g. audit, Care Quality Commission (CQC) reviews, public health surveillance, commissioning, monitoring waiting times). All organisations use the NHS number as a consistent identifier
- Individuals' rights to have full access to their health and care records, without charge (emphasised in National Information Board - Personalised Health and Care 2020: Using Data and Technology to Transform Outcomes for Patients and Citizens); and
- Where personal information is not held in confidence, the duty to share introduced by the Health and Social Care (Safety and Quality) Act 2015 Act will apply

9.3 Caldicott Guardian

9.3.1 The recommendations of the Caldicott Committee (1997 Caldicott Report) defined the confidentiality agenda for NHS organisations. A key recommendation was the appointment in each organisation of a "Guardian" of patient identifiable information to oversee the arrangements for the use and sharing of patient information.

9.3.2 The Guardian should be, in order of priority:

- An existing member of the senior management team
- A senior health or social care professional
- The person with responsibility for promoting clinical governance or equivalent functions.

9.3.3 The Guardian acts as the 'conscience' of an organisation, actively supports work to enable information sharing where it is appropriate to share and advises on options for lawful and ethical processing of information.

9.3.4 NHS and Social Care Caldicott Guardians are required to be registered on the National Register of Caldicott Guardians.

9.3.5 The Caldicott Guardian works with Caldicott Guardians and Senior Information Risk Owners (SIROs) in other organisations, for example, to help manage conflicts of interest.

9.3.6 ICB staff are required to seek advice of the Caldicott Guardian on such issues and in some cases, seek their formal sign off on requests. Such requests are recorded in the Caldicott Log and reviewed by the Audit Committee.

9.4 NHS Care Record Guarantee

9.4.1 The NHS Care Record Guarantee sets out the rules that govern how patient information is used in the NHS and what control the patient can have over this. It covers people's access to their own records; controls on others' access; how access will be monitored and policed; options people have to further limit access; access in an emergency; and what happens when someone cannot make decisions for themselves.

9.4.2 Everyone who works for the NHS, or for organisations delivering services under contract to the NHS, must comply with this guarantee.

9.5 The NHS Constitution

9.5.1 The NHS Constitution sets out a series of patients' rights and NHS pledges.

9.5.2 The relevant rights for this requirement are:

- You have the right to be informed about how your information is used
- You have the right to request that your confidential information is not used beyond your own care and treatment and to have your objections considered, and where your wishes cannot be followed, to be told the reasons including the legal basis.

9.5.3 The relevant pledges for this requirement are that the NHS commits:

- To anonymise the information collected during the course of your treatment and use it to support research and improve care for others
- Where identifiable information has to be used, to give you the chance to object wherever possible
- To inform you of research studies in which you may be eligible to participate.

9.5.4 All NHS bodies and private and third sector providers supplying NHS services are required by law to take account of the constitution in their decisions and actions. Any breaches could have possible disciplinary sanctions or end of contract.

9.5.5 The Information Commissioner's Office (ICO) may order organisations to pay a penalty for serious breaches.

9.6 Common Law Obligations

9.6.1 Common Law requires that there be a lawful basis for the use or disclosure of personal information that is held in confidence.

9.6.2 Unlike the DPA 2018 which applies to legal organisations in their entirety, common law applies to the clinic, team or workgroup caring for an individual, i.e. those not caring for the individual cannot assume they can access confidential information about the individual in a form that identifies them even when they are working in the same organisation.

9.6.3 Normally the basis of access to confidential information will be the consent of the individual concerned and this must be obtained before disclosure or use of the information.

9.6.4 Consent can be implied in some circumstances, but not in others. It is generally accepted that consent can be implied where the purpose is directly concerned with an individual's care or with the quality assurance of that care and the disclosure should not reasonably surprise the person concerned.

10. Using Information for Purposes Unconnected to Care

10.1 The Department of Health's response to the Caldicott 2 Report placed an expectation on all health and care organisations to:

- Clearly explain to patients and the public how the personal information they collect could be used in de-identified form for research, audit, public health and other purposes (Fair Processing Notice)
- Make clear what rights the individual has open to them, including any ability to actively dissent.

10.2 The NHS Constitution includes a commitment to inform people about research and to use anonymised information to support research.

10.3 Where an organisation wishes to disclose confidential personal information for a purpose unrelated to care, consent cannot be implied. In most cases, individuals should be asked for their explicit consent for information to be shared with non-care organisations, for example:

- Housing departments
- Education services
- Voluntary services
- Sure Start teams
- The Police
- Government departments.

10.4 Individuals must also be asked for explicit consent for their confidential personal information to be shared for non-care purposes, such as those in the Table 1 below.

10.5 Where explicit consent cannot be obtained, the organisation may be able to rely on the public interest justification or defence. This is where the organisation believes that the reasons for disclosure are so important that they override the obligation of confidentiality (e.g. to prevent someone from being seriously harmed or for safeguarding).

10.6 Where consent is not appropriate as a legal basis for processing identifiable data, the ICB will consider other legal bases to continue to ensure compliance with Data Protection legislation. This is detailed in the ICB's Fair Processing Notice.

10.7 Disclosure may also be required by Court Order or under an Act of Parliament, i.e. there is a statutory or other legal basis for the disclosure. This includes disclosures permitted under **section 251** of the National Health Service Act 2006. Applications for approval to use Section 251 powers are considered by the Confidentiality Advisory Group (CAG) of the Health Research Authority.

10.8 For any of the above disclosures the advice of the Caldicott Guardian should be sought.

10.9 Information Asset Owners (IAOs) are required to report all activities that involve the use or sharing of confidential personal information that do not have a lawful basis as an IG Serious Incident (IG SI) using the Data Protection and Security Toolkit Incident Reporting Tool.

10.10 Where the ICB contracts with a third party, the contracts must prevent personal information from being used for purposes other than those contracted for and must also ensure that there is explicit consent, or some other lawful basis where required.

10.11 Possible reasons for sharing confidential personal information for non-care purposes:

Table 1
Checking quality of care • Testing the safety and effectiveness of new treatments and comparing the cost-effectiveness and quality of treatments in use. • Supporting Care Quality Commission audit studies. • Comparative performance analysis across clinical networks; and • Ensuring the needs of service users within special groups are being met e.g. children at risk, chronically sick, frail and elderly.
Protecting the health of the general public • Drug surveillance (pharmacovigilance) and other research-based evidence to support the regulatory functions of the Medicines and Healthcare products Regulatory Agency. • Surveillance of disease and exposures to environmental hazards or infections and immediate response to detected threats or events. • Vaccine safety reviews. • Safety monitoring of devices used in healthcare. • Linking with existing National Registries for diseases / conditions; Analysis of outcomes following certain health interventions (i.e. public health interventions as well as treatments). • Monitoring the incidence of ill health and identifying associated risk factors; and Identifying groups of patients most at risk of a condition that could benefit from targeted treatment or other intervention.
Managing care services • Capacity and demand planning. • Commissioning. • Data for Standards and Performance Monitoring. • National Service Frameworks. • Clinical indicators. • Information to support the work of the Care Quality Commission. • Evidence to support the work of the National Institute for Health and Clinical Excellence. • Measuring and monitoring waiting times, in support of the 18-week target. • Data to support Productivity Initiatives. • Agenda for Change; and • Benchmarking.
Supporting research • Assessing the feasibility of specific clinical trials designed to test the safety and/or effectiveness and/or cost-effectiveness of healthcare interventions. • Identification of potential participants in specific clinical trials, to seek their consent. • Providing data from routine care for analysis according to epidemiological principles, to identify trends and unusual patterns indicative of more detailed research; and • Providing specific datasets for defined approved research projects.

11. Information Sharing

11.1 The ICB has signed up to an overall Information Sharing Protocol and has a number of supporting sharing agreements with a wide range of third parties, reviewed regularly by the Information Governance Advisory Group.

11.2 IAOs must review all their transfers of data into and out of the organisation and review the security of these transfers. The Information Asset Register will record mitigations to reduce any risk.

11.3 Any information governance breaches must be reported in line with the ICB's Incident Reporting Policy.

11.4 Decisions on whether to transfer person identifiable information must only be taken by a senior manager and/or IAO.

11.5 Of particular risk are transfers outside the UK. Under GDPR personal data may only be transferred outside of the UK in compliance with the conditions for transfer set out in Chapter 5 of the GDPR. The EU GDPR adequacy decision means that data can continue to flow in the majority of cases from the European Economic Area (EEA).

11.6 Data can still flow freely from the EEA because the EU have adopted adequacy decisions about the UK. Transfers may also be made where the Commissioner has decided that a third country, a territory or one or more specific sectors in the third country, or an international organisation ensures an adequate level of protection.

11.7 Potential risk areas to be taken into account include: -

- What information is being transferred?
- Have the data subjects been informed?
- To what country is the information being transferred?
- What are the purposes of the transfer?
- What data protection laws are in place in the overseas country?
- Is data protection appropriately covered in the contractual arrangements between the organisations?
- Is restriction on further use appropriately covered in the contractual arrangements between the organisations?
- How is the information to be transferred?
- What security measures are in place to protect the information during transfer?
- What security measures are in place in the recipient organisation?

11.8 Information about overseas transfers of information must be included within the ICB's Data Protection notification to the Information Commissioner and must be included in the SIRO report to Board meetings, with associated risk mitigations in place to manage the risk.

11.9 The ICB will obtain an assurance statement from third parties that process the personal data of their service users or staff overseas. This assurance may be within the contract between the two organisations or within other terms of processing.

11.10 All information assets, data flows and the legal basis for sharing information will be recorded within a Record of Processing Activities in accordance with Article 30 of the GDPR.

12. Fair Processing

12.1 The DPA 2018 requires that individuals be informed, in general terms, what information is collected about them, how it is held, how the information may be used, and the organisations or types of organisation it may be disclosed to. This is termed Fair Processing in the Act.

12.2 Fair Processing applies equally to information about staff as it does to information about service users.

12.3 The ICB, where it does not directly provide services to service users and do not have contact with them, must ensure that the respective websites provide clear information on Fair Processing.

12.4 The ICB's Fair Processing Notice must distinguish between personal information and sensitive personal information as different requirements of the DPA 2018 apply to each.

12.5 For the processing of personal information for employment purposes, it is usually sufficient to ensure that staff are aware of the types of information collected, how it will be held/stored and what the employer will use the information for, e.g. HR/personnel purposes, payroll and pensions. This is outlined within the staff Fair Processing Notice.

12.6 For special category data, further steps need to be taken to ensure the processing satisfies one of the conditions in the Act for processing special category data. Such processing may, therefore, require the consent of the employee and it is unlikely that this can be implied.

12.7 The ICB should ensure that new employees are informed (and existing employees reminded) of:

- How the organisation holds, uses and shares their personal information.
- How to inform the employer of changes in their personal details.
- How to raise concerns about what the organisation is doing with data that relates to them; and
- The method of gaining access to the records held about them. More information about this is provided in the ICB's Subject Access Request Policy.

12.8 IAOs should review all existing data collection forms to ensure that any personal information collected is actually required.

13. Roles and Responsibilities

13.1 The ICB's Accountable Officer has the ultimate responsibility for compliance with the DPA 2018 and should ensure that:

- An Executive Lead is appointed for data protection issues.
- A Data Protection Lead/Manager is nominated.
- The role of Caldicott Guardian is assigned and supported.
- Staff are made aware of individual responsibilities through policy and training.

13.2 The Caldicott Guardian is the senior staff member appointed to protect patient information and advise on options for lawful and ethical processing of information.

13.3 The SIRO is responsible for ensuring information risk is managed.

13.4 The Corporate Governance Manager supports the Caldicott Guardian and SIRO to ensure the confidentiality and data protection work programme is implemented and provides regular reports to senior management. They ensure the ICB adheres to the DPA 2018, maintaining notification, developing policies and guidance for staff and providing advice to staff.

13.5 The Data Protection Officer (DPO) is responsible for informing and advising the organisation and its employees of their obligations pursuant to the GDPR and national data protection legislation, and monitoring compliance, reporting to the highest management level of the organisation – i.e. board level. This DPO function is provided by the CSU.

13.6 The CSU's Information Governance team provides support for subject access requests, smartcards and Registration Authority.

13.7 Every staff member is responsible for processing personal data, special category data and corporate data in a confidential manner, for reporting all breaches of confidentiality, both near misses and incidents.

14. Training

14.1 The confidentiality and data protection framework should be supported by adequate skills, knowledge and experience across the whole organisation. The levels of competency should be in line with the duties and responsibilities of particular posts to provide an adequate level of assurance.

14.2 The ICB has carried out a Training Needs Assessment (TNA) and staff are required to undertake relevant training, including mandatory IG training for all.

14.3 Some staff may require higher levels of awareness, specific training or a professional or other recognised qualification to enable them to carry out their duties to the level required by the organisation e.g. the necessary skills, knowledge and experience to develop corporate strategies, policies or procedures to guide staff. The ICB has outlined this in the TNA.

14.4 The TNA is monitored by the DPO, Senior Management Team and the Audit Committees.

15. Monitoring and Assurance

15.1 The Audit Committee will review the Caldicott Log, Incident Breach log and Subject Access Requests log as standing items on the agenda.

15.2 The Audit Committee formally monitors the implementation of the IG Strategy and supporting policies. It reviews the mitigation of information governance and security risks.

15.3 The SIRO will report on information risks and breaches of the DPA 2018 and Caldicott Principles to the Governing Bodies.

15.4 The DPO will report on the management of information assets and compliance with the ICB's obligations in relation to GDPR and the national data protection legislation to the Governing Bodies.

15.5 There is an annual programme of internal and external audits in place which provides validation and assurance of the information governance systems.

15.6 The ICB uses the complaints system to effectively respond to complaints in connection with the DPA 2018 and information governance.

15.7 Training data is regularly reviewed by the Audit Committee.

Appendix A - Equality Impact Assessment

Quality and Equality Impact Assessment
The following assessment screening tool will require judgement against all listed areas of risk in relation to quality. Each proposal will need to be assessed whether it will impact adversely on patients / staff / organisations.

Insert your assessment as positive (P), negative (N) or neutral (N/A) for each area.
Record your reasons for arriving at that conclusion in the comment's column. If the assessment is negative, you must also calculate the score for the impact and likelihood and multiply the two to provide the overall risk score. Insert the total in the appropriate box.
Quality Impact Assessment

Scheme Title:	Data Protection and Confidentiality Policy		
Project Lead:	Laura Whiteley, Governance and Corporate Affairs Manager	**Senior Responsible Officer:**	Andy Wilkins, Director of Corporate Governance
		Quality Sign Off:	n/a – policy does not require quality review
Intended impact of scheme:	This policy outlines how to keep personal information secure and to respect confidentiality stems from common law, data protection and human rights legislation and applies to all organisations. Staff working for and on behalf of the organisation must also meet these legal requirements and may be bound by professional obligations, employment contracts or other contractual measures. It is essential therefore, that organisations ensure their staff understand what they need to do to keep information safe and secure.		
How will it be achieved:	Through the process detailed in this document.		

Name of person completing assessment:	Laura Whiteley
Position:	Governance and Corporate Affairs Manager
Date of Assessment:	28/10/2024

Quality Review by:	Matt Hopkins
Position:	**Governance and Corporate Affairs Officer**
Date of Review:	29/10/2024

High level Quality and Equality Questions

The risk rating is only to be done for the potential negative outcomes. We are looking to assess the likelihood of the negative outcome occurring and the level of negative impact. We are also seeking detail of mitigation actions that may help reduce this likelihood and potential impact.

AREA OF ASSESSMENT		OUTCOME ASSESSMENT (Please tick one)			Evidence/Comments for answers	Risk rating (For negative outcomes)			Mitigating actions
		Positive	Negative	Neutral		Risk impact (I)	Risk likelihood (L)	Risk Score (IxL)	
Duty of Quality Could the scheme impact positively or negatively on any of the following:	Effectiveness – clinical outcome			**N/A**	Effective process ensures the organisation is sighted on and can address issues as a result of complaints and improve the quality of care and patient experience				
	Patient experience			**N/A**	"				
	Patient safety			**N/A**	"				
	Parity of esteem			**N/A**	"				
	Safeguarding children or adults			**N/A**	"				
NHS Outcomes Framework Could the scheme impact positively or negatively on the delivery of the five domains:	Enhancing quality of life			**N/A**	"				
	Ensuring people have a positive experience of care			**N/A**	"				
	Preventing people from dying prematurely			**N/A**	"				
	Helping people recover from episodes of ill health or following injury			**N/A**					
	Treating and caring for people in a safe environment and protecting them from avoidable harm			**N/A**					
Patient services Could the proposal impact positively or negatively on any of the following:	A modern model of integrated care, with key focus on multiple long-term conditions and clinical risk factors			**N/A**					

	Access to the highest quality urgent and emergency care			**N/A**					
	Convenient access for everyone			**N/A**					
	Ensuring that citizens are fully included in all aspects of service design and change			**N/A**					
	Patient Choice			**N/A**					
	Patients are fully empowered in their own care			**N/A**					
	Wider primary care, provided at scale			**N/A**					
Access Could the proposal impact positively or negatively on any of the following:	Patient choice			**N/A**					
	Access			**N/A**					
	Integration			**N/A**					
Compliance with NHS Constitution	Quality of care and environment			**N/A**					
	Nationally approved treatment/drugs			**N/A**					
	Respect, consent and confidentiality			**N/A**					
	Informed choice and involvement			**N/A**					
	Complain and redress			**N/A**					

Equality Impact Assessment

Project / Policy Details

What is the aim of the project / policy?
The aim of this policy is to ensure compliance with the DPA 2018, the GDPR and Caldicott principles and enable the ICB to safeguard personal, sensitive information.

Who will be affected by this work? e.g staff, patients, service users, partner organisations etc.
All staff and data subjects

Is a full Equality Analysis Required for this project?			
Yes	Proceed to complete this form.		Explain why further equality analysis is not required.
If no, explain below why further equality analysis is not required. For example, the decision concerned may not have been made by the ICB or it is very clear that it will not have any impact on patients or staff.			
N/A			

Equality Analysis Form

1. Evidence used
What evidence have you identified and considered? This can include national research, surveys, reports, NICE guidelines, focus groups, pilot activity evaluations, clinical experts or working groups, JSNA or other equality analyses.
The Data Protection Act (DPA) 2018 The General Data Protection Regulations (GDPR) NHS Codes of Practice on Confidentiality and Information Security Management, Access to Health Records Act 1990 The Caldicott Principles The NHS Care Record Guarantee for England The NHS Constitution NHS Care Record Guarantee (1997 Caldicott Report) Health and Social Care (Safety and Quality) Act 2015 Personalised Health and Care 2020

2. Impact and Evidence:
In the following boxes detail the findings and impact identified (positive or negative) within the research detailed above; this should also include any identified health inequalities which exist in relation to this work.
Age: A person belonging to a particular age (e.g., 32 year old's) or a range of ages (e.g., 18-30 year old's)
This policy applies to ICB staff of all ages. There is no evidence or informal intelligence to suggest that differing ages would cause anyone to be disadvantaged more than another in applying this policy

Disability: A person has a disability if he/she has a physical, hearing, visual or mental impairment, which has a substantial and long-term adverse effect on that person's ability to carry out normal day-to-day activities
Describe disability related impact and evidence. This can include attitudinal, physical, communication and social barriers as well as mental health/ learning disabilities, cognitive impairments: This policy applies to all staff and there is no evidence or informal intelligence to suggest that anyone with a disability would be disadvantaged more than someone who did not have a disability.
Gender reassignment (including transgender): Where a person has proposed, started or completed a process to change his or her sex.
Describe any impact and evidence on transgender people. This can include issues such as privacy of data and harassment. N/A
Marriage and civil partnership: A person who is married or in a civil partnership.
Describe any impact and evidence in relation to marriage and civil partnership. This can include working arrangements, part-time working, and caring responsibilities: N/A
Pregnancy and maternity: A person is protected against discrimination on the grounds of pregnancy and maternity. With regard to employment, the person is protected during the period of her pregnancy and any statutory maternity leave to which she is entitled. Also, it is unlawful to discriminate against women breastfeeding in a public place.
Describe any impact and evidence on pregnancy and maternity. This can include working arrangements, part-time working, and caring responsibilities: This policy applies to all and there is no evidence or informal intelligence to suggest any disadvantage in applying this policy.
Race: A group of people defined by their race, colour, and nationality (including citizenship) ethnic or national origins.
This policy applies to all and there is no evidence or informal intelligence to suggest any disadvantage in applying this policy.
Religion or belief: A group of people defined by their religious and philosophical beliefs including lack of belief (e.g., atheism). Generally, a belief should affect an individual's life choices or the way in which they live.
This policy applies to all irrespective of their religion/religious beliefs and there is no evidence or informal intelligence to suggest that people holding differing religious beliefs would be disadvantaged more than another in applying this policy.

Gender:
This policy applies to all and there is no evidence or informal intelligence to suggest any disadvantage in applying this policy.
Sexual orientation: Whether a person feels generally attracted to people of the same gender, people of a different gender, or to more than one gender (whether someone is heterosexual, lesbian, gay or bisexual).
There is no evidence or informal intelligence to suggest that people of differing sexual orientation will be disadvantaged more than another in applying this policy.
Carers: A person who cares, unpaid, for a friend or family member who due to illness, disability, a mental health problem or an addiction cannot cope without their support
This policy applies to ICB staff irrespective of carer responsibilities. There is no evidence or informal intelligence to suggest that people with carer responsibilities would be disadvantaged more than someone who did not.
Other disadvantaged groups:
Describe any impact and evidence on groups experiencing disadvantage and barriers to access and outcomes. This can include lower socio-economic status, resident status (migrants, asylum seekers), homeless, looked after children, single parent households, victims of domestic abuse, victims of drugs / alcohol abuse: (This list is not exhaustive) **N/A**

3. Human Rights

FREDA Principles / Human Rights	Question	Response
Fairness – Fair and equal access to services	How will this respect a person's entitlement to access this service?	N/A
Respect – right to have private and family life respected	How will the person's right to respect for private and family life, confidentiality and consent be upheld?	N/A
Equality – right not to be discriminated against based on your protected characteristics	How will this process ensure that people are not discriminated against	N/A

	and have their needs met and identified?	
Dignity – the right not to be treated in a degrading way	How will you ensure that individuals are not being treated in an inhuman or degrading way?	N/A
Autonomy – right to respect for private & family life; being able to make informed decisions and choices	How will individuals have the opportunity to be involved in discussions and decisions about their own healthcare?	N/A
Right to **Life**	Will or could it affect someone is right to life? How?	N/A
Right to **Liberty**	Will or could someone be deprived of their liberty? How?	N/A

4. Engagement, Involvement and Consultation		
If relevant, please state what engagement activity has been undertaken and the date and with which protected groups:		
Engagement Activity	**Protected Characteristic/ Group/ Community**	**Date**
N/A		
For each engagement activity, please state the key feedback and how this will shape policy / service decisions (E.g., patient told us …. So we will ….):		
N/A		

5. Mitigations and Changes
Please give an outline of what you are going to do, based on the gaps, challenges and opportunities you have identified in the summary of analysis section. This might include action(s) to mitigate against any actual or potential adverse impacts, reduce health inequalities, or promote social value. Identify the **recommendations** and any **changes** to the proposal arising from the equality analysis.
N/A

6. How will you measure how the proposal impacts health inequalities?
e.g. Patients with a learning disability were accessing cancer screening in substantially lower numbers than other patients. By revising the pathway, the ICB is able to show increased take up from this group, this is a positive impact on health inequalities. You can also detail how and when the service will be monitored and what key equality performance indicators or reporting requirements will be included within the contract.
N/A

7. Is further work required to complete this assessment?			
Please state what work is required and to what section. e.g., additional consultation or engagement is required to fully understand the impact on a particular protected group (e.g., disability).			
Work needed	**Section**	**When**	**Date completed**
N/A			

8. Sign off		
The Equality Analysis will need to go through a process of **quality assurance** by a Senior Manager within the department responsible for the service concerned before being submitted to the Policy, Procedure and Strategy Assurance Group for approval. Committee approval of the policy / project can only be sought once approval has been received from the Policy, Procedure and Strategy Assurance Group.		
Requirement	**Name**	**Date**
Senior Manager Signoff	Laura Whiteley	24/10/2024
Which committee will be considering the findings and signing off the EA?	**Audit Committee**	TBC 12/11/2024
Approved by the Policy Procedure and Strategy Assurance Group.	PAG	29/10/2024

Appendix B - Data Protection Act 2018 - principles

(a) principle (requirement that processing be lawful and fair).
(b) principle (requirement that purposes of processing be specified, explicit and legitimate).
(c) principle (requirement that personal data be adequate, relevant and not excessive).
(d) principle (requirement that personal data be accurate and kept up to date).
(e) principle (requirement that personal data be kept for no longer than is necessary).

Data Controller - a person who [either alone or jointly or in common with other persons] determines the purpose for which, and the manner in which any personal data are, or are to be, processed.

A data controller must be a “person” recognised in law, that is to say:

- individuals.
- organisations; and
- other corporate and unincorporated bodies of persons.

Data controllers will usually be organisations but can be individuals e.g. self-employed consultants. Even if an individual is given responsibility for data protection in an organisation, they will be acting on behalf of the organisation, which will be the data controller.

In relation to data controllers, the term jointly is used where two or more persons (usually organisations) act together to decide the purpose and manner of any data processing. The term in common applies where two or more persons share a pool of personal data that they process independently of each other.

Data controllers must ensure that any processing of personal data for which they are responsible complies with the Act. Failure to do so risks enforcement action, even prosecution, and compensation claims from individuals.

Data Subject - an individual who is the subject of personal data. The Act does not count as a data subject an individual who has died or who cannot be identified or distinguished from others.

Data Processor, in relation to personal data, means any person [other than an employee of the data controller] who process the data on behalf of the data controller.

Appendix C - General Data Protection Regulations

Article 5 of the GDPR requires that personal 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 on 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 that is accurate, having regard to the purposes for which it is processed, erased or rectified without delay.

e) Kept in a form which permits identification of the data subject for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored longer periods insofar as the personal data will 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 organisation measures required by the GDPR in order to safeguard the rights and freedoms of the individual; and

f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against loss, destruction or damage, using appropriate technical or organisational measures.

Appendix D - Confidentiality Audit Procedure

1. Introduction

1.1 Organisations should ensure that access to confidential personal information is monitored and audited locally and that confidentiality events are investigated appropriately.

1.2 Failure to ensure that adequate controls to safeguard confidentiality contravenes legislation, including the Data Protection Act 2018, the Human Rights Act 1998 and the Common Law Duty of Confidentiality. The NHS Care Record Guarantee for England sets out high-level commitments for protecting and safeguarding service user information. All NHS bodies and private and third sector providers supplying NHS services are required by law to take account of the NHS Constitution which includes patients' rights in respective of privacy and confidentiality.

1.3 Assurances that these controls are working effectively should be part of the ICB's overall assurance framework.

2. Responsibilities

2.1 The ICB has assigned overall responsibility for monitoring and auditing access to confidential personal information to the SIRO, supported by the Information Asset Owners (IAOs).

2.2 The SIRO should ensure that the confidentiality audit procedure described below is communicated to any staff member with the potential to access confidential personal information.

2.3 The SIRO takes responsibility for the investigation of confidentiality events and will ensure that the investigation and management of these is in line with the ICB's Information Risk Policy and the NHS Digital: Information Security Incident Good Practice Guide.

2.4 Staff should be aware that following investigation, it may be necessary to undertake disciplinary action in line with the ICB's Disciplinary Policy.

2.5 The SIRO will request the CSU as provider of IM&T to the ICB to provide assurances that confidentiality audits are carried out for IT systems.

3. Confidentiality Audit Procedure

3.1 Monitoring will be carried out by the Governance Manager using the templates in Annex 1 and 2, annually or as requested by the Audit Committee.

3.2 Areas to be audited include but are not limited to: -

- Security applied to manual files, e.g. storage in locked cabinets/locked rooms.
- Arrangements for recording access to manual files, e.g. tracking cards, access requests by solicitors, police, data subjects etc.
- Evidence that checks have been carried out to ensure that the person requesting access has a legitimate right to do so.
- Retention and disposal arrangements.
- The location of fax machines and answer phones which receive confidential information in a properly designated “Safe Haven.”
- Confidential information sent or received via e-mail, security applied, and e-mail system used.
- Information removed from the workplace.
- Security arrangements applied, i.e. transportation in secure containers.
- The understanding of staff within a department of their responsibilities with regard to confidentiality and restrictions on access to confidential information.
- Security applied to laptops, compliance with the ICB’s Remote Access Policy.
- Logical access management, providing access to data stored on the Network Use of Smart Cards to access personal information on the “Spine”

3.3 Actual or potential breaches of confidentiality will be reported, following the IG incident reporting process outlined in the Information Risk Policy, in order that action can be taken to prevent further breaches taking place.

3.4 A follow up audit will be undertaken where issues of non-compliance were observed, to confirm that recommendations have been fully implemented. The Audit Committee will formally close off the audit when satisfied.

3.5 The SIRO is responsible for ensuring that the Audit Committee are informed of any concerns highlighted as a result of monitoring access to confidential information.

Annex 1: Audit Checklist

Department:		**Interviewee:**		**Page:**
Process:		**Auditor:**	**Reference:**	**Date:**
Question or Check:	**Document Examined:**	**Finding or Observation:**		**Result:**

Annex 2: Audit Finding Report

<table>
<tr><td>Department:</td><td>Audit Date</td><td>Audit Ref:

Finding Ref:</td></tr>
<tr><td colspan="3">Details of Non-Compliance:</td></tr>
<tr><td>Extent of Non-Compliance:</td><td>Auditors Name:</td><td rowspan="2">Date of Findings:</td></tr>
<tr><td>Business Impact Assessment:

Major/Minor</td><td>Auditors Signature:</td></tr>
<tr><td colspan="3">Recommendations:</td></tr>
<tr><td colspan="3">Reported To/Action By:</td></tr>
<tr><td>Target Date for Completion:</td><td colspan="2">Auditee Signature:</td></tr>
<tr><td>Follow-up Date:</td><td colspan="2">Additional Comments:</td></tr>
<tr><td colspan="3">Follow-up Observations:</td></tr>
<tr><td>Compliance Assessment:</td><td>Auditors Name:</td><td rowspan="2">Date
Re- assessed</td></tr>
<tr><td>Compliant/Major/Minor:</td><td>Auditors Signature:</td></tr>
</table>