


Information Governance Policy, Framework & Strategy

Document Status:

This is a controlled document. Any printed or downloaded copies are not controlled. The version of this document published on the Bedfordshire, Luton & Milton Keynes Integrated Care Board website is the controlled copy
www.befordshirelutonandmiltonkeynes.icb.nhs.uk

Sustainable Development - Environmental

 Do you really need to print this document?

Please consider the environment before you print this document and where possible copies should be printed double-sided. Please also consider setting the page range in the print properties, when relevant to do so, to avoid printing the document in its entirety.

| Document Control | |
|----------------------|--|
| Document Owner: | Senior Information Risk Owner |
| Document Author(s): | Information Governance Team |
| Directorate: | Finance Directorate |
| Approved By: | The Board of the Integrated Care Board |
| Date of Approval: | 01-07-2022 |
| Date of Next Review: | 01-09-2023 |
| Effective Date: | 01-07-2022 |

| Version Control | | | |
|-----------------|------------|-------------|--|
| Version | Date | Reviewer(s) | Revision Description |
| v1.0 | 01-07-2022 | | The Board of the Integrated Care Board adopted the policy as approved. |

Implementation Plan

| | |
|---|--|
| Development and Consultation: | <p>The following individuals were consulted and involved in the development of this document:</p> <ul style="list-style-type: none"> ▪ Information Governance Team ▪ Information Governance Group |
| Dissemination: | <p>Staff can access this document via the website and will be notified of new / revised versions via the staff briefing.</p> <p>This document will be included in the organisation's Publication Scheme in compliance with the Freedom of Information Act 2000.</p> |
| Training: | <p>The following training will be provided to make sure compliance with this document is understood:</p> <p>All new staff are required to attend a compulsory Induction Programme which incorporates Information Governance.</p> <p>In addition to this, all staff are required to annually complete and pass the NHS Digital's Data Security Awareness Level 1 module on the Electronic Staff Record (ESR) e-Learning portal.</p> <p>Please also refer to the Training Needs Analysis (TNA) section of this policy.</p> |
| Monitoring: | <p>Monitoring and compliance of this document will be carried out via:</p> <p>The Information Governance Group with progress reported to the Audit and Risk Assurance Committee.</p> <p>An assessment of compliance with assertions which make up the Data Security and Protection Toolkit, will be undertaken each year and audited by internal auditors.</p> <ul style="list-style-type: none"> ▪ In addition the ICBs Information Governance Department will undertake additional monitoring of compliance with this policy as a response to identification of any gaps or as a result of risks identified by incidents, external reviews or other sources of information and advice |
| Review: | <p>The Document Owner will ensure this document is reviewed in accordance with the review date on page 2.</p> <p>The Information Governance Strategy will be reviewed annually or in response to any significant changes to statutory, requirements, NHS standards or guidance or as a result of significant incidents.</p> <p>A revised work programme will be developed annually, against the Data Security and Protection (DSP) Toolkit 10 Data Security Standards assertions and evidence, identifying key areas for a programme of continuous improvement.</p> |
| Equality, Diversity and Privacy: | <p>Appendix 1 - Equality Impact Assessment</p> <p>Appendix 2 - Data Protection Impact Assessment</p> |

| | |
|------------------------------|---|
| Associated Documents: | <p>The following documents must be read in conjunction with this document:</p> <ul style="list-style-type: none"> ○ Data Protection Policy ○ Information Sharing Policy ○ Subject Access & Access to Health Records Policy ○ Records Management & Lifecycle Policy ○ Social Media Policy ○ Integrated Risk Management Policy ○ Offsite Storage Procedures ○ Controlled Environment for Finance Procedures ○ Information & Cyber Security Incident Procedure ○ Working From Home Guidance ○ Staff IG Handbook |
| References: | <p>The following articles were accessed and used to inform the development of this document:</p> <ul style="list-style-type: none"> ○ Records Management Code of Practice for Health and Social Care (2021) ○ Caldicott Principles ○ A Manual for Caldicott Guardians (2017) ○ Information: To Share or Not to Share (2013) (Caldicott2) ○ Review of Data Security, Consent and Opt-outs (2016) (Caldicott 3) |

Table of Contents

| | | |
|------|--|----|
| 1.0 | Introduction..... | 6 |
| 2.0 | Scope | 6 |
| 3.0 | Definitions..... | 6 |
| 4.0 | Policy Statement..... | 8 |
| 5.0 | Roles and Responsibilities | 10 |
| 6.0 | Processes and Procedures | 16 |
| 6.1 | Data Security and Protection Toolkit | 16 |
| 6.2 | National Data Security Standards..... | 16 |
| 6.3 | Caldicott Principles | 16 |
| 6.4 | Freedom of Information (FOI) Act 2000 | 17 |
| 6.5 | Common Law Duty of Confidentiality..... | 17 |
| 6.6 | Human Rights Act..... | 17 |
| 6.7 | UK General Data Protection Regulations & Data Protection Act 2018 ... | 17 |
| 6.8 | Incident Reporting | 19 |
| 6.9 | Information Asset Management and Business Continuity | 20 |
| 6.10 | Training Needs Analysis (TNA) | 20 |
| 6.11 | Policies, Procedures & Staff Guidance..... | 21 |
| | Appendix 1 - Equality Impact Assessment Initial Screening | 22 |
| | Appendix 2 - Data Protection Impact Assessment Initial Screening | 24 |
| | Appendix 3 - Processes/Flow diagram | 25 |
| | Appendix 4 - Information Governance Reporting | 26 |
| | Appendix 5 - Data Security & Protection Standards | 27 |
| | Appendix 6 - Information Governance Strategy..... | 30 |

1.0 Introduction

- 1.1 NHS Bedfordshire, Luton and Milton Keynes Integrated Care Board (ICB) aims to ensure robust governance through its formal written procedural documents, such as this document, which communicate standard organisational ways of working. These documents help clarify operational requirements and consistency within day-to-day practice. They can improve the quality of work, increase the successful achievement of objectives and support patient safety, quality and experience. The ICB aims to ensure its procedural documents are user friendly, up-to-date and easily accessible.
- 1.2 The ICB must design and implement procedural documents that meet the diverse needs of our service and workforce, ensuring that none is placed at a disadvantage over others, in accordance with the Equality Act 2010. The Equality Impact Assessment initial screening, which was used to determine the potential impact this policy might have with respect to the individual protected characteristics is incorporated at Appendix 1.
- 1.3 A Data Protection Impact Assessment is a process which helps assess privacy risks to individuals in the collection, use and disclosure of personal information. The Data Protection Impact Assessment initial screening, which was used to determine the potential impact this policy might have with respect to an individual's privacy is incorporated at Appendix 2.
- 1.4 The purpose of this policy is to enable all staff to understand their obligations with regard to any information which they come into contact in the course of their work and to provide assurance that such information is dealt with legally, securely, fairly and effectively

2.0 Scope

- 2.1 This policy applies, to all ICB staff members, including Ordinary Members of the Board of the ICB, and Practice Representatives, involved in the ICB's policy-making processes, whether permanent, temporary or contracted-in under a contract for service (either as an individual or through a third party supplier) - here in after referred to as 'staff'.
- 2.2 Failure to adhere to this policy may result in disciplinary action and/or referral to the regulatory body to which a staff member may be registered.
- 2.3 This Policy covers all aspects of information within the ICB, including but not limited to, patient/client/service user information, staff information etc. held in any format e.g., paper, electronic etc.

3.0 Definitions

This section provides staff members with an explanation of terms used within this policy.

3.1 Concept of Confidentiality

- 3.1.1 A duty of confidentiality arises when a person discloses information to another person under conditions where it is realistic to expect that the information provided will be treated in confidence.
- 3.1.2 Disclosure of this information can either be authorised or unauthorised where only limited staff members have the authority to disclose information.
- 3.1.3 A breach of confidentiality is the unauthorised disclosure of information provided in confidence.

3.2 Confidential Information

- 3.2.1 Confidential information can be anything that relates to patients, staff or any other commercially sensitive information (such as contracts and tenders) held in any form (such as paper, electronic, microfilm, audio or video) howsoever stored (such as patient records, paper diaries, computer or on mobile devices such as laptops, tablets, smartphones, BlackBerrys) or even passed by word of mouth.

3.3 Data Controller

- 3.3.1 A data controller means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

3.4 Data Processor

- 3.4.1 A data processor, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

3.5 Personal Data

- 3.5.1 This means data which relate to a living individual who can be identified from those data and includes any expression of opinion about the individual. Typical examples of this type of data could include;
 - Person's name, address, full postcode, date of birth.
 - Email address and telephone numbers.
 - Pictures, photographs, videos, audio-tapes or other images of patients.
 - NHS number or local unique identifiers, these are considered identifiable if the organisation holds the means to re-identify the person from this unique identifier.
 - Any other data, or linked data, that may be used to identify a patient directly or indirectly. For example, rare diseases, drug treatments or statistical analyses which have very small numbers within a small population may allow individuals to be identified.

3.6 Special Category Data

3.6.1 Data held about an individual which contains both personal and sensitive information. Under the UKGDPR the following types of information are deemed as special category:

- Race,
- Ethnic origin,
- Religious or other beliefs,
- Political opinions,
- Trade union membership,
- Genetics,
- Biometrics (where used for ID purposes),
- Physical or mental health,
- Sexual life, and
- Criminal proceedings or convictions.

3.7 Processing

3.7.1 Processing means obtaining, recording, holding the information or data or carrying out an operation on the information or data. An operation could include organising, adapting or altering the data. It also includes retrieving, consulting, linking to other data sources or using the information or data.

3.7.2 Disclosing the information or data by transmission or dissemination indicates processing as does alignment, combination, blocking, erasure and destruction. Viewing data on a computer screen is considered to be processing under the Data Protection Act 2018 and the UKGDPR.

4.0 Policy Statement

4.1 There are a number of legal obligations placed upon the ICB for the processing of personal identifiable information which it MUST comply with. The key ones are:

- Data Protection Act 2018
- UK General Data Protection Regulations (UKGDPR)
- Access to Health Records (Deceased) Act 1990
- Common Law Duty of Confidentiality
- Human Rights Act 1998
- Computer Misuse Act 1990
- Health and Social Care Act 2012
- Health and Social Care (Safety and Quality) Act 2015
- Privacy and Electronic Communications Regulations

4.2 UKGDPR is the key legislation and sets out clear obligations for the ICB and rights for data subjects. The key obligations are listed below and in section 6 of this policy.

Rights of the data subjects are also detailed in section 6.

- **Payment of a Fee to the ICO**

The ICB must pay a fee to the ICO, on an annual basis, and will have their details published by the ICO in a Data Protection Register.

The ICOs Data Protection Register can be viewed here <https://ico.org.uk/about-the-ico/what-we-do/register-of-fee-payers/>

- **Appointment of a Data Protection Officer (DPO)**

The ICB must appoint a suitably trained DPO and has direct access to the Executive Team, act as the first point of contact for the ICO and have their contact details made available to data subjects.

The ICB DPO is lyndaharris2@nhs.net

- **Reporting Breaches to the ICO**

The ICB must report certain personal data breaches to the ICO within 72 hours of becoming aware of the breach, where feasible.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms (see Rights of the Data Subject in section 6), the ICB must also inform those individuals without undue delay.

For breach reporting procedures please see section 6.

- **Monetary Penalty Notice (for serious non-compliance)**

The Criminal Justice and Immigration Act 2008 extends the powers of the Information Commissioner under DPA18 to allow fines of up to £500,000 for individuals or organisations found guilty of deliberate or reckless disclosure of information, including failure to take appropriate security precautions.

In addition, individuals can receive a prison sentence on conviction of an offence under DPA and fines for organisations from the ICO under UKGDPR can be up to £17.5 million.

- **Accountability**

Accountability is one of the key UK GDPR data protection principles. It requires the ICB to put appropriate technical and organisational measures in place to meet the requirements of UK GDPR and be able to demonstrate compliance.

The ICB has a number of measures in place including, but not limited to:

- IG, IT Security and Cyber Security policies, including policies for the effective and secure management of its information assets and resources

- IG & data protection procedures and staff guidance – see IG section on the ICBs Staff Intranet.
- A privacy by design and default approach – see Data Protection Policy.
- Written contracts in place with organisations that process personal data on the ICBs behalf.
- A record of the ICBs processing activities, including the legal basis for each activity.
- Recording, investigating, learning from and where necessary, reporting personal data breaches.
- An appropriately trained and supported DPO as detailed above.
- Mandatory Data Security & Protection staff training – see section 6.
- Fair Processing Notices – see Data Protection Policy.
- Regular assessments and audits of the ICBs information and IT security arrangements as part of the annual review and submission of the DSPT
- Promoting effective cyber and information security practice to staff through policies, procedures, training and communication of alerts.
- Records Management and Information Lifecycle Policy and guidance covering all aspects of records management, consistent with the Records Management Code of Practice for Health and Social Care 2016 – see Record Management and Information Lifecycle Policy and Guidance.
- Promote data quality through policies.

4.3 There are also a number of NHS standards which the ICB should comply with, including, but not limited to:

- Records Management Code of Practice for Health and Social Care (2021)
- Caldicott Principles
- A Manual for Caldicott Guardians (2017)
- Information: To Share or Not to Share (2013) (Caldicott2)
- Review of Data Security, Consent and Opt-Outs (2016) (Caldicott 3)

4.4 The ICB will perform an annual assessment of its compliance against the assertions which make up the Data Security and Protection Toolkit and have the evidence provided for the assessment further assessed by its internal auditors.

4.5 The ICB will conduct periodic reviews and audits to ensure the way it manages its records is in line with statutory obligations and NHS standards.

5.0 Roles and Responsibilities

The following have specific responsibilities in relation to this policy.

5.1 The Board of the Integrated Care Board

- 5.1.1 The Board is accountable for ensuring that the necessary support and resources are available for the effective implementation of this policy. It has responsibility for the IG Agenda supported by identified senior roles which they are required to appoint including the Caldicott Guardian, Senior information Risk Owner and Data Protection Officer.

5.2 **Audit and Risk Assurance Committee**

- 5.2.1 The Audit and Risk Assurance Committee will receive regular IG Reports via the IG Group. The Senior Information Risk Owner is a member of the Audit and Risk Assurance Committee.

5.3 **Information Governance (IG) Group**

- 5.3.1 The Chair of the IG Group is the Senior Information Risk Owner. Other members of the group include the Head of Digital (when required) and the Head of IG/Data Protection Officer. The Group will coordinate, supervise and direct the work of others as appropriate to ensure the ICB maintain a co-ordinated approach to IG.
- 5.3.2 The IG Group is accountable to and will provide regular reports to the Audit and Risk Assurance Committee.
- 5.3.3 The Group will also sign off final submission of the Data Security & Protection Toolkit (see section 6 below) with advice from the Head of IG & Data Protection Officer (see section 5.6 below).

5.4 **Senior Information Risk Owner (SIRO)**

- 5.4.1 The SIRO has overall responsibility for the implementation of risk management across the ICB, for ongoing management of information risks and is the owner of the ICB's Information Asset Registers and Information Risk Registers.
- 5.4.2 The SIRO is a member of the Board and provides advice to the Chief Executive Officer on the content of the Annual Governance Statement and the Statement of Internal Control in regard to information risk.
- 5.4.3 The SIRO is supported by Information Asset Owners, the ICB's Caldicott Guardian, the Head of IT and the Head of IG/Data Protection Officer.
- 5.4.4 Key responsibilities:
- Own the ICB's overall information risk assessment process and for ensuring information asset risk reviews are completed.
 - For ensuring that all information risks are recorded, controls have been identified and mitigated where applicable including, but not limited to, ensuring that all records management issues (including electronic media) are managed in accordance with this Framework.
 - To oversee the development of an information governance strategy

- To take ownership of the risk assessment process for information risk, including review of the annual information risk assessment to support and inform the Statement of Internal Control.
- To ensure that the ICB's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff.
- To provide a focal point for the resolution and/or discussion of information risk issues.
- To ensure the Board is adequately briefed on information risk issues.
- To advise the Chief Executive Officer and the Board on information risk management strategies and provide periodic reports and briefings on progress.

5.5 **Caldicott Guardian**

5.5.1 The Caldicott Guardian has an advisory role with particular focus on ensuring patient identifiable information is shared in an appropriate and secure manner. They are known to be the conscience of the organisation, as they will look at a situation from the perspective of a patient/service user. They are supported in their role by the IG Team.

5.5.2 Key responsibilities:

- Strategy and Governance - champions' confidentiality issues at Board/executive management team level and sits on the ICBs IG Group.
- Confidentiality and Data Protection expertise - develops a strong knowledge of confidentiality and data protection matters, drawing upon support from internal and external sources of advice and guidance where available and applicable.
- Internal information processing - ensures that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff.
- Information sharing - oversees arrangements, protocols and procedures where confidential personal information is shared with external bodies including social care and safeguarding. This includes flows of information to and from partner agencies, sharing through IT systems, disclosure for research and disclosure to the police and other enforcement authorities.
- Subjects Rights – provide approval for the release of information requested under the data subject's right of access (known as subject access requests (SAR) and the Access to Health Records (deceased) Act.

5.6 **Head of IG & Data Protection Officer (DPO)**

5.6.1 The Head of IG & DPO plans and implements the ICBs approach to data protection and works closely with and supports the CG and SIRO in their roles. They are responsible for providing support and guidance to ICB staff to ensure processing of personal identifiable information is undertaken in line with legal

obligations and good practice as detailed in the Data Security & Protection Toolkit.

5.6.2 The DPO is responsible for monitoring compliance with data protection law and ensuring data practices comply with applicable legislation and guidance. The DPO is the primary contact for data subjects (individuals whose data is processed by the ICB) and the Information Commissioners Office (ICO – the body which enforces Information Rights laws and regulations), with whom they are registered.

5.6.3 The DPO reports to the SIRO on relevant matters and escalates any serious concerns or issues to the Board.

5.6.4 The DPO is a legally required role as part of the UKGDPR accountability principle, which is one of the key principles for data protection. Their job description must be compliant with UKGDPR requirements and they must have:

- Direct access to the highest management level of the organisation – this does not necessarily imply line management at this level, but direct and unimpeded access to the senior management team.
- Adequate resources: financial and human resources, and is supported in maintaining his or her expertise.
- Proven 'expert knowledge of data protection law and practices', the ability to perform the tasks specified in the UKGDPR, and sufficient understanding of the organisation's business and processing.
- Timely involvement in all data protection issues.
- Involvement in incident management.
- Have their contact details published in transparency information for subjects and communicated to the ICO through the DPO registration process.

5.6.5 In addition, the DPO must not receive any instruction regarding the exercise of his or her tasks, and is protected from disciplinary action, dismissal or other penalties and where they perform another role or roles, that there is no conflict of interest.

5.7 Information Asset Owners (IAOs)

5.7.1 IAOs are directly accountable to the SIRO and must provide assurance that information risk is being managed effectively in respect of the information assets that they are owners of.

5.7.2 IAOs also lead and help foster, within their respective Directorates, a culture that values, protects and uses information.

5.7.3 IAOs are staff senior enough to. IAOs are generally at director level (so senior enough to make decisions concerning their assets), although they can delegate this role to a responsible deputy.

- 5.7.4 Their role is also to understand and assess risks to their information asset and to provide assurance to the SIRO on the security and use of those assets. They ensure that all threats, vulnerabilities and impacts are properly assessed and included in their Information Asset Register (IAR).
- 5.7.5 IAOs can assign day to day responsibility for each information asset to an administrator or manager known as an Information Asset Administrator (see section 5.8 below).
- 5.7.6 The SIRO is responsible for the appointment and management (in terms of information assets) of the IAOs. IAOs are expected to understand the overall business goals of the organisation and how the information assets they own contribute to and affect these goals.
- 5.7.7 IAO's will take appropriate actions to:
- Know what information the asset holds and understands the nature and justification of any information flows to and from the asset.
 - Know who has access to their assets and why, and ensure their use is monitored and compliant with policy.
 - Ensure the confidentiality, integrity, and availability of all information that their system creates, receives, maintains, or transmits and protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
 - Conduct Data Protection Impact Assessments in line with the ICB's Data Protection Policy.
 - Participate in the ICBs IAR review process by ensuring their IARs are kept up to date and are accurate.
 - Appoint Information Asset Administrators, where appropriate.
 - Understand and address risks to the asset and provide assurance to the SIRO.

5.8 Information Asset Administrators (IAAs)

- 5.8.1 IAOs are responsible for appointing Information Asset Administrators (IAAs). It is at the IAOs discretion how many IAAs are appointed to support them in their role.
- 5.8.2 IAAs are operational staff with day to day responsibility for managing risks to their information assets.
- 5.8.3 Responsibilities of the IAA:
- Providing support to their IAOs to ensure that policies and procedures are followed and to recognise potential or actual security incidents.
 - Consulting their IAOs on incident management to ensure that information asset registers are accurate and maintained up to date.
 - Ensuring compliance with relevant Information Sharing Agreements (ISAs) and that information handling procedures are fit for purpose and are properly applied.

- Under the direction of their IAO, they will ensure that personal information is not unlawfully processed, and they will, upon recognising new information handling requirements (e.g. a new type of information arises) that the relevant IAO is consulted over appropriate procedures.
- They will consult with the IAOs regarding any potential or actual security incidents.
- Reporting to the relevant IAO on current state of local information handling and ensure that local information handling constraints (e.g. limits on who can have access to the assets) are applied, referring any difficulties to the relevant IAO.
- They will act as first port of call for local managers and staff seeking advice on the handling of information.
- Under the direction of their IAO, they will ensure that information is securely destroyed when there is no further requirement for it.

5.9 Heads of Departments/Services

5.9.1 All Head of Departments/Services within the ICB are responsible for ensuring that their staff are aware of and comply with the ICBs IG policies and supporting standards and guidelines and for ensuring they are built into departmental processes and procedures.

5.10 All Staff

5.10.1 IG compliance is a legal and contractual obligation for all staff.

5.10.2 Staff should note that there is confidentiality clauses in their contract and that they are required to participate in induction, annual mandatory training and comply with the ICBs IG policies and supporting guidelines.

5.10.3 Any breach of confidentiality, inappropriate use of information or abuse of computer systems is a disciplinary offence, which may result in dismissal or termination of contract.

5.10.4 All employees are personally responsible for compliance with the law in relation to the UK General Data Protection Regulation, Data Protection Act 2018 and the Common Law Duty of Confidentiality.

5.11 Contracted Third Parties

5.11.1 It is not unusual to have third parties gaining access to the ICB's information assets and for them to process personal identifiable information on behalf of the ICB. These third parties have appropriate information governance clauses included in their contracts and where appropriate, the contract is underpinned with a Data Processing Agreement.

5.11.2 Third parties are required to demonstrate their compliance with IG by annually completing and submitting a DSPT and registering with the ICO.

5.11.3 A register of all contracts is maintained by the ICBs Contracts Department.

6.0 Processes and Procedures

6.1 Data Security and Protection Toolkit

- 6.1.1 The ICB is mandated to use the Data Security & Protection Toolkit (DSPT) to measure its compliance with IG. The ICB is required to submit a DSPT assessment each year following internal audit review of the evidence provided.
- 6.1.2 The ICB's performance against the assertions which make up the DSPT are reported to the Department of Health and forms a part of the assurance processes associated with the Care Quality Commission; NHS England and NHS Improvement (NHSE & NHSI) and the NHS Resolution risk management standards.
- 6.1.3 The outcome of the ICB's annual Data Security and Protection Toolkit Assessment is reported to the IG Group and the Audit and Risk Assurance Committee.
- 6.1.4 HBLICT as the ICBs IT provider is responsible for ensuring the ICBs Head of IG/DPO is provided with the information and documentation necessary for the ICB to be able to evidence compliance with IT Security & Cyber Security assertions.

6.2 National Data Security Standards

- 6.2.1 The DSPT has been developed in accordance with the National Data Security Standards following a review of data security, consent and opt outs by the National Data Guardian (NDG). The NDG recommended that Data Security Standards be applied in the health and social care system in England. These are listed in appendix 4.

6.3 Caldicott Principles

- 6.3.1 The Caldicott Committee Report on the Review of Patient-Identifiable Information 1997 found that compliance with confidentiality and security arrangements was patchy across the NHS and identified six good practice principles for the health service when handling patient information. These principles can be extended to also apply to social care service user information.
- 6.3.2 A further Caldicott2 review was published in March 2013 which amended the Caldicott Principles, as follows:
- Justify the purpose(s)
 - Don't 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
- The duty to share information can be as important as the duty to protect patient confidentiality.

6.3.3 Further details about the revised Caldicott Principles and how to apply them can be found in the Data Protection Policy.

6.4 Freedom of Information (FOI) Act 2000

6.4.1 Information about the organisation will be available to the public in line with the Freedom of Information Act, Environmental Information Regulations and Protection of Freedoms Act unless an exemption applies. The ICB maintains a Publication Scheme in line with legislation and guidance from the Information Commissioner – see Freedom of Information Policy.

6.4.2 There are a number of legal obligations placed upon the ICB for the processing of personal identifiable information, the key ones are:

6.5 Common Law Duty of Confidentiality

6.5.1 Common law duty of confidentiality is not a written law, it is common law based on legal precedent from historical legal cases.

6.5.2 The common law duty of confidentiality means that information confided by a patient/service user or otherwise obtained (e.g. during medical examination or when receiving personal care), where it is expected that a duty of confidence applies, should not generally be used or disclosed further, except as originally understood by the confider or with their subsequent permission.

6.5.3 This duty of confidentiality may be set aside and confidential information disclosed where it is in the public interest or when it is a legal requirement to do so – see Information Sharing Policy

6.6 Human Rights Act

6.6.1 Article 8 of the Human Rights Act establishes the right to respect for an individual's private and family life. Compliance with the Data Protection Act 2018 and the common law duty of confidentiality will satisfy this right.

6.7 UK General Data Protection Regulations & Data Protection Act 2018

6.7.1 The Data Protection Act 2018 (DPA18) sets out the framework for data protection law in the UK. It updates and replaces the Data Protection Act 1998 and came into effect on 25 May 2018. It was amended on 01 January 2021 by regulations

under the European Union (Withdrawal) Act 2018, to reflect the UK's status outside the EU.

- 6.7.2 DPA18 sits alongside and supplements the UK General Data Protection Regulations (UK GDPR) by providing exemptions and sets the Information Commissioner's functions and powers.
- 6.7.3 The Information Commissioners Office is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. They regulate data protection compliance in the UK promote good practice, monitor breach reports, conduct audits and advisory visits, consider complaints, monitor compliance and take enforcement action where appropriate.
- 6.7.4 The UK General Data Protection Regulation (UK GDPR) is a UK law which came into effect on 01 January 2021. It sets out the key principles, rights and obligations for most processing of personal data in the UK, except for law enforcement and intelligence agencies.
- 6.7.5 It is based on the EU GDPR (General Data Protection Regulation (EU) 2016/679 which applied in the UK until 31st December 2020, with some changes to make it work more effectively in a UK context.
- 6.7.6 Data protection laws take a flexible, risk-based approach, which puts the onus on the ICB to think about and justify how and why it uses personal data. It applies to all person identifiable information about living individuals held in any format, including, but not limited to paper documents, computer databases, visual images, audio recordings, CCTV footage, videos, emails etc.
- 6.7.7 Article 5 of the UK GDPR sets out 7 basic 'Key Principles' (known as the Data Protection Principles) which lay at the heart of data protection law. Compliance with these principles is therefore a fundamental building block for good data protection practice and key to compliance with data protection law.
- 6.7.8 These principles stipulate that personal data must be:
- Processed fairly, transparently and lawfully processed
 - Processed for limited and specific purposes
 - Adequate, relevant and not excessive (i.e. minimised)
 - Accurate and up to date
 - Not kept longer than necessary
 - Securely held with integrity and confidentiality
 - Accountability
- 6.7.9 Further details about these principles and how to apply them can be found in the Data Protection Policy. For details about the 'Accountability' principle, please see section 4.

6.7.10 UK GDPR also sets out rights for data subjects. These are:

- The right of access
- The right to be informed
- Right to rectification
- Right to be forgotten
- Right to restriction
- The right to object to processing
- Automated decision making including profiling
- Portability

6.7.11 Further details about these rights, how to recognise a request from a data subject asserting one of their rights and details of how these are processed by the ICB, please see Subject access & Access to Health Records Policy and Data Protection Policy.

6.8 Incident Reporting

6.8.1 IG and IT related incidents, including cyber security incidents, must be reported and managed through the ICB's IG & Cyber Incident Reporting Procedure which requires the IG Team to be informed immediately of all IG, information security and cyber security incidents. These include, but are not limited to, NHSD's classifications:

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

6.8.2 On receiving notification of a potential serious incident requiring investigation, the IG Team will inform the SIRO and Caldicott Guardian as soon as practicably possible (if they are not already aware) to seek advice and guidance, as appropriate.

6.8.3 All IG and IT related incidents will be reviewed by the IG team and where necessary escalated to NHS Digital, Department of Health and the Information Commissioner's Office using the Incident Reporting functionalities of the DSPT.

6.8.4 The decision to report externally to the ICO is made in line with NHSD's Guide to the Notification of Data Security and Protection Incidents, with the ultimate decision being made by the SIRO, based on the advice of the DPO.

6.8.5 The DPO monitors IG incidents to identify trends and guide overarching remedial action to those trends.

6.9 Information Asset Management and Business Continuity

6.9.1 A core IG objective is that Information Assets (IAs) and the use of information held within them is identified and that the business importance/purpose is established.

6.9.2 IAs are those that are central to the efficient running of the ICB and specific departments, for example, clinical systems (such as Broadcare), record repositories (such as Datix) and so on. They also include, but are not limited to the following examples:

- Information – system documentation and procedures, archive media and data.
- Software – databases, application programs, systems, development tools and utilities.
- Physical – infrastructure, equipment, furniture and accommodation used for data processing.
- Services – computing and communications, heating, lighting, power, air conditioning used for data processing.
- People – qualifications, skills and experience in the use of information systems.
- Intangible – the ICB's reputation.

6.9.3 Essentially, it is information in any format that is of value to the organisation and would be problematic if it were not accessible.

6.9.4 Departments across the ICB are required to keep an Information Asset Register (IAR). The IG Team has processes and procedures in place to periodically request and review IARs and escalate any concerns to the SIRO. The ICB has clear lines of accountability for Information Risk Management (IRM) that reports directly to the Board through the SIRO.

6.10 Training Needs Analysis (TNA)

6.10.1 Staff holding specialist IG roles including, SIRO, Caldicott Guardian, DPO, IAOs and IAAs receive additional training commensurate with their role.

6.10.2 In IG TNA is developed, monitored and updated by the ICBs Head of IG as the DPO.

6.10.3 The need for any further IG training should be determined by line managers and their staff as part of the ICB's appraisal process.

6.11 Policies, Procedures & Staff Guidance

6.11.1 The ICB has a comprehensive range of IG Policies, procedures and staff guidance which support the IG agenda. Legal and professional registration guidance should also be considered where appropriate.

6.11.2 Policies and guidance documents are available to all staff on the Staff Intranet. As part of the ICBs openness and transparency obligations the ICBs policies are also available on the ICBs public website www.blmkicb.nhs.uk

Appendix 1 - Equality Impact Assessment Initial Screening

Please answer the questions against each of the protected characteristic and inclusion health groups. If there are significant impacts and issues identified a full Equality / Quality Impact Assessment (EQIA) must be undertaken. It is against the law to discriminate against someone because of these protected characteristics. For support and advice on undertaking EQIAs please contact: agcsu.equalities@nhs.net

| | |
|---------------------------------|------------------------------------|
| Name of Policy: | Information Governance Policy |
| Date of assessment: | 1/9/2022 |
| Screening undertaken by: | Head of Information Governance/DPO |

| Protected characteristic and inclusion health groups. Find out more about the Equality Act 2010, which provides the legal framework to tackle disadvantage and discrimination: https://www.equalityhumanrights.com/en/equality-act/protected-characteristics | Could the policy create a disadvantage for some groups in application or access? (Give brief summary) | If Yes - are there any mechanisms already in place to mitigate the potential adverse impacts identified? If not, please detail additional actions that could help. If this is not possible, please explain why |
|---|--|--|
| Age A person belonging to a particular age (for example 32 year olds) or range of ages (for example 18 to 30 year olds). | No | |
| Disability A person has a disability if she or he has a physical 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. | No | |
| Gender reassignment The process of transitioning from one gender to another. | No | |
| Marriage and civil partnership Marriage is a union between a man and a woman or between a same-sex couple. Same-sex couples can also have their relationships legally recognised as 'civil partnerships'. | No | |
| Pregnancy and maternity Pregnancy is the condition of being pregnant or expecting a baby. Maternity refers to the period after the birth and is linked to maternity leave in the | No | |

| | | |
|--|----|--|
| employment context. In the non-work context, protection against maternity discrimination is for 26 weeks after giving birth, and this includes treating a woman unfavourably because she is breastfeeding. | | |
| Race Refers to the protected characteristic of race. It refers to a group of people defined by their race, colour and nationality (including citizenship) ethnic or national origins. | No | |
| Religion or belief Religion refers to any religion, including a lack of religion. Belief refers to any religious or philosophical belief and includes a lack of belief. Generally, a belief should affect your life choices or the way you live for it to be included in the definition. | No | |
| Sex A man or a woman. | No | |
| Sexual orientation Whether a person's sexual attraction is towards their own sex, the opposite sex, to both sexes or none. | No | |
| Carers Individuals within the ICB which may have carer responsibilities. | No | |
| Please summarise the improvements which this policy offers compared to the previous version or position. | | |
| Reviewed to take into account ICB and new reporting mechanisms | | |
| Has potential disadvantage for some groups been identified which require mitigation? | | |
| No – (If there are significant impacts and issues identified a full Equality / Quality Impact Assessment (EQIA) must be undertaken.) | | |

Appendix 2 - Data Protection Impact Assessment Initial Screening

Data protection is the fair and proper use of information about people. Before completing this form, please refer to the Data Protection Impact Assessment (DPIA) Guidance in the Information Governance (IG) section on the staff Intranet or contact the Data Protection Officer for support via blmkicb.ig@nhs.net

A DPIA is a process to help you identify and minimise the data protection risks. You must do a DPIA for processing that is likely to result in a high risk to individuals. You can use our screening checklist below to help you decide when to do one. If you have answered 'Yes' to any of the 10 screening questions, you must then carry out a full DPIA using the Stage 2 form, which is also available on the Intranet in the IG section.

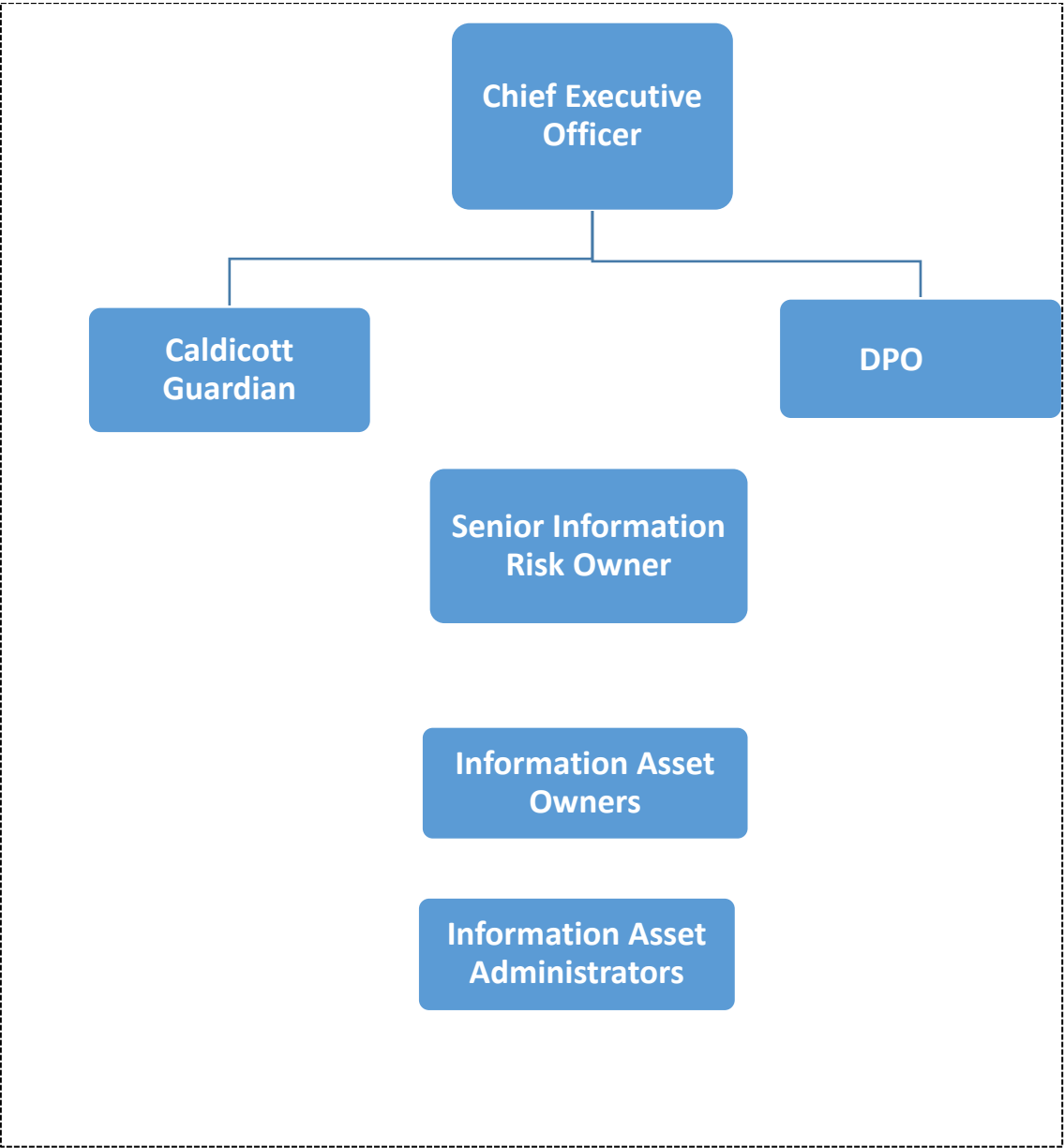
| | |
|---------------------------------|------------------------------------|
| Name of Policy: | Information Governance Policy |
| Date of assessment: | 14/03/2022 |
| Screening undertaken by: | Head of Information Governance/DPO |

Stage 1 – DPIA form

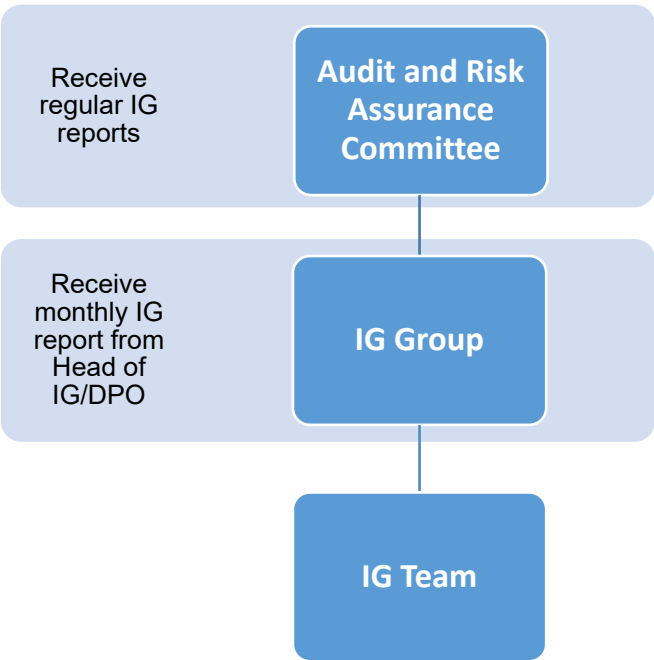
please answer 'Yes' or 'No'

| | |
|---|-----|
| 1. Will the policy result in the processing of personal identifiable information / data? This includes information about living or deceased individuals, including their name, address postcode, email address, telephone number, payroll number etc. | Yes |
| 2. Will the policy result in the processing of sensitive information / data? This includes for living or deceased individuals, including their physical health, mental health, sexuality, sexual orientation, religious belief, National Insurance No., political interest etc. | Yes |
| 3. Will the policy involve the sharing of identifiers which are unique to an individual or household? e.g., Hospital Number, NHS Number, National Insurance Number, Payroll Number etc. | Yes |
| 4. Will the policy result in the processing of pseudonymised information by organisations who have the key / ability to reidentify the information? Pseudonymised data - where all identifiers have been removed and replaced with alternative identifiers that do not identify any individual. Re-identification can only be achieved with knowledge of the re-identification key. Anonymised data - data where all identifiers have been removed and data left does not identify any patients. Re-identification is remotely possible, but very unlikely. | No |
| 5. Will the policy result in organisations or people having access to information they do not currently have access to? | Yes |
| 6. Will the policy result in an organisation using information it already holds or has access to, but for a different purpose? | No |
| 7. Does the policy result in the use of technology which might be perceived as being privacy intruding? e.g., biometrics, facial recognition, CCTV, audio recording etc. | Yes |
| 8. Will the policy result in decisions being made or action being taken against individuals in ways which could have a significant impact on them? Including profiling and automated decision making. (This is automated processing of personal data to evaluate certain things about an individual i.e., diagnosis and then making a decision solely by automated means - without any human involvement) | No |
| 9. Will the policy result in the collection of additional information about individuals in addition to what is already collected / held? | No |
| 10. Will the policy require individuals to be contacted in ways which they may not be aware of and may find intrusive? e.g., personal email, text message etc. | Yes |

Appendix 3 - Processes/Flow diagram



Appendix 4 - Information Governance Reporting



Appendix 5 - Data Security & Protection Standards

Data Security Standard 1

All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form.

Personal confidential data is only shared for lawful and appropriate purposes. Staff understand how to strike the balance between sharing and protecting information, and expertise is on hand to help them make sensible judgments. Staff are trained in the relevant pieces of legislation and periodically reminded of the consequences to patients, their employer and to themselves of mishandling personal confidential data.

Data Security Standard 2

All staff must understand their responsibilities under the Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.

All staff understand what constitutes deliberate, negligent or complacent behavior and the implications for their employment. They are made aware that their usage of IT systems is logged and attributable to them personally. Insecure behaviors are reported without fear of recrimination and procedures which prompt insecure workarounds are reported, with action taken.

Data Security Standard 3

All staff complete annual security training that is followed by a test, which can be re-taken unlimited times but which must ultimately be passed. Staff are supported by their organisation in understanding data security and in passing the test. The training includes a number of realistic and relevant case studies.

Data Security Standard 4

Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.

The principle of 'least privilege' is applied, so that users do not have access to data they have no business need to see. Staff do not accumulate system accesses over time. User privileges are proactively managed so that there is, as far as is practicable, a forensic trail back to a specific user or user group. Where necessary, organisations will look to non-technical means of recording IT usage (such as sign in sheets, CCTV, correlation with other systems, shift rosters).

Data Security Standard 5

Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.

Past security breaches and near misses are recorded and used to inform periodic workshops to identify and manage problem processes. User representation is crucial. This should be a candid look at where high risk behaviors are most commonly seen, followed by actions to address these issues while not making life more painful for users (as pain will often be the root cause of an insecure workaround). If security feels like a hassle, it's not being done properly.

Data Security Standard 6

Cyber-attacks against services are identified and resisted and NHS Digital Data Security Centre security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.

All staff are trained in how to report an incident, and appreciation is expressed when incidents are reported. Sitting on an incident, rather than reporting it promptly, faces harsh sanctions. Their Board understands that it is ultimately accountable for the impact of security incidents, and bear the responsibility for making staff aware of their responsibilities to report upwards. Basic safeguards are in place to prevent users from unsafe internet use. Anti-virus, anti-spam filters and basic firewall protections are deployed to protect users from basic internet-borne threats.

Data Security Standard 7

A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.

A business continuity exercise is run every year as a minimum, with guidance and templates available from NHS Digital Data Security Centre. Those in key roles will receive dedicated training so as to make judicious use of the available materials, ensuring that planning is modelled around the needs of their own business. There should be a clear focus on enabling senior management to make good decisions, and this requires genuine understanding of the topic, as well as the good use of plain English.

Data Security Standard 8

No unsupported operating systems, software or internet browsers are used within the IT estate.

Guidance and support is available from NHS Digital Data Security Centre to ensure risk owners understand how to prioritise their vulnerabilities. There is a clear recognition that not all unsupported systems can be upgraded and that financial and other constraints should drive intelligent discussion around priorities. Value for money is of utmost importance, as is the need to understand the risks posed by those systems which cannot be upgraded. It's about demonstrating that analysis has been done and informed decisions were made.

Data Security Standard 9

A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework. This is reviewed at least annually. NHS Digital Data Security Centre assists risk owners in understanding which national frameworks do what, and which components are intended to achieve which outcomes.

Security standard nine expands the organisations cyber security framework to detail the granular technical controls expected to meet mandated MCSS and NIS requirements. For example, DSPT assertion 9.3.6 mandates that the organisation is protecting data in transit (including email) using well configured TLS 1.2 or better.

There is a clear understanding that organisations can tackle the NDG Standards in whichever order they choose, and that the emphasis is on progress from their own starting points.

Data Security Standard 10

IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the Data Security Standards.

IT suppliers understand their obligations as data processors under the UKGDPR, and the necessity to educate and inform customers, working with them to combine security and usability in systems. IT suppliers typically service large numbers of similar organisations and as such represent a large proportion of the overall 'attack surface'. Consequently, their duty to robust risk management is vital and should be built into contracts as a matter of course. It is incumbent on suppliers of all IT systems to ensure their software runs on supported operating systems and is compatible with supported internet browsers and plug-ins.

Appendix 6 - Information Governance Strategy

INFORMATION GOVERNANCE STRATEGY 2022-2023

| | |
|--------------------|------------------------------------|
| Author | Head of Information Governance/DPO |
| Reviewed by | IG Group |
| Approved by | |
| Version | 0.2 |
| Review date | September 2023 |

CONTENTS

1. Purpose
2. Developments to achieve the ICB and wider NHS objectives
3. Scope of the strategy
4. Review

Annex A – Equality Impact Assessment form

1. Purpose

The purpose of this document is to describe the ICB strategy for IG and broad implementation plans to achieve this strategy.

This strategy sets out the approach to be taken within the ICB to provide a robust Information Governance framework that encompasses the National Guardian's ten data security standards for the management and sharing of information. All organisations that have access to NHS patient data and systems must use NHS Digital's Data Security and Protection Toolkit (DSPT) to provide assurance they are practicing good data security and that personal information is handled correctly. <https://www.dsptoolkit.nhs.uk/>.

The NHS Digital DSPT will inform the IG workplan.

2. Developments to achieve the ICB strategy

This strategy outlines the approach the ICB will take to ensure it develops effective information governance processes throughout the organisation, which will enable it to deliver its objectives and meet its statutory requirements.

The ICB needs to address the following priorities:

- Ensure the GP IT Operating Framework Model which outlines the ICB responsibilities toward GP DPO support is in place. The ICB has outsourced the DPO service for Bedfordshire, Luton & Milton Keynes practices and has an IG Facilitator who provides advice and guidance to GP practices and links in with the GP DPO service.
- The ICB is required to ensure staff members understand their personal accountability for data handling. A thematic review of incidents i.e. CHC team will be undertaken to the avoidance of future data incidents.

- Annual IG training is mandatory. The ICB will continue to monitor on a monthly basis the uptake of the online Data Security Module 1. Bespoke MS teams IG training will be kept up to date or designed as required.
- The ICB must ensure access to personal identifiable data is restricted and authorised. Access must be auditable. The ICB will continue to promote Data Protection by Design and will conduct an audit of Data Protection Impact Assessments during 2022.
- The ICB will continue to link with HBLICT (I.T provider) ensuring cyber security is robust and demonstrated by their participation in any national initiatives and schemes to improve resilience to cyber-attacks.
- The IG team will work with ICB members in supporting the archiving and/or deletion of electronic records in accordance with records management guidance.
- ICB members IAOs/IAAs will continue to update and review their information assets and data flow spreadsheets ensuring any data flows have relevant data processing agreements in place. IG team will offer support/training to members as required.
- To link in with the ICS IG projects and initiatives and the impact these may have on ICB and GP/PCNs as we move toward integrated ICS working.

3. Scope of the strategy

The key component underpinning this strategy, is:

- The ICB Information Governance Policy and Management Framework, which outlines the broader objectives for information governance; and
- Fundamental to the success of delivering the Information Governance Strategy is maintaining and further developing the information governance culture within the ICB.

4. Review

The strategy will be reviewed in September 2023 or prior to this should new legislation or national guidance require it.

Annex A – Equality Impact Assessment Form
Initial screening

| | |
|--|---|
| Name of proposal (policy/strategy/function/service being assessed) | ICB Information Governance Strategy |
| Those involved in assessment: | IG team and for agreement by the IG Group |
| Is this a new proposal? | Yes |
| Date of initial screening | 14 March 2022 |

| | |
|---|--|
| What are the aims and objectives? | To ensure the effective management of information governance and that the strategic vision and framework |
| Who will benefit? | All staff working for and on behalf of the ICB |
| Who are the main stakeholders? | All staff working for and on behalf of the ICB |
| What are the desired outcomes? | Staff awareness of the strategy through being advised of its availability on the ICBs' website IG page |
| What factors could detract from the desired outcomes? | Lack of awareness of the existence of this strategy |
| What factors could contribute to the desired outcomes? | Knowledge of the strategy and its implementation |
| Who is responsible? | All staff |
| Have you consulted on the proposal? If so with whom? If not, why not? | Strategy developed in consultation with the IG Group. |

What protected characteristics could be affected and be disadvantaged by this proposal (please tick).

| | | Yes | No |
|--------------------------------|---|-----|----|
| Age | Consider: Elderly or young people | | X |
| Disability | Consider: Physical, visual, aural impairment, mental or learning disabilities | | X |
| Gender reassignment | Consider: Transsexual people who propose to, are doing or have undergone a process of having their sex reassigned | | X |
| Marriage and civil partnership | Consider: impact relevant to employment and/or training | | X |
| Pregnancy and maternity | Consider: Pregnancy related matter/illness or maternity leave related matter | | X |
| Race | Consider: Language and cultural factors, include Gypsy or Travellers Group | | X |

| | | | |
|---------------------|--|--|---|
| Religion and Belief | Consider: Practices of worship, religious or cultural observance, include non-belief | | X |
| Sex/Gender | Consider: Male or Female | | X |
| Sexual Orientation | Consider: Know or perceived orientation | | X |

What information and evidence do you have about the groups that you have selected above?

The above characteristics will have no adverse impact.

What consultation has taken place has taken place or is planned with each of the identified groups?

The Strategy was developed in consultation with the IG Group.

What was the outcome of the consultation undertaken?

Approval and endorsement sought.

What changes or actions do you propose to make or take as a result of research and/or consultation?

The Information Governance team on behalf of the SIRO and IG Group will be responsible for ensuring this strategy is implemented, including any supporting guidance and training deemed necessary to support the implementation.

Will the planned changes to the proposal?

| | |
|---|-----|
| a) Lower the negative impact? | N/A |
| b) Ensure that the negative impact is legal under anti-discriminatory law? | N/A |
| c) Provide an opportunity to promote equality, equal opportunity and improve relations i.e a positive impact? | N/A |

Taking into account the views of the groups consulted and the available evidence, please clearly state the risks associated with the proposal, weighed against the benefits.

Information risk – The ICB must respect patient confidentiality in accordance with national legislation and guidance.

What monitoring/evaluation/review systems have been put in place?

Monitoring will be undertaken by the Information Governance team.

When will it be reviewed?

June 2022.

Date completed: 14 March 2022

Name: Lynda Harris, Head of Information Governance/DPO

Approved by:

Date approved: