NHS
Kernow
Clinical Commissioning Group

Information Governance Policy

Date approved: 19 March 2019

NHS
Kernow
Clinical Commissioning Group

Document control sheet

Title of document:	Information Governance Policy
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
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
2.0	February 2019	Jodeigh Phelps	Minor amends following staff feedback
2.1	February 2019	Trudy Corsellis	EIA added

Contents

1. Introduction

Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources. It plays a key part in clinical governance, service planning, delivery and performance management.

It is of paramount importance to ensure that information is efficiently and securely managed and that appropriate policies, procedures and management accountability and structures provide a robust governance framework for information management.

Information governance encompasses the following areas:

- Data protection, confidentiality and compliance with legislation
- The Caldicott principles
- Information security and cyber security
- Records management and data quality
- Business operations and management
- Business intelligence – including ‘big data’, procurement and finance

2. Purpose

The purpose of this policy is to describe a system that ensures NHS Kernow meets its responsibilities for the management of its information assets and resources. It is essential that NHS Kernow ensures its information is:

- Held securely and confidentially
- Obtained fairly and efficiently
- Recorded accurately and reliably
- Used effectively and ethically
- Shared proportionately and lawfully, and,
- Disposed of effectively and securely

3. Principles

NHS Kernow recognises the statutory and professional need for an appropriate balance between openness and confidentiality in the management and use of information. It fully supports the principles and requirements of information governance and recognises its responsibility and public accountability, placing importance on the confidentiality and security arrangements to safeguard personal information about patients and staff. NHS Kernow also recognises the need to share patient information with other health organisations and agencies in a controlled manner consistent with the interests of the patient and in some circumstances, the public interest.

NHS Kernow believes that accurate, timely and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of all managers and clinicians to ensure and promote the quality of information and to use information in decision making processes.

There are 5 key interlinked strands to the Information Governance (IG) policy:

i. Openness
ii. Legal compliance
iii. Information security
iv. Quality assurance
v. Records management

3.1. Openness

- Non confidential information about NHS Kernow and its services should be available to the public through a variety of media.
- NHS Kernow will establish and maintain policies to ensure compliance with the Freedom of Information Act.
- NHS Kernow will undertake or commission annual assessments and audits of its Freedom of Information policies and arrangements.
- Patients should have ready access to information relating to their own health care, their options for treatment and their rights as patients in line with the NHS Constitution and Data Protection Act.
- NHS Kernow will have clear procedures and arrangements for liaison with the press and broadcasting media as indicated within the Media Handling Policy.
- NHS Kernow will have clear procedures and arrangements for handling queries from patients and the public.

3.2. Legal Compliance

- NHS Kernow regards all identifiable personal information relating to patients as confidential.
- NHS Kernow will undertake or commission annual assessments and audits of its compliance with legal requirements.
- NHS Kernow regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise.

- NHS Kernow will establish and maintain policies to ensure compliance with the Data Protection Act, Freedom of Information, Human Rights Act and the common law duty of confidentiality.
- NHS Kernow will establish and maintain policies for the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation (e.g. Health and Social Care Act, Crime and Disorder Act, Protection of Children Act).

3.3. Information and Cyber Security

- NHS Kernow will establish and maintain policies for the effective and secure management of its information assets and resources.
- NHS Kernow will undertake or commission annual assessments and audits of its information and IT security arrangements.
- NHS Kernow will undertake risk assessments to determine appropriate security controls are in place for existing or potential information systems
- NHS Kernow will promote effective confidentiality and security practice to its staff through policies, procedures, induction and training.
- NHS Kernow will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.
- NHS Kernow will use BS ISO/IEC 27001: 2005, BS ISO/IEC 27002: 2005 BS 7799-2: 2005 as the basis of its information security management arrangements.

3.4. Quality Assurance

- NHS Kernow will establish and maintain policies and procedures for information quality assurance.
- NHS Kernow will undertake or commission annual assessments and audits of its information quality.
- Managers are expected to take ownership of, and seek to improve, the quality of information within their services.
- Wherever possible, information quality should be assured at the point of collection.
- Data standards will be set through clear and consistent definitions of data items, in accordance with national standards.
- NHS Kernow will promote information quality and effective records managements through policies, procedures, induction and training.

3.5. Records Management

- NHS Kernow will establish and maintain policies and procedures for the effective management of records
- NHS Kernow will undertake or commission annual assessments and audits of its records management
- Managers are expected to ensure effective records management within their service areas
- NHS Kernow will promote records management through policies, procedures and training
- NHS Kernow will use Records Management: NHS Code of Practice as its standard for records management

4. Responsibilities

This document is relevant to all staff, volunteers, contractors and third parties who work on behalf of NHS Kernow.

It is the role of NHS Kernow's Governing Body to define its policy in respect of information governance, taking into account legal and NHS requirements. The Governing Body is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

All information used in the NHS is subject to handling by individuals and it is necessary for these individuals to be clear about their responsibilities. NHS Kernow must ensure support and appropriate education and training are provided for all staff.

To manage its obligations NHS Kernow will issue and support standards, policies and procedures ensuring information is held, obtained, recorded, used and shared correctly.

The Chief Officer, as Accountable Officer for NHS Kernow, has overall accountability for IG in NHS Kernow and is required to provide assurance, through the Statement of Internal Control (SIC), that all risks relating to information are effectively managed.

The nominated Senior Information Risk Owner (SIRO) will act as an advocate for information risk at Governing Body level and via any internal discussions. The SIRO, who is also the Chief Operating Officer, is responsible for providing written advice to the Accountable Officer on the content of the annual SIC with regard to information risk.

The Information Governance Sub Committee (IGSC) is responsible for overseeing day to day IG issues. It ensures the annual IG work plan is maintained and monitored against the requirements of the Data Security and Protection (DSP) Toolkit through the co-ordination of different work streams such as developing and maintaining policies, strategies, structures, procedures and guidance and raising awareness of information governance. The Committee also ensures annual assessments and submissions of the toolkit are undertaken. The IGSC is accountable to the Workforce Committee meeting. It is chaired by the Deputy Director of Corporate Governance who also assumes the Data Protection Officer role for the organisation.

The Head of IG is responsible for raising awareness throughout NHS Kernow with regard to the requirements of the DSP Toolkit, for ensuring mandatory standards are met and providing support to NHS Kernow staff and work streams.

Managers within NHS Kernow are responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance.

All staff, whether permanent, temporary or contracted and contractors are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with these on a day to day basis.

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

Greater detail regarding the roles of the SIRO, Data Protection Officer and the Information Asset Owners can be found at

5. Related Policy Documents

There are a wide range of policy documents which support this policy which can be found in Appendix 3.

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 and Audit

NHS Kernow will monitor this policy and related strategies, policies 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 with their findings being formally reported to members of the Executive Team and the Audit Committee.

The IGSC will implement the information governance requirements and standards using action plans and regular updates.

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

8. Legal Framework

There are a number of legal obligations placed upon NHS Kernow for the use and security of personally identifiable information these can be found in Appendix 3.

9. Regulatory Framework

In relation to the legislation outlined in Appendix 2, the NHS has set out and mandated a number of elements of regulations that constitute "information governance" through a national programme.

The DSP Toolkit, which replaced the IG Toolkit in 2018, requires organisations to assess their performance against the National Data Guardian's ten data security standards. Compliance is based on achieving and being able to evidence performance against series of mandatory assertions. The ten data security standards sit within three leadership obligation domains and cover the following areas:

Leadership obligation 1 – People:

- Data Security Standard 1 - Personal Confidential Data
- Data Security Standard 2 - Understand Your Responsibilities
- Data Security Standard 3 – Training

Leadership obligation 2 – Process:

- Data Security Standard 4 - Managing Data Access
- Data Security Standard 5 - Process Reviews
- Data Security Standard 6 - Responding to Incidents
- Data Security Standard 7 - Continuity Planning

Leadership obligation 3 – Technology

- Data Security Standard 8 - Managing Unsupported Systems
- Data Security Standard 9 - IT Protection
- Data Security Standard 10 - Accountable Suppliers

Additional regulatory frameworks are:

- The Caldicott Guardian Manual 2010, based upon a report by Dame Caldicott in 1997. Subsequent Caldicott reviews and report will also be taken into account.
- ISO/IEC 27001: 2005, BS ISO/IEC 27002: 2005 BS 7799-2: 2005 is the Standard for Information Security Management which was originally mandated for the NHS in 2001.
- Information Quality Assurance
- Confidentiality: NHS Code of Practice November 2003
- NHS Guidance on Consent to Treatment
- Records Management: NHS Code of Practice 2016

10. Monitoring Compliance and Effectiveness

Compliance with this policy will be monitored through the Information Governance Sub-Committee and the Workforce Committee. 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 policy, as appropriate.

11. Update and Review

This policy will typically be reviewed in 3 years but can, should legislation change, be re-considered sooner, if needed.

Appendix 1: The Ten National Data Security Standards

Leadership Obligation 1 - People: Ensure staff are equipped to handle information respectfully and safely, according to the Caldicott principles.

1. Data Security Standard 1 - Personal Confidential Data

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.

2. Data Security Standard 2 - Understand Your Responsibilities

All staff understand their responsibilities under the National Data Guardian's 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 behaviour and the implications for their employment. They are made aware that their usage of IT systems is logged and attributable to them personally. Insecure behaviours are reported without fear of recrimination and procedures which prompt insecure workarounds are reported, with action taken.

3. Data Security Standard 3 – Training

All staff complete appropriate annual data security training and pass a mandatory test, provided linked to the revised Information Governance Toolkit.

All staff complete an annual security module, linked to 'CareCERT Assurance'. The course 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.

Leadership Obligation 2 – Process: Ensure the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses

4. Data Security Standard 4 - Managing Data Access

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 should 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 (e.g. sign in sheets, CCTV, correlation with other systems, shift rosters etc.).

5. Data Security Standard 5 - Process Reviews

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 behaviours 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.

6. Data Security Standard 6 - Responding to Incidents

Cyber-attacks against services are identified and resisted and CareCERT 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. [The 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.

7. Data Security Standard 7 - Continuity Planning

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 [CareCERT Assurance]. 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.

Leadership Obligation 3 – Technology: Ensure technology is secure and up-to-date

8. Data Security Standard 8 - Managing Unsupported Systems

No unsupported operating systems, software or internet browsers are used within the IT estate.
Guidance and support is available from CareCERT Assurance 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.

9. Data Security Standard 9 - IT Protection

A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.

[CareCERT Assurance] assists risk owners in understanding which national frameworks do what, and which components are intended to achieve which outcomes. 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.

10. Data Security Standard 10 - Accountable Suppliers

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

IT suppliers understand their obligations as data processors under the GDPR, 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 2: Legal and 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 3: NHS Kernow Related Policy Documents

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

- Information Governance Strategy
- 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 4: Equality Impact Assessment

Name of policy to be assessed	Policies relating to Data Protection and Information Governance. Including: Confidentiality Code of Conduct, Pseudonymisation Policy, Data Protection Policy, Data Quality Policy, Safe Haven Policy, Information Governance Policy, Information Governance Strategy, Records Management Policy.		
Section	Information Governance	**Date of Assessment**	12/02/2019
Officer responsible for the assessment	Data Protection Officer	**Is this a new or existing policy?**	Existing
1. Describe the aims, objectives and purpose of the policy.			
The policies identified above outline how NHS Kernow will meet its legal obligations and NHS requirements and will provide documented evidence of continued commitment to the securing of both corporate and person identifiable information and processes that comply with confidentiality, General Data Protection Regulations (GDPR) and the Data Protection Act 2018 (DPA 2018). The policies provide guidance to staff to ensure the consideration of legal responsibilities and the privacy of all individuals when processing data. The requirements within the Policies are primarily based upon the DPA 2018 which is the key piece of legislation covering security and confidentiality of personal information.			
2. Are there any associated objectives of the policy? Please explain.			
Associated objectives are NHS Kernow compliance with the Data Security Protection Toolkit, the attainment of the commitments in the NHS Constitution, Data Protection Act, General Data Protection Regulations, Human Rights Act, Care Records Guarantee and information security standards.			

3. Who is intended to benefit from this policy, and in what way?
NHS Kernow staff will benefit from the implementation of robust information security controls to protect them and the information processed as part of the services provided. Patients will benefit from the provision and availability of high quality information and data which meets the Data Protection Act, Freedom of Information Act, Human Rights Act and Records Management: NHS Code of Practice.
4. What outcomes are wanted from this policy?
That the information processed by NHS Kernow and its staff, in all formats, is of a high quality and is protected to the highest possible standards and available quickly, processed in line with legislation and all confidentiality requirements, Government standards and NHS Digital requirements.
5. What factors/ forces could contribute/ detract from the outcomes?
Staff awareness of the content of the policies and staff completing Information Governance training will contribute to information governance practices
6. Who are the main stakeholders in relation to the policy?
The main stakeholders are NHS Kernow Governing Body and its constitutional committees in order to meet its responsibilities. In addition, the Data Protection Officer, the Head of Information Governance, all staff as well as the Information Governance Sub Committee have key operating functions and responsibilities for implementing information governance throughout NHS Kernow. These policies are also important for Individuals in the community.
7. Who implements the policy, and who is responsible for the policy?
The Data protection Officer, Head of Information Governance and the Information Governance Sub Committee providing assurance and escalation to the Workforce Committee.

8. What is the impact on people from Black and Minority Ethnic Groups (BME) (positive or negative)?
Consider relevance to eliminating unlawful discrimination, promoting equality of opportunity and promoting good race relations between people of different racial groups. Issues to consider include people's race, colour and nationality, Gypsy, Roma, Traveller communities, employment issues relating to refugees, asylum seekers, ethnic minorities, language barriers, providing translation and interpreting services, cultural issues and customs, access to services.
The policies reflect the current national guidance and best practice and is designed to protect the rights of all, irrespective of racial groups. The standards of Information Governance, documents referenced in the policies and training will take account of the need to provide data in required formats or languages to ensure accessibility to all to ensure correct use and handling. The new data protection framework protects personal data ‘revealing racial or ethnic origin’ as a ‘special category of data’ and processing of it as ‘sensitive processing’.
How will any negative impact be mitigated?
A requirement of the information governance programme specifically relates to the provision of information in differing formats and evidence is collated to support this.
9. What is the differential impact for male or female people (positive or negative)?
Consider what issues there are for men and women e.g. responsibilities for dependants, issues for carers, access to training and employment issues, attitudes towards accessing healthcare.
The policies reflect the current national guidance and best practice and is designed to protect the rights of all, irrespective of sex.
How will any negative impact be mitigated?
There are no sections within the policies that distinguish between sexes.
10. What is the differential impact on disabled people (positive or negative)?
Consider what issues there are around each of the disabilities e.g. access to building and services, how we provide

services and the way we do this, producing information in alternative formats and employment issues. Consider the requirements of the NHS Accessible Information Standard. Consider attitudinal, physical and social barriers. This can include physical disability, learning disability, people with long term conditions, communication needs arising from a disability.
The policies outline the importance of confidentiality and there should therefore be a positive impact on individuals with a disability as this information should not be shared without the express permission of the individual. The new data protection framework protects personal data ‘concerning health’ as a ‘special category of data’ and processing of it as ‘sensitive processing’. Additional safeguards are provided throughout the new data protection policies. This may have an impact on those not capable of, or with varying capacity to, give consent, which is ‘freely given, specific, informed and unambiguous’, such as people with a learning disability.
How will any negative impact be mitigated?
Adjustments will be made for any member of staff with a disability requiring assistance to enable them to understand how to implement Data Protection to the necessary standards. The standards of Information Governance, documents referenced in the policies and training will take account of the need to provide data in any required format or language to ensure accessibility to all to ensure correct use and handling of corporate and personal information.
11. What is the differential impact on sexual orientation?
Consider what issues there are for the employment process and training and differential health outcomes amongst lesbian and gay people. Also consider provision of services for e.g. older and younger people from lesbian, gay, bi-sexual. Consider heterosexual people as well as lesbian, gay and bisexual people.
The policies support the protection of personal data, and whilst there may be a requirement to collect personal sensitive data, this should not then be shared inappropriately therefore the sexual orientation of the individual should be protected. The new data protection framework protects personal data ‘concerning sex life and sexual orientation’ as a ‘special category of data’ and processing of it as ‘sensitive processing’. The existing condition for processing personal data ‘for the purpose of identifying or keeping under review the existence or absence of equality of opportunity’ is newly expanded to include personal data concerning an individual’s sexual orientation.

How will any negative impact be mitigated?
There are no sections within the policies that will negatively impact an individual due to their sexual orientation.
12. What is the differential impact on people of different ages (positive or negative)?
Consider what issues there are for the employment process and training. Some of our services impact on our community in relation to age e.g. how do we engage with older and younger people about access to our services? Consider safeguarding, consent and child welfare.
The policies support the protection of personal data, and whilst there may be a requirement to collect personal sensitive data, this should not then be shared inappropriately therefore the age of the individual should be protected.
How will any negative impact be mitigated?
The policies, their content and implementation will not negatively impact those of differing ages.
13. What differential impact will there be due religion or belief (positive or negative)?
Consider what issues there are for the employment process and training. Also consider the likely impact around the way services are provided e.g. dietary issues, religious holidays, days associated with religious observance, cultural issues and customs, places to worship.
The policies support the protection of personal data, and whilst there may be a requirement to collect personal sensitive data, this should not then be shared inappropriately therefore the impact on those with a religious affiliation or belief should be positive. The new data protection framework protects personal data regarding ‘religious or philosophical beliefs’ as a ‘special category of data’ and processing of it as ‘sensitive processing’.
How will any negative impact be mitigated?
The policies, their content and implementation will not negatively impact those with a religious affiliation or belief.

14. What is the impact on marriage of civil partnership (positive or negative)? NB: this is particularly relevant for employment policies
This characteristic is relevant in law only to employment, however, NHS Kernow will strive to consider this characteristic in all aspects of its work. Consider what issues there may be for someone who is married or in a civil partnership. Are they likely to be different to those faced by a single person? What, if any are the likely implications for employment and does it differ according to marital status?
The policies support the protection of personal data, and whilst there may be a requirement to collect personal sensitive data, this should not then be shared inappropriately therefore the impact on marriage or civil partnership status of the individual should be positive.
How will any negative be mitigated?
The policies do not negatively impact those who are married or in a civil partnerships.
15. What is the differential impact who have gone through or are going through gender reassignment, or who identify as transgender?
Consider what issues there are for people who have been through or a going through transition from one sex to another. How is this going to affect their access to services and their treatment when receiving NHS care? What are the likely implications for employment of a transgender person? This can include issues such as privacy of data and harassment.
The policies outline the legal basis for collecting sensitive information, limits how and when it may be shared and when it should be destroyed. They also outline the expectations of staff to maintain confidentiality.
How will any negative impact be mitigated?
No negative impact has been identified for those who gone through or are going through gender reassignment, or who identify as transgender.
16. What is the differential impact on people who are pregnant or breast feeding mothers, or those on maternity leave?

This characteristic applies to pregnant and breast feeding mothers with babies of up to six months, in employment and when accessing services. When developing a policy or services consider how a nursing mother will be able to nurse her baby in a particular facility and what staff may need to do to enable the baby to be nursed. Consider working arrangements, part-time working, infant caring responsibilities.
The Data Protection Policy includes the requirement for training of all staff to Information Governance standards. Information Governance training and all documentation will remain available to staff on maternity leave or on return from maternity leave. Knowledge and skills following maternity leave will be updated using the mandatory training requirements. Staff are required to maintain the code of confidentiality and therefore under these policies are expected not to share information relating to pregnancy or maternity leave without the consent of the individual. The new data protection framework protects personal data ‘concerning health’ as a ‘special category of data’ and processing of it as ‘sensitive processing’. Additional safeguards are provided throughout the new data protection framework.
How will any negative impact be mitigated?
There is nothing in the policies which would negatively impact those who are pregnant or on maternity leave.
17. Other identified groups:
Consider carers, veterans, different socio-economic groups, people living in poverty, area inequality, income, resident status (migrants), people who are homeless, long-term unemployed, people who are geographically isolated, people who misuse drugs, those who are in stigmatised occupations, people with limited family or social networks, and other groups experiencing disadvantage and barriers to access.
No negative impact has been identified for these groups. However there may be a positive impact in that the policies set out how personal information should be handled and how long it should be retained. The policies also set out the requirements for staff to maintain a code of confidentiality. We also acknowledge and will work with individuals who, in order to exercise their rights, may need to speak rather than write to the CCG formally.
How will any negative impact be mitigated?
No negative impact has been identified.

18. How have the Core Human Rights Values been considered in the formulation of this policy/strategy? If they haven’t please reconsider the document and amend to incorporate these values.

- **Fairness;**
- **Respect;**
- **Equality;**
- **Dignity;**
- **Autonomy**

The requirements and principles of the Data Protection Act, which is linked to the Human Rights Act, have been taken into account when writing these policies, including the individual rights of data subjects. Fairness in informing individuals of the uses to be made of their data in a fair processing notice have been produced, respect for privacy, dignity and choice have been written into all Information Governance Policies.

19. Which of the Human Rights Articles does this document impact?

The right:	**Yes / No:**
• To life	No
• Not to be tortured or treated in an inhuman or degrading way	No
• To liberty and security	No
• To a fair trial	No
• To respect for home and family life, and correspondence	Yes
• To freedom of thought, conscience and religion	No
• To freedom of expression	No
• To freedom of assembly and association	No
• To marry and found a family	No
• Not to be discriminated against in relation to the enjoyment of any of the rights contained in the European Convention	Yes
• To peaceful enjoyment of possessions	No

a) What existing evidence (either presumed or otherwise) do you have for this?

All documentation produced as part of the Information Governance programme of work has taken account of the Human Rights Act and this has been referenced where necessary.

20. How will you ensure that those responsible for implementing the Policy are aware of the Human Rights implications and equipped to deal with them?

The Act has been referenced within the policies and procedures produced and any monitoring of compliance will include the awareness of patients and staff having a right to privacy, dignity, respect and choice.

21. Describe how the policy contributes towards eliminating discrimination, harassment and victimisation.

By setting out how personal information will be handled and stored and the expectations of staff in these matters information should not be held for the purposes of discrimination, harassment and victimisation. The policies also allow for individuals to rectify information where it is believed to be held incorrectly.

22. Describe how the policy contributes towards advancing equality of opportunity.

The policies describe how and when information should be collected, stored and for how long. This should mean that the organisation does not hold inappropriate information about people without a considered business reason. The code of confidentially sets out how staff should treat information in their care.

23. Describe how the policy contributes towards promoting good relations between people with protected characteristics.

The policies set out how information both personal and corporate will be managed by the organisation. If the policies are followed then those individuals with protected characteristics should be positively impacted as sensitive data can only be collected within a lawful basis and then must be kept confidential.

24. If the differential impacts identified are positive, explain how this policy is legitimate positive action and will improve outcomes, services or the working environment for that group of people.

The policies can be provided in multiple formats if necessary.

25. Explain what amendments have been made to the policy or mitigating actions have been taken, and when they were made.
Not applicable
26. If the negative impacts identified have been unable to be mitigated through amendment to the policy or mitigating actions, explain what your next steps are.
Not applicable.