NHS
Kernow
Clinical Commissioning Group

Information Governance Strategy

Date approved: 19 March 2019

Document control sheet

Title of document:	Information Governance Strategy
Originating Directorate:	Corporate Governance
Originating team:	Information Governance
Document type:	Policy
Subject category:	Information Governance
Author(s) name:	Trudy Corsellis
Date ratified:	19 March 2019
Ratified by:	Workforce Committee
Review frequency:	Three years - with an annual review of the organisational objectives
To be reviewed by date:	19 March 2022
Target audience:	All staff
Can this policy be released under FOI?	Yes
	Give reasons for exemption if no:

Version control

Version No	Revision date	Revision by	Nature of revisions
1.0	December 2018	Trudy Corsellis	Update to take account of new legislation and revised organisational objectives
2.0	January 2019	Trudy Corsellis	Shared with Workforce Committee and staff for comments
2.1	February 2019	Trudy Corsellis	Objectives updated based on comments from Workforce Committee

Contents

1. Aim

NHS Kernow is required to have effective arrangements in place to govern the uses of information and information systems within the organisation. It aims to achieve a standard of excellence in Information Governance (IG) by ensuring information is dealt with legally, securely, efficiently, and effectively in the course of NHS Kernow business, in order to commission and support high quality patient care.

Within NHS Kernow a framework exists which establishes a set of policies and procedures to ensure that appropriate standards are defined, implemented and maintained. It brings together the legal rules, guidance and best practice. In addition it assists with the assurance processes, including validating the IG processes of the organisations we commission.

Information governance is about setting a high standard for the handling of information and giving the organisation and its staff the tools to achieve that. The ultimate aim is to demonstrate that NHS Kernow can be trusted to maintain the confidentiality and security of information, by helping individuals to practice good information governance and be consistent in the way they handle personal, sensitive and corporate information. To achieve this we will:

- Implement central advice and guidance
- Comply with the law
- Put in place year on year improvement plans

2. The Scope of the Strategy

Information Governance (IG) has four fundamental aims:

- To support the provision of high quality care by promoting the effective and appropriate use of information
- To encourage responsible staff to work closely together, preventing duplication of effort and enabling more efficient use of resources
- To continue to develop support arrangements and provide staff with appropriate tools and support to enable them to carry out their responsibilities to consistently high standards
- To enable organisations to understand their own performance and manage improvement in a systematic and effective way

The security of processing personal information is covered in Article 32 of the General Data Protection Regulations (GDPR). It states organisations shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk including, as appropriate:

- the pseudonymisation and encryption of personal data
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing

However, suitably adjusted, the 4 concepts above also apply to confidential, not just personal, data. In order to fulfil its statutory and legal obligations NHS Kernow will also treat its confidential information with a similar level of due diligence. The completion of the Data Security and Protection Toolkit (DSPT) supports this process and is based on the ten National Data Guardian Standards. The assertions and mandatory components the DSPT contains inform the improvement plan and organisational objectives.

3. Principles

NHS Kernow will abide by the principles outlined below.

3.1 Information Security

Information security is characterised as the preservation of:

- **Confidentiality** – ensuring that access to the information is limited to those with the appropriate authority to see it
- **Integrity** – ensuring that information is complete, accurate, and reliable, and that its authenticity is guaranteed
- **Availability** – ensuring that the information is available to authorised users when and where required
- **Accountability** – ensuring that audit trail processes track all viewing, creating, amending, and deleting of the information

In order to maintain required levels of information security, the organisation will:

- Establish and maintain policies for the effective and secure management of its information assets and resources

- Promote effective confidentiality and security practice to its staff through policies, procedures and training
- Monitor and investigate all reported instances of actual or potential breaches of confidentiality and information security
- Undertake or commission regular assessments and audits of its information and IT security arrangements.

In recognition of the rising risk of cyber attacks across all sectors, NHS Kernow will implement and follow the Care Computer Emergency Response Team (CARECert) advice received from NHS Digital to ensure the CCG response effectively and safely to such attacks. (Please refer to appropriate IT policies and procedures as listed in Appendix 4.

3.2 Information Risk

A governance and assurance structure is in place to support the information risk agenda which includes:

- The Chief Operating Officer is the designated Senior Information Risk Owner (SIRO)
- The Deputy Director of Corporate Governance is the named Data Protection Officer and the Chair of the Information Governance Committee
- The Head of Information Governance and the Head of Corporate Governance provide advice, guidance and support relating to risks
- The Information Asset Owners (IAOs) have been tasked reviewing and their information assets to ensure compliance with national guidance and best practice and have identified their Information Asset Administrators
- Risks form a standing agenda item of the Information Governance Sub-Committee and can be escalated to the Workforce Committee, as appropriate

3.3 Information Registers

During 2018 the information flow mapping register was reviewed and updated to take account of legal requirements outlined in the Data Protection Act (2018) and the DSPT.

The Caldicott Guardian Log captures personal information breaches by NHS Kernow staff (or contractors) as well as breaches by other organisations that send CCG staff personal information inappropriately. The Log was revisited to provide greater rigour in managing the breach reporting process and ensuring the learning from such incidents informs our IG improvement plan.

3.4 Records Management and Subject Access Requests

NHS Kernow is committed to a systematic and planned approach to the management of records within the organisation, from their creation to their ultimate disposal. This includes both personal information and corporate information. NHS Kernow will ensure that it controls the quality and quantity of the information it generates, can maintain that information in an effective manner, and can dispose of the information efficiently when it is no longer required. It will ensure records are managed in accordance with the Records Management Code of Practice for Health and Social Care (2016) produced by the Information Governance Alliance and subject access requests are complied with within 30 days.

3.5 Data Protection by Design and Default

To increase accountability and focus, 'data protection by design and default' has become a legal requirement under the GDPR. As part of its systems and processes NHS Kernow will demonstrate how it is complying with the accompanying requirements and obligations. The use of Data Protection Impact Assessments (DPIAs) will support this work. In the unlikely event a DPIA results in a high risk rating, it is recognised that mitigations need to be put in place to reduce the risk. If this is not feasible, the DPIA will be shared with the Information Commissioners Office (ICO) before any processing of personal information takes place.

3.6 Information Sharing Agreements (ISAs) and Contractual Clauses

Sharing information about an individual between partner organisations is vital to the provision of co-ordinated and seamless services. The need for shared information standards and robust information security to support the implementation of joint working arrangements is recognised.

Establishing an information agreement in itself does not provide a lawful basis for sharing personal confidential information. NHS Kernow, and its partner organisations, will therefore ensure any such ISAs produced have "rules" which are clearly understood and legal requirements and guidance is met.

NHS Kernow typically relies on the NHS standard contract which incorporates information governance responsibilities - General Conditions section 21 applies. Should other contract forms be used, the appropriate information and data protection clauses shall be inserted. Such clauses are an essential element of ensuring the organisations we commission services from are meeting the legal requirements in respect of information governance.

Should NHS Kernow ever find itself in the situation of wishing to transfer personal information to countries outside of the European Economic Area (EEA):

- The Caldicott Guardian will be informed and a log of such transfers be maintained
- Explicit consent will be sought from the individual
- The addition of binding corporate rules will be incorporated into the appropriate contract documentation

3.7 Freedom of Information (FOI)

NHS Kernow will ensure compliance with the Freedom of Information Act 2000 by:

- Maintaining a publication scheme on the CCG's website, containing a range of business information about the organisation
- Managing all requests for information and co-ordinating the responses in accordance with the requirements of the FOI Act.

3.8 Regulatory Framework

Information governance encompasses many local, national and legal regulations. The outline, which is not an exhaustive list, is given in **Appendix 3**.

3.9 NHS Kernow Related Policy Documents

To complement the regulatory framework, NHS Kernow relies on numerous policies, procedures and plans. These are given in **Appendix 4**. Once again, the list is not exhaustive.

Support, guidance and training is always available through the Information Governance team who can be contacted on kccg.corporategovernance@nhs.net.

4. Responsibilities

The roles and committees which ensure information is dealt with legally, securely, efficiently and effectively are given below. Together with the policies and procedures outlined in Appendix 4, these combine to give rise to NHS Kernow's Information Governance Management Framework.

4.1 Chief Officer

The Chief Officer has overall accountability for IG and is required to provide assurance, through the Governance Statement within the annual report, that all risks relating to information are effectively managed.

4.2 Senior Information Risk Owner (SIRO)

The Chief Operating Officer is the SIRO and has organisational responsibility for all aspects of risks associated with information governance, including those relating to confidentiality and data protection. More detail is available at **Appendix 1**.

4.3 Caldicott Guardian

The Chief Nursing Officer is the Caldicott Guardian and is responsible for:

- The protection and confidentiality of patient-identifiable information, both within the organisation and when sharing it with other organisations
- Agreeing levels of access to the organisations patient information systems

4.4 Data Protection Officer (DPO)

The Deputy Director of Corporate Governance is the named Data Protection Officer and Chairs the Information Governance Sub-Committee. Whilst being line managed by the Chief Operating Officer, the role has a direct right of access on relevant matters and to escalate serious concerns or issues to members of the Governing Body.

An outline of the DPO’s responsibilities is available at **Appendix 2**.

4.5 The Head of Information Governance

The Head of IG is the senior manager responsible for IG and will manage the work of the IG Sub Committee and DSP Toolkit. They are also responsible for:

- Co-ordinating the production of the annual audit and improvement plan
- Activities as detailed in the improvement plan
- Operational support including management of IG training, query resolution, incident support, legal compliance requirements
- Routine performance monitoring to the Workforce Committee and Governing Body, when necessary

4.6 Information Security Manager

The Information Security Manager provides information security (including cyber security) expertise. The role is provided by Cornwall IT Services (CITS) and is hosted by Royal Cornwall Hospital Trust. The Information Security Manager provides advice on all aspects of information security and risk management, utilising either their own expertise or external advice. The role provides advice and guidance on meeting the IT aspects of the DSP Toolkit and is a member of the Information Governance Sub-Committee.

4.7 Information Asset Owners (IAOs)

Information Asset Owners (IAOs) are senior individuals involved in the running of their respective business functions and are directly accountable to the SIRO. IAOs must provide assurance that information risk is being managed effectively in respect of the information assets they are responsible for and that any new changes introduced to their business processes and systems follow the data security by design and default requirements as well as the production of data protection impact assessments (DPIAs).

4.8 All Managers and Employees

The IG agenda is clearly wide with some impact on every member of staff. For an organisation to ensure an appropriate level of compliance, many individuals and groups across NHS Kernow are required to have specific responsibilities. These will be outlined in the IG Policy. The scope of this strategy is to set out the structure for IG management and activity, ensuring that NHS Kernow addresses all areas effectively.

It is expected that all staff must abide by the Confidentiality: NHS Code of Practice and clauses within their employment contract.

4.9 Information Governance Sub-Committee (IGSC)

The IGSC is a formal sub-committee named in NHS Kernow’s Constitution. It is chaired by the Deputy Director of Corporate Governance who is also the Data Protection Officer.

5. IG Organisational Objectives for 2019/20

This strategy sets out the approach to be taken within NHS Kernow to provide a robust IG framework for the current and future management of information.

The IG Strategy cannot be seen in isolation as information plays a key part in corporate governance, strategic risk, clinical governance, service planning, informatics, performance and business management. The strategy is therefore closely linked with these functions.

The success factor for effective IG will be to continue to develop a staff culture of good management of information, information systems and records. This will primarily be achieved by an effective programme of awareness and training identified and implemented within NHS Kernow.

The high level IG organisational objectives that NHS Kernow is seeking to achieve are given below. Further detail is available as part of the Information Governance Sub-Committee and Workforce Committee reports.

i. Maintain clear lines of accountability and individual responsibility for IG, ensuring there are appropriate policies and procedures in place for the effective management of information

ii. Ensure there is sufficient provision of training, awareness and supervision to ensure all employees operate within information governance requirements

iii. Incorporate IG into formal NHS Kernow monitoring arrangements to ensure adherence to expected standards, any risks are highlighted and/or areas of non-compliance acted upon

iv. Ensure existing electronic systems and any new systems, or processes where appropriate, comply with IG requirements with documentation available to evidence compliance

v. Continue to develop formal and effective communication channels for both staff and the public regarding IG

vi. The timely implementation of all new CARECert cyber security requirements

vii. Ensure the new requirements introduced in 2018 by the GDPR and the new Data Protection Act are implemented which includes:

    - Revised consent arrangements, explanations regarding the rights of individuals plus clear information regarding how information is recorded and shared within NHS Kernow and how concerns can be raised
    - Building the new legal requirement of data protection by design and default into all appropriate policies and procedures
    - The regular use of data protection impact assessments – including notifying the ICO of any systems and processes with high data protection risks that cannot be mitigated
    - Abiding by shorter subject access request timescales
    - Revised breach reporting procedures to the ICO

viii. Introduce greater rigour in respect of:

    - Retention and disposal of records
    - Use of emails – with a particular emphasis on deleting and filing appropriately

- P-file arrangements
- Service level agreements, information sharing agreements and contracts which are not based on the NHS standard contract

ix. Ensure robust implementation plans are developed for any additional 2019/20 DSPT requirements

6. Training and Awareness Requirements

IG training is a mandatory requirement of induction training. All new staff will receive instruction to complete e-learning modules within the Data Security and Awareness (DSA) e-learning programme.

All staff are required to complete annual DSA training and the IG training needs analysis identifies any additional training required for key roles such as information asset owners, the SIRO, Caldicott Guardian, Data Protection Officer, etc.

7. Monitoring, Compliance and Audit

NHS Kernow will monitor this Strategy, related policy documents and guidance using the self-assessment of the Data Security and Protection (DSP) Toolkit requirements. It is expected that each year all mandatory requirements shall be met.

The CCG's Internal Auditors also audit NHS Kernow's compliance with the Toolkit. Their findings are formally reported to the members of the Executive Team, the Information Governance Sub-Committee, the Workforce Committee and the Audit Committee.

The IGSC will implement the information governance requirements and standards using action plans and regular updates. NHS Kernow will also work with Cornwall Information Technology Services (CITS), Cornwall Partnership Foundation NHS Trust (CPFT) and other local health and social care services to implement this IG strategy, as appropriate.

Regular reports, work plans and associated actions plans are presented to Workforce Committee for discussion and approval.

8. Update and Review

This Strategy will be reviewed every 3 years but the organisational objectives will be revisited on an annual basis.

Appendix 1: Senior Information Risk Owner Responsibilities

SIRO responsibilities include:

- Take ownership of the organisation's Information Governance Policy and risk assessment process
- Act as advocate for information risk for the Governing Body and provide written advice to the accountable officer (if this is not the SIRO) on the content of the Annual Governance Statement in regard to information risk
- Understand how the strategic business goals of the organisation may be impacted by information risks
- Oversee the implementation of the IT Security Policy within the existing IG framework
- Take ownership of risk assessment processes for information risk, including the review of the annual information risk assessment to support and inform the Annual Governance Statement
- Ensure that identified information security threats are followed up and incidents managed
- Review and agree action in respect of identified information risks
- Ensure that NHS Kernow's approach to information risk is effective in terms of resources, commitment and execution and that this is communicated to all staff
- Provide a focal point for the resolution and/or discussion of information risk issues
- Ensure the Governing Body is adequately briefed on information risk issues
- Be required to undertake and pass strategic risk management training at least annually
- Ensure sufficient resources are provided to support Information Governance
- Define NHS Kernow's policy in respect of IG and records management, taking into account legal and NHS requirements

Appendix 2: Data Protection Officer Responsibilities

- The Data Protection officer (DPO) is responsible for monitoring compliance with data protection law and ensuring data practices internally comply with applicable requirements. The DPO, supported by the Head of Information Governance, is also responsible for staff training, data protection impact assessments and internal audits. They serve as the primary contact for the Information Commissioners Office (ICO) and for individuals whose data is processed by NHS Kernow (or their data controllers).

- The DPO shall report to the SIRO on any relevant matters and escalate serious concerns or issues to the Governing Body.
- The DPO is an essential role in facilitating 'accountability', including NHS Kernow's ability to demonstrate compliance with the GDPR and the DPA2018. In particular, the post-holder must ensure:
- The report to the highest relevant management level of the organisation.
- They are able to operate independently, and cannot be dismissed or penalised for performing their task. (However they can still be dismissed or penalised for misconduct or negligence relating to their task.)
- They are provided with adequate resources to enable them to meet their obligations including financial and human resources and is supported in maintaining their expertise
- They have proven expert knowledge of data protection law and practices, the ability to perform the tasks specified in the GDPR, and sufficient understanding of NHS Kernow's business and processing
- That information governance and related policies address:
- Organisational accountability
- DPO reporting arrangements
- Timely involvement of the DPO in all data protection issues
- Compliance assurance – including privacy by design and default
- Advising on where data protection impacts assessments are required
- The DPO's role in incident management
- Where the DPO fulfils other roles there is no conflict of interest
- That the details of the DPO are published on NHS Kernow's website as part of its transparency and IG information

Appendix 3: Regulatory Framework

Information Governance currently encompasses the following local, national and legal regulations:

- Data Protection Act 2018
- General Data Protection Regulations
- Freedom of Information Act 2000
- Human Rights Act 1998
- Access to Health Records Act 1990
- Computer Misuse Act 1990
- Confidentiality: NHS Code of Practice
- BS ISO/IEC 27000 series of Information Security Standards
- Caldicott Guardian Manual and Reviews 2006 and 2013
- Common Law Duty of Confidentiality
- Records Management: NHS Code of Practice
- Health and Social Care (Safety and Quality) Act 2015
- Access to Medical Records Act 1988
- Copyright, Designs and Patents Act 1988
- Copyright (Computer Programs) Regulations 1992
- Crime and Disorder Act 1998
- Electronic Communications Act 2000
- Environmental Information Regulations 2004
- Health and Social Care Act 2012 & Health and Social Care (Safety and Quality) Act 2015
- Information Security Management: NHS Code of Practice
- Regulation of Investigatory Powers Act 2000 (and Lawful Business Practice Regulations 2000)
- Public Interest Disclosure Act 1998
- NHS Trusts and Primary Care Trusts (Sexually Transmitted Diseases) Directions 2000
- Abortion Regulations 1991
- Mental Capacity Act 2005
- NHS Care Records Guarantee
- NHS Constitution
- Public Records Act 1958
- Regulations under the Health and Safety at Work Act 1974

- Re-Use of Public Sector Information Regulations 2005
- Data Security and Protection Toolkit

The above list is not exhaustive.

Appendix 4: NHS Kernow Related Policy Documents

This Strategy should be read in conjunction with the following policies and documents:

- Information Governance Policy
- Data Protection Policy
- Records Management Code of Practice
- Cornwall Partnership Foundation Trust - Subject Access Request Policy
- Pseudonymisation Policy
- IT Security Policy and all linked policies
- Integrated Identity Management Policy
- Email Policy
- Disciplinary Policy and procedures
- Acceptable Use Policy
- Safe Haven Policy
- Data Quality Policy
- Business Continuity Plans
- Risk Management Strategy and Policy
- Incident Management Policy
- Freedom of Information Policy
- NHS Kernow’s Privacy Notice
- Home Working Policy
- Information Sharing Protocols and Agreements
- Serious Incident Policy
- Confidentiality Code of Conduct for Employees
- NHS Kernow’s Information Governance Handbook

This list is not exhaustive.

Appendix 5: Equality Impact Assessment

A generic equality impact assessment (EIA) has been produced. It covers all the data protection and information governance related policies named above. To see the full version of the EIA please refer to one of those policies, all of which are available on NHS Kernow’s document library available at: http://intranet-kccg.cornwall.nhs.uk/get-information/documents-library/ .