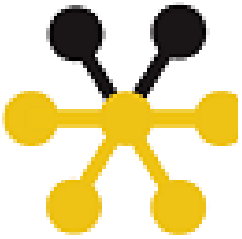
INFORMATION GOVERNANCE & DATA PROTECTION POLICY



Kernow Health

Policy Name	Information Governance & Data Protection Policy
Version	V5
Name of responsible (ratifying) committee	Kernow Health CIC Board
Date Agreed	05/05/2020
Date ratified	28/05/2020
Document Manager (job title)	Business & Quality Assurance Manager
Date issued	04/06/2020
Review date	March 2021
Electronic location	Whole Organisation\Policies & SOPS\Data Protection & Information Governance
Related Policies/ Procedural Documents	Complaints Policy Confidentiality Policy Information Risk Assessment & Management Guidance Data Protection and Impact Assessment Policy Records Retention and Destruction Policy Email Policy Subject Access Request Guidance Incident Reporting & Duty of Candour 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	

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

INFORMATION GOVERNANCE & DATA PROTECTION POLICY

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 encompassing the 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. Records support policy formation and managerial decision-making, protect 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 The organisation's 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.

1.5 This policy is the responsibility of the Information Governance Steering Group (IGSG). They will approve revisions and annually review its adequacy.

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 Digital (www.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. This includes ensuring 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, the organisation commits itself to:

a) **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.

b) **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.

c) **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.

d) **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 Kernow Health CIC, including consultants who are carrying out work on behalf of Kernow Health CIC. All staff are responsible for remaining up to date with and adhering to this policy.

4. DUTIES

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

4.2 The *Board of Directors* is responsible for ensuring that the information governance function is addressed at a strategic level. They will ensure 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 The *Chief Operating Officer* and *Head of Primary Care Operations*, 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.

4.4 The *Head of Primary Care Operations* is responsible for information governance at an operational level and is accountable to *the Board of Directors*. The Head of Primary Care Operations is the Data Protection Officer and as such 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 The Head of Primary Care Operations as the *Senior Information Risk Owner (SIRO*) oversees development and delivery of the information governance function.

4.6 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 and Board Assurance Framework (BAF) Policy and that all information incidents follow the organisation's Incident Reporting & Duty of Candour Policy.

4.7 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 and to approve new policies, amendments to policies and related documents. The IGSG provide monthly updates to the Kernow Health CIC Board.

4.8 The *Chief Operating Officer & Head of Primary Care Operations are* the owners of the organisation's Corporate Risk Register and lead the Governance/Admin Team. The Head of Primary Care Operations also fulfils the role of *Information Governance Manager*.

4.9 The *Information Governance Manager* has day-to-day operational responsibility for all aspects of Information Governance which includes answering detailed questions from people using our services about 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 and chair the IGSG. Each year they write an information governance strategy/improvement plan which includes the following key elements:

a) objectives and deliverables which 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

b) resources to deliver the work programme;

c) risks and issues that may impact upon delivery;

4.10 The *Caldicott Guardian (Medical Director)* has overall responsibility for ensuring information relating to patients is used confidentially and handled with the appropriate safeguards.

4.11 All staff are reminded of the need to adhere to the Caldicott Principles as set out in Appendix A. Alongside the Data Protection Act Principles, 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 The IT Manager 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 (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 The *Head of Primary Care Operations and Business & Quality Assurance Manager* fulfils the role of *Information Quality and Records Manager* and is responsible for ensuring arrangements are in place to ensure the organisation complies with its information quality and records management obligations. This includes monitoring performance, in order that any needs are considered and addressed.

4.15 The *Business & Quality Assurance Manager* has responsibility for ensuring staff receive appropriate and timely training to ensure they are aware of their information governance responsibilities.

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

4.17 *Staff* are individually responsible for ensuring that they comply with the information governance framework and will ensure that all work programmes acknowledge the requirements of the framework.

5. TRAINING & AWARENESS

5.1 *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. 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
- The HM Government Publication: Information Sharing – Pocket Guide
- Information Commissioner's Office - Privacy Impact Assessment Handbook

7. EQUALITY IMPACT ASSESSMENT

7.1 An initial equality impact assessment has been carried out and there are no differential impacts on any of the protected characteristics. Therefore a full equality impact assessment is not required.

Appendix A

The revised Caldicott principles

1. Justify the purpose(s)

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

2. Don't use personal confidential data unless it is absolutely necessary

Personal confidential data should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

3. Use the minimum necessary personal confidential data

Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data transferred or accessible as is necessary for a given function to be carried out.

4. Access to personal confidential data should be on a strict need-to-know basis

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

5. Everyone with access to personal confidential data should be aware of their responsibilities

Action should be taken to ensure that those handling personal confidential data – both clinical and non-clinical staff – are made fully aware of their responsibilities and obligations to respect patient confidentiality.

6. Comply with the law

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

7. The duty to share information can be as important as the duty to protect patient confidentiality

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.

Appendix B

Information Governance Management Framework
2020/ 2021

Senior Roles		
Roles	**Nominated Lead**	**Responsibilities**
Caldicott Guardian	Dr Jonathan Katz	• Ensuring information relating to patients is used confidentially and handled appropriately as per the Caldicott principles
Acting Information Governance Lead	Dr Jonathan Katz	• Overall responsibility of information governance • Oversee development & delivery of information governance
Data Protection Officer	Maria Harvey, Head of Primary Care Operations	• Advise and monitor compliance • Provide advice on DPIA's • Main contact with the ICO • Advise on other aspect of information governance and data protection within the organisation(s)
Senior Information Risk Owner	Maria Harvey, Head of Primary Care Operations	• Responsible for information risk • Lead on information security assurances • Ensuring that information governance is a thread through any new service or changes to services.

Governing Bodies	
Board/ Group	**Responsibilities**
Kernow Health CIC Board	• Responsible for the strategic overview of the information governance agenda • Ensuring that there are adequate resources available to fulfill the information governance function
Information Governance Steering Group	• Ensure that Kernow Health has effective policies and management processes in place to manage the information governance function • Undertake annual assessments and audits of its information governance policies and arrangements • Report back to the Board on any information governance issues • Investigate and report any potential

	information breaches
Key Policies	
• Information Governance and Data Protection Policy • Confidentiality Policy • Data Quality Policy • Incident Reporting & Duty of Candour • Information Risk Assessment & Management • Pseudonymisation & Anonymisation Policy • Subject Access Guidance	
Staff Responsibilities	
Role	**Responsibilities**
Head of Primary Care Operations	• It is the responsibility of the Head of Primary Care Operations as the SIRO and Governance Lead, to ensure that there are processes in place to safeguard information • Ensuring that any new services have information governance included within their set-up • Ensure that staff are aware of their roles in information governance
Business & Quality Assurance Manager	• Responsible for ensuring that policies and procedures are reviewed as required • Ensuring that training is carried out by Kernow Health CIC staff • Monitoring compliance with information governance and completing the requirements of the Data Security and Protection (DSP) Toolkit • Ensuring that the Information Asset Register is maintained and regularly updated with information held; Information Asset Owners; and Information Asset Administrators assigned • Updating and reviewing the Information Risk Register alongside the Head of Primary Care Operations • Ensuring compliance with records management and advising staff or their responsibilities
IT Manager	• Ensuring staff have the right access levels to I.T. systems • Liaising with CITS as our I.T. Systems and security provider • Respond to and manage any I.T. incidents
Corporate Business Support Manager	• Ensuring that financial and HR records are kept safe and secure • Ensuring that new and existing staff have

	the appropriate access levels
Information Asset Owner	• Ensure that any information being held is identified on the Information Asset Register • Ensure that there are security and access levels in place to safeguard information
Information Asset Administrator	• Ensure that information is kept secure • Ensure information being kept is correct
All Staff	• Ensuring that they keep all information safe and secure • Ensure that their I.G. training is up to date • Ensure that they familiarise themselves with policies and procedures around information governance • Report any information governance and data security incidents/ breaches

Training & Guidance
• All staff to have completed their online I.G. Training on a mandatory basis • Specific training to be available for staff with specific roles in relation to the information governance framework and agenda • All staff to be aware of current policies and procedures, including how to report potential information breaches

Appendix C

SYSTEMS AND PROCESSES

Access to Information

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 Admin Team for processing unless there are *exceptional circumstances* where this is not possible. In the event that information must be shared, staff should consult their line manager who can seek assistance from Senior Management/ Caldicott Guardian as appropriate.

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 Admin Team to deal with such requests and as per the SAR procedure.

Freedom of Information Requests

The organisation 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.

Information Asset Access

Access to the organisation's information technology, infrastructure, computer networks and all other information assets is 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 are their passwords to be shared. All requests for new or updated access to any system must follow the User Access Amendment Process. If a user is asked for their password they should refuse to give it and inform their line manager or the Information Governance Manager of the request.

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

Information Security Assurance

The Senior Information Risk Officer (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.

Therefore in the organisation 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.

Information Governance Incidents

The organisation has a well-established Incident Reporting & Duty of Candour Policy. All information governance incidents are investigated in line with this policy by the Head of Primary Care Operations, Business & Quality Assurance Manager, the Information Asset Owners, Information Asset Administrators and the relevant line managers.

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.