INFORMATION GOVERNANCE AND DATA PROTECTION POLICY

Version: 8.0
April 2025

Kernow Health

Policy Name	Information Governance and Data Protection Policy
Version	V8.0
Name of responsible (ratifying) committee	KHCIC Board
Date Agreed	05/06/2025
Date Ratified	25/06/2025
Responsible Policy Lead	Business & Quality Assurance Manager
Document Manager (job title)	Business & Quality Assurance Manager
Date issued	26/06/2025
Review date	March 2028 (subject to legislative changes)
Electronic location	SharePoint
Related Policy/Procedure Documents	Compliments, Complaints and Feedback Policy Confidentiality Policy Risk Management Policy Data Protection and Impact Assessment Policy Records Retention and Destruction Policy Email Use Policy Subject Access Request Guidance Patient Safety & Incident Reporting Policy
In the case of hard copies of this policy the content can only be assured to be accurate on the date of issue marked on the document. For assurance that the most up to date policy is being used, staff should refer to the version held on the intranet	

Amendment History

Version	Status	Date	Reason for Change	Authorised
1.0	New	14/06/2017		
2.0	Final	11/09/2017	Review	L Manolchev
3.0	Final	13/03/2018	Annual review to include GDPR requirements	L Manolchev
4.0	Final	11/06/2019	Annual Review	L Manolchev
5.0	Final	07/05/2020	Annual Review	L Manolchev
6.0	Final	16/04/2021	Annual Review	L Manolchev
7.0	Final	April 2022	Review	L Manolchev
8.0	Final	April 2025	Review	L Manolchev

INFORMATION GOVERNANCE AND DATA PROTECTION POLICY

Contents

1. INTRODUCTION

1.1. Information governance is the framework of law and best practice that regulates the manner in which information, (including information relating to and identifying individuals) whether internally or externally generated and in any format or media type is managed (i.e. obtained, handled, used and disclosed). It is a complex and rapidly developing area and one of utmost importance since information lies at the heart of the organisation and underpins everything it does.

1.2. 'Information governance' is an umbrella term for a collection of distinct but overlapping disciplines. Reference to 'information governance' in this policy shall mean reference to the following areas as well:

- Access to information including Freedom of Information Act 2000, Data Protection Act 2018, UK General Data Protection Regulations (GDPR)
- Confidentiality and data protection
- Information security assurance
- Information quality assurance
- Records and document management

1.3. The organisation's records are its corporate memory, providing evidence of actions and decisions and representing a vital asset to support daily functions and operations. Good record keeping supports policy formation and managerial decision-making, protects the interests of the organisation and the rights of patients, staff and members of the public. They support consistency, continuity, efficiency and productivity and help deliver services in consistent and equitable ways.

1.4. KHCIC Board has adopted this policy and is committed to on-going improvement of its information governance functions to ensure that it continues to use information safely, securely and for the purposes it is intended for.

2. PURPOSE

2.1. The organisation is committed to ensuring that its information is managed to the highest standards and in accordance with all relevant legislative requirements, including the Data Protection Act 2018, the Freedom of Information Act 2000; best practice guidance from organisations such as the Information Commissioner's Office (www.ico.gov.uk) and NHS England Digital (digital.nhs.uk/).

2.2. The purpose of this policy is to ensure that all types of information held by the organisation, whether that is corporate, patient or personnel information, are kept safe, secure and are managed appropriately, so that:

- records are available when needed
- records can be accessed
- records can be interpreted
- records can be trusted
- records can be maintained through time
- records are secure
- records are retained and disposed of appropriately
- staff are trained
- patients are informed

2.3. To this end, KHCIC commits itself to:

Information Governance and Data Protection Management: establishing and maintaining robust operational and management accountability structures as well as assigning appropriate resources and expertise to ensure information governance issues are dealt with appropriately, effectively and at levels within the organisation that are consistent with the type and gravity of the issue in question.

Systems and Processes: implementing information systems and processes to enable the efficient and secure storage and retrieval of information and the management of information risk.

Training and Awareness: implementing a system of training and awareness that is role based, assessed and capable of equipping staff with the skills and knowledge necessary to carry out their responsibilities.

Audit: monitoring staff compliance with the information governance framework through regular audits.

3. SCOPE

3.1. This policy sets out the organisation's approach to ensuring it has a robust information governance framework to manage its information assets. In particular, the operational and management structures, roles, responsibilities, systems, policies, procedures and audit controls that the organisation has established to ensure such issues are appropriately addressed throughout the organisation.

3.2. This policy will be available to all staff employed by KHCIC, including consultants, temporary staff, agency workers, and bank staff who carry out work on behalf of KHCIC. All staff are responsible for remaining up to date with and adhering to this policy.

4. ROLES & RESPONSIBILITIES

4.1. Information Governance Lead

The Information Governance Lead has overall responsibility for information governance in the organisation.

4.2. KHCIC Board

The Board of Directors is responsible for ensuring that the information governance function is addressed at a strategic level. They will make certain there is an adequate level of resources and expertise to deal with the range of issues that arise across the information governance function.

4.3. Chief Executive and Information Governance Lead

The Chief Executive and Information Governance Lead are responsible for ensuring that staff within the organisation are aware of their obligations in relation to Data Protection Act 2018 and other data protection laws. They are also the owners of the organisation's Corporate Risk Register and lead the organisation's governance function.

4.4. Data Protection Officer

The Data Protection Officer is responsible for ensuring that KHCIC continues to meet its duties under data protection legislation by monitoring compliance, managing internal processes and advise and conduct internal audits.

4.5. **Privacy Officer**

The Privacy Officer is responsible for ensuring the appropriate accesses are in place for systems that KHCIC use. The Privacy Officer will assist in investigating in breaches of data where records have been accessed inappropriately. The Privacy Officer will also conduct audits and check systems to ensure the appropriate access levels are in place and taking the appropriate actions where this is not the case.

4.6. **Digital Clinical Safety Officer**

The Digital Clinical Safety Officer is responsible for ensuring that there is effective clinical risk management processes in place on current and new health IT systems that are in use. They are also responsible for:

- Managing and overseeing clinical safety cases as a result of health IT systems
- Raise awareness and understanding of clinical risk management within the organisation to reinforce safety culture
- Work closely with key suppliers to ensure assurance is sought on the clinical safety of health systems the organisation uses

4.7. **Senior Information Risk Owner**

The Senior Information Risk Owner (SIRO) oversees development and delivery of the information governance function.

The Senior Information Risk Owner (SIRO) acts as champion for information risk on behalf of the Board. They advise the Board of the performance of the Information Governance function of the organisation, ensure it is given appropriate resources and commitment and is appropriately communicated to all staff. They lead on information security assurance; ensure that all information risks are dealt with in line with the Risk Management Policy and the Board Assurance Framework (BAF) and that all information incidents follow KHCIC's Patient Safety and Incident Reporting Policy.

4.8. **Information Governance Steering Group**

The Information Governance Steering Group (IGSG) will meet monthly to monitor progress against the Information Governance agenda. The Board has granted the IGSG authority to make decisions relating to the Information Governance agenda. The IGSG will provide monthly updates to Governance Committee and KHCIC Board.

4.9. **Business and Quality Assurance Manager**

The Business and Quality Assurance Manager is responsible for ensuring arrangements are in place so that KHCIC complies with its information quality and records management obligations. This includes monitoring performance, in order that any needs are considered and addressed. The Business and Quality Assurance Manager is also responsible for ensuring staff receive appropriate and timely training so that they are aware of their information governance responsibilities.

4.10. **Governance Team**

The Business and Quality Assurance Manager as manager of the Governance Team has day-to-day operational responsibility for all aspects of Information Governance which includes answering detailed questions from people using KHCIC's services regarding the use of their information.

In particular they are responsible for developing policy and advising on the obtaining, handling, use and disclosure of information. They are also responsible for creating and maintaining the organisation's Information Asset Register. They act as the link between the various groups and individuals involved in the Information Governance agenda. Where required, an information governance strategy/improvement plan will be written which includes the following key elements:

- Objectives and deliverables should be:
    - Specific - define exactly what improvement is to be made
    - Measurable - describe how it will be known that the improvement has been achieved
    - Achievable - set realistic plans that can be achieved within the time constraints and resources available
    - Relevant - relate the specific actions to ongoing improvement work
    - Time-bound - set a date for completion
- Liaising with the SIRO to identify resources to deliver the work programme
- Risks and issues that may impact upon delivery

4.11. **Caldicott Guardian**

The Caldicott Guardian has overall responsibility for ensuring information relating to patients is used confidentially and handled with the appropriate safeguards.

All staff are reminded of the need to adhere to the Caldicott Principles as set out in Appendix 2. Alongside the Data Protection Act 2018, these represent best practice for using and sharing confidential or identifiable information and should be applied whenever a disclosure or use of information is being considered.

4.12. **Head of Digital**

The Head of Digital has responsibility for information security, working alongside Cornwall I.T Services (CITS) in terms of delivering all aspects of information security and risk management.

4.13. **Information Asset Owners**

Information Asset Owners (IAOs) and Information Asset Assistants (IAAs) are responsible for maintaining the confidentiality, integrity, and availability of all information their Information Asset holds. A Business Continuity Plan is needed for all information assets should a threat occur.

Each Information asset will be recorded on the Information Asset Register which will be regularly maintained and updated with the relevant IAO to ensure its accuracy.

4.14. **Line Managers**

Line Managers are responsible for operational staff and monitor their compliance with the information governance agenda.

4.15. **Staff**

All staff are individually responsible for ensuring that they comply with the information governance framework and associated policies. Staff are also responsible for ensuring all information governance and data protection training is kept up to date

5. STANDARDS AND PRACTICE

5.1. Information Requests

All requests for potentially confidential or sensitive information should be processed in line with the Confidentiality Policy and Subject Access Request Guidance and passed to the Governance Team for processing unless there are exceptional circumstances where this is not possible. In the event that information must be shared, staff should consult with their line manager who can seek assistance from a Senior Management/Caldicott Guardian as appropriate.

5.2. Subject Access Requests

Data subjects can access the information about them kept by the organisation through a Subject Access Request (SAR). It is the responsibility of the Governance Team to deal with such requests and as per the SAR procedure.

5.3. Freedom of Information Requests

KHCIC is not a public body and therefore does not have a legal responsibility under the Freedom of Information Act. However, any reasonable request for information will be considered on its own merit and, where possible, complied with.

5.4. Information Asset Access

Access to the organisation's information technology, infrastructure, computer networks and all other information assets are restricted to authorised personnel only.

Staff access to the organisation's information assets is restricted to that which is necessary and appropriate for them to carry out their role.

Staff are assigned login access to electronic information assets (for example databases or the network). Under no circumstances should staff share their passwords either with another member of staff or to an external party. All requests for new or updated access to any system must be requested by the staff member's manager and the request to be sent to kernowhealthcic.it@nhs.net If a user is asked for their password they should refuse and inform the IT team.

Generic email accounts are not generally used due to potential information security threats. However, where they are required, the decision will be made on a case-by-case basis with stringent procedures in place to ensure accountability and safe use of such accounts.

5.5. Information Security Assurance

The SIRO is responsible for leading on information security assurance within the organisation. It is recognised that in order to ensure that work related to information security management is appropriately carried out, a robust support structure is required.

The SIRO is supported principally in this role by the IGSG. Where there are significant risks or work being undertaken, this will be escalated to the Governance Committee and Board where relevant.

5.6. Information Governance Incidents

The organisation has a well-established Patient Safety and Incident Reporting Policy. All information governance incidents are investigated in line with this policy by the appropriate manager.

Any significant risks identified must be reported directly to the SIRO.

All significant information governance incidents are reported to the IGSG and escalated further to the Governance Committee and Board if appropriate. This will also seek to provide assurance to the Governance Committee and Board of any lessons learned and progress to embed any changes across the organisation.

5.7. **Training and Awareness**
Staff will be provided with information governance training relevant to their role at induction and are required to complete further mandatory training on an annual basis.

6. MONITORING AND COMPLIANCE

6.1. **To ensure compliance of this policy the following will be undertaken:**

- Regular audits
- Review of information flows
- Number of data breaches reported
- Training undertaken
- Annual Data Security and Protection Toolkit submission pending the move towards the Cyber Assurance Framework-Aligned Data Security and Protection Toolkit from July 2025.

7. DISSEMINATION AND IMPLEMENTATION

7.1. A copy of the policy will be stored electronically on the shared drive and on the staff pages on the KHCIC website.

7.2. Staff will be made aware of this policy through bulletins.

8. EQUALITY IMPACT ASSESSMENT

8.1. An initial equality impact assessment has been carried out and there are no differential impacts identified on any of the protected characteristics. Therefore, a full equality impact assessment is not required (see appendix 1).

Appendix 1 - Initial Equality Impact Assessment Form

Name of strategy/ policy/ proposal/ service function to be assessed:	Information Governance and Data Protection Policy
Service Area:	Corporate
Is this a new or existing strategy/ policy/ proposal/ service?	Existing
Name of individual(s) completing assessment:	L Manolchev
Date:	24/04/2025

1) Policy aim *Who is the strategy/ policy/ proposal/ service function aimed at?*	The aim of the policy is to ensure that all information held by KHCIC is managed safely, securely and is used for the purpose it was collected for. It provides a framework for all information governance processes which is supported by other policies that support this agenda.				
2) Policy objectives	• To ensure that all information collated and processed is kept safe and secure • To have a robust framework in place for staff to refer to • To ensure that there are clear responsibilities and expectations for all staff across the organisation that handle personal and sensitive information				
3) Policy – Intended Outcomes	• Safe and effective practices to maintain confidentiality and ensure information is kept safe and secure. • Reduction in breaches, and reportable breaches to Information Commissioners Office (ICO)				
4) How will you measure the outcome?	• Regular audits • Review of information flows • Number of data breaches reported • Training undertaken • Annual Data Security and Protection Toolkit submission and the Cyber Assurance Framework Aligned Data and Security Protection Toolkit from July 2025				
5) Who is intended to benefit from the strategy/ policy/ proposal/ service function?	• Patient/public will benefit as their information is kept safe and will maintain trust • Staff will benefit as it provides a framework to ensure the integrity of the information being handled and also provides information on reporting any breaches or concerns • KHCIC will benefit as it will maintain trust with the public and commissioners that it continues to keep information safe.				
6a) Who did you consult with?	Workforce	Patients	Local Groups	Ext. Organisations	Other

6b) Please identify the groups who have been consulted about this strategy/ policy/ proposal/ service function? *Please records specific names of groups*	Not applicable – review of policy and no significant changes were made
7) What was the outcome of the consultation?	As above

8) The Impact

Are there any concerns that the function being assessed **could** have differential impact on:

Equality Strands:	Yes	No	Unsure	Rationale for Assessment/ Existing Evidence
Age		✓		
Sex (male, female, trans-gender/ gender reassignment)		✓		
Race/ Ethnic Communities/ Groups		✓		
Disability – Learning disability, physical impairment, sensory impairment, mental health conditions and some long term health conditions		✓		
Religion/ Other Beliefs		✓		
Marriage and Civil Partnerships		✓		
Pregnancy & Maternity		✓		
Sexual Orientation – Bisexual, Gay, Heterosexual, Lesbian		✓		

You will need to continue to a full Equality Impact Assessment if the following have been highlighted:

- You have ticked "Yes" in any column above and
- No consultation or evidence of there being consultation - this excludes any *policies* which have been identified as not requiring consultation**; or**
- Major this relates to service redesign or development

9) Please indicate if a full equality analysis is recommended	**Yes**		**No**	✓

10) If you are not recommending a Full Impact Assessment please explain why.
This is a review of an existing policy and no significant changes have been made. There are no differential impacts identified on any of the protected characteristics and as such a full equality impact assessment is not required.

Sign Off	
Group/ Committee sign off:	Governance Committee
Date signed off:	3rd June 2025

Appendix 2 – Eight Caldicott Principles

NDG National Data Guardian for health and social care

The Eight Caldicott Principles

Good information sharing is essential for providing safe and effective care. There are also important uses of information for purposes other than individual care, which contribute to the overall delivery of health and social care or serve wider public interests.

These principles apply to the use of confidential information within health and social care organisations and when such information is shared with other organisations and between individuals, both for individual care and for other purposes.

The principles are intended to apply to all data collected for the provision of health and social care services where patients and service users can be identified and would expect that it will be kept private. This may include for instance, details about symptoms, diagnosis, treatment, names and addresses. In some instances, the principles should also be applied to the processing of staff information.

They are primarily intended to guide organisations and their staff, but it should be remembered that patients, service users and/or their representatives should be included as active partners in the use of confidential information.

Where a novel and/or difficult judgment or decision is required, it is advisable to involve a Caldicott Guardian.

Principle 1: Justify the purpose(s) for using confidential information

Every proposed use or transfer of confidential information should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed by an appropriate guardian.

Principle 2: Use confidential information only when it is necessary

Confidential information should not be included unless it is necessary for the specified purpose(s) for which the information is used or accessed. The need to identify individuals should be considered at each stage of satisfying the purpose(s) and alternatives used where possible.

Principle 3: Use the minimum necessary confidential information

Where use of confidential information is considered to be necessary, each item of information must be justified so that only the minimum amount of confidential information is included as necessary for a given function.

Principle 4: Access to confidential information should be on a strict need-to-know basis

Only those who need access to confidential information should have access to it, and then only to the items that they need to see. This may mean introducing access controls or splitting information flows where one flow is used for several purposes.

Principle 5: Everyone with access to confidential information should be aware of their responsibilities

Action should be taken to ensure that all those handling confidential information understand their responsibilities and obligations to respect the confidentiality of patient and service users.

Principle 6: Comply with the law

Every use of confidential information must be lawful. All those handling confidential information are responsible for ensuring that their use of and access to that information complies with legal requirements set out in statute and under the common law.

Principle 7: The duty to share information for individual care is as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share confidential information in the best interests of patients and service users within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Principle 8: Inform patients and service users about how their confidential information is used

A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information - in some cases, greater engagement will be required.

Published December 2020

Appendix 3 Legislation and Key Documents

- The Data Protection Act 2018
- Freedom of Information Act 2000
- Common Law Duty of Confidentiality
- Records Management: NHS Code of Practice 2021 updated December 2023
- The HM Government Publication: Information Sharing – Pocket Guide
- Information Commissioner's Office - Privacy Impact Assessment Handbook