Northumbria Healthcare
NHS Foundation Trust

IG 01

Northumbria Healthcare NHS Foundation Trust

Information Governance Policies

Information Governance Policy

Version	04
Sub Committee & approval date	IG Group 28/02/2022
Date ratified by Assurance Committee	19/04/2022
Name of policy author	Tracey Best Head of Quality & Performance
Date issued	22/04/2022
Review Date	22/04/2025
Target audience	All Trust staff, Agency staff & Volunteers

This Policy has been Impact Assessed against the Equality Act 2010

History of previous versions of this document:

Date Approved by Sub Committee / Group	Date Ratified by Assurance Committee	Version	Issue Date	Review Date	Policy Author
25/03/2019	14/05/2019	3	16/05/2019	16/05/2022	Jonathan Walmsley, Information Governance Manager
12/03/2018	29/05/2018	2.1	30/05/2018	15/12/2019	Jonathan Walmsley, Information Governance Lead
03/11/2015	10/11/2015	2	15/12/2015	15/12/2018	Tracey Best, Information Governance Manager
19/01/2012	04/09/2012	1	14/09/2012	14/09/2015	Tracey Best, Information Governance Manager

Statement of changes made: 03

Version	Date	Description
04	15/02/2021	Policy has had a substantial review. Duties for accountability and governance have been updated accordingly including definition of terms used/ associated documentation.

Contents

1. Operational Summary

Policy Aim

This policy has been developed to provide guidance, assistance and awareness for Northumbria Healthcare NHS Foundation Trust staff, agency staff and volunteers to ensure a standard, consistent compliance to Information Governance (IG) and any issues which may arise.

This policy sets out to further develop and implement a change in culture towards IG by all staff. IG is a key component of performance management, i.e. it is central to the working practices of all staff, of all grades and roles, permanent or temporary, working within the Trust. Through the implementation of the IG Policy, the Trust will:

- Establish robust Information Governance processes conforming to the law, NHS and Department of Health standards
- Ensure that all policies and procedures relating to the processing of personal information, including handling and holding personal and Trust corporate information are legal and conform to best and/or recommended practice
- Provide clear advice and guidance to staff and ensure that they understand and apply the principles of IG to their working practices in relation to protecting the confidentiality and security of personal information
- Ensure that procedures are reviewed on a regular basis to monitor their effectiveness in order that improvements or deficiencies in information handling standards can be recognised and addressed
- Work to embed an IG culture in the Trust through increasing awareness
- Maintain a clear reporting structure and ensure that through management action and training all staff understand the IG requirements
- Undertake regular reviews and audits of how information is recorded, held and used.
- Ensure that there are robust procedures for notifying and learning from IG breaches and incidents in line with the Incident Reporting Procedure

Policy Summary

The purpose of this policy is to ensure the Trust complies with NHS requirements and legislation along with highlighting roles and responsibilities for accountability and governance.

This policy applies to those members of staff that are employed by the Trust, both permanent and non-permanent, and for whom the Trust has legal responsibility.

What it means for staff

Policy Authors – are responsible for ensuring the policy is regularly reviewed and kept up to date.

Managers/Supervisors – are responsible for ensuring adequate dissemination and implementation of policies.

All Trust Employees, Agency Staff and Volunteers – are responsible for reading the new/revised policies to maintain current awareness of changes which impact on their roles and responsibilities.

2. Introduction

The Trust has a statutory duty to have in place appropriate organisation-wide policies/procedural documents to comply with legislation and Care Quality Commission (CQC) to enable staff to fulfil the requirements of their role safely and competently.

Information Governance is the framework of law and best practice that regulates the manner in which information, (including, but not restricted to, information relating to and identifying individuals) is managed i.e. obtained, handled, used and disclosed.

The Trust recognise the importance of maintaining an appropriate and robust system of information governance management – so as to underpin and support the Trust in the exercise of its functions, to protect privacy and confidentiality, and in order to maintain public trust.

This policy sets out the Trusts approach to ensuring that it has a robust information governance framework to manage its information assets.

This policy applies to those members of staff that are employed by the Trust, both permanent and non-permanent, agency staff and for whom the Trust has legal responsibility.

3. Purpose

The purpose of this policy is to inform all members of staff that are employed by the Trust, both permanent and non-permanent, agency staff or for whom the Trust has legal responsibility, of their Information Governance responsibilities and the management arrangements and other policies that are in place to ensure demonstrable compliance.

- This is the central policy in a suite of policies that informs staff of what they should do:
    - To maximise the value of organisational assets by ensuring that data is: Held securely and confidentiality
    - Processed fairly and lawfully
    - Obtained for specific purpose(s)
    - Recorded accurately and reliably
    - Used effectively and ethically, and
    - Shared and disclosed appropriately and lawfully

- To protect the organisation's information assets from all threats, whether internal or external, deliberate or accidental. All staff, both permanent and non-permanent, agency or for whom the Trust has legal responsibility for, will ensure a commitment to:
    - Protect information against unauthorised access i.e. sensitive information
    - Assure confidentiality of information
    - Maintain integrity of information
    - Support information with high quality data
    - Comply with regulatory and legislative requirements
    - Complete Information Governance Training annually
    - Produce, maintain and test business continuity plans
    - Report all IG breaches, actual or suspected, to the Information Governance Team in conjunction with the Data Protection Officer.

The Trust has developed a framework for the Information Governance Policy. This is supported by a set of Information Governance Policies and relates procedures to cover all aspects of Information Governance which are aligned with the NHS Data Security and Protection Toolkit requirements. All associated Information Governance Policies can be found in Section 10.

Many of the Information Governance Policies are supported by underpinning procedures.

4. Duties

Chief Executive/Trust Board – have ultimate responsibility for the implementation of this policy including ensuring that the Trust policies comply with all legal, statutory and good practice requirements.

Caldicott Guardian – Will ensure that the Trust satisfies the highest practical standards for handling patient identifiable information. They have a strategic role which involves representing and championing confidentiality and information sharing requirements and issues at senior management level.

In addition, they actively support information sharing and advise on options for lawful and ethical processing of information and oversee all arrangements, protocols and procedures where confidential patient information may be shared with external bodies within, and outside, the NHS.

Senior Information Risk Owner (SIRO) – Has overall ownership of the organisation's Information Risk Policy and will act as an advocate for information risk on the board. They will understand the strategic business goals of the Trust and how other Trust business goals may be impacted by information risks, and how those risks may be managed. They will implement and lead on internal discussions and will receive training as necessary to ensure they remain effective in their role. i

Data Protection Officer –Will report to the SIRO, but will act independently of the SIRO to inform and advise the organisation and the board in relation to data protection matters. These may include Information Governance risks to the organisation, privacy concerns or recommendations with regard to potential changes to, or new initiatives that, involve processing of personal data.

They monitor compliance with the GDPR and other Data Protection laws, including managing internal data protection activities, advising on data protection impact assessments, training to staff and conducting internal audits where appropriate. They also act as a first point of contact for supervisory authorities and for individuals whose data is processed.

Information Governance Manager – Is responsible for managing the Information Governance agenda across the Trust. This will include monitoring compliance with those requirements around Information Risk Management within the Data Security & Protection Toolkit and ensure that these standards are met.

They are also responsible for issuing guidance to support the implementation and compliance with this policy:

- Publicise and promote this policy
- Ensuring training programme is in place to support the policy
- Monitoring performance of this policy through Quality Control and Internal Audits

Information Assurance and Security Manager – Is responsible for managing the Information Security agenda across the Trust. This will include monitoring compliance with those requirements around Information Security within the Data Security & Protection Toolkit and ensure that these standards are met.

Information Governance Group – ensures the development and subsequently recommends approval of Information Governance policies and management arrangements covering all aspects of Information Governance in line with current legislation, NHS guidance and professional codes of practice as a delegate authority of the IM&T Committee.

The Information Governance Group is responsible for collating all identifiable information risks and maintaining the Trust's Information Governance Risk Log. The Group is responsible for communicating identified risks and their assessed impact and suggested mitigation to the SIRO and the Risk Management and IM&T Committees.

In addition, the Data Security and Protection Toolkit is 'signed off' prior to submission at the Information Governance Group. The Information Governance Group will ensure compliance with the Data Security and Protection Toolkit and will develop, implement and monitor action plans for compliancy.

Senior Information Asset Owners (SIAO) - Are the designated individuals within the Trust that hold responsibility for key Trustwide systems containing patient related personal information. These are systems that form part of the Trust-wide IT Systems Group.

The full responsibilities of the Senior Information Asset Owners can be found within IG08 Information Risk Management Policy.

Information Asset Owners (IAO) – Are responsible for ensuring that their service works within the Information Governance framework. The full responsibilities for Information Asset Owners can be found within IG08 Information Risk Management Policy

Information Asset Administrators - Information Asset Administrators will provide support to Information Asset Owners to. The full responsibilities for Information Asset Administrators, can be found within IG08 Information Risk Management Policy

System Owner – Are the day to day mangers are specific Trust-wide systems that are used within the Trust. They have operational responsibility as part of their role and are accountable to the Senior Information Asset Owners.

All Staff – are responsible for co-operating with the development and implementation of this policy as part of their normal duties and responsibilities. They are responsible for ensuring that they maintain up to date awareness of corporate and local policies with regard to their own staff roles and responsibilities. All staff are mandated to undertake mandatory information governance training annually.

5. Definitions of Terms Used

Information Governance - is a term that is used to describe how organisations and individuals manage the way information is handled within the health and social care system. It covers the requirements and standards that the organisations and their suppliers need to achieve to fulfil the obligations that information is handled legally, securely, efficiently, effectively and in a manner, which maintains public trust. IG encompasses information security, information risk management, patient and staff confidentiality, information sharing, clinical and organisational records management, data quality, secondary uses of information and freedom of access to public information. Good information management is the organisational ability to protect personal confidential data, use this information effectively and ethically for the purposes the information was collected.

Data Protection Act 2018 - Incorporates the General Data Protection Regulations which were implemented on 25th May 2018. It sets standards which must be satisfied when obtaining, recoding, holding, using or disposing of personal data. These are summarised by six data protection principles.

The Freedom of Information (FOI) Act 2000 - is part of the Government's commitment to greater openness in the public sector, The Freedom of Information Act 2000 will further this aim by helping to transform the culture of the public sector to one of greater openness. It will enable members of the public to question the decisions of public authorities more closely and ensure that the services we provide are efficiently and properly delivered.

Information Commissioners Office (ICO) - Appointed by the Government to regulate information related legislation in the UK, including the Data Protection Act 2018 and the Freedom of Information Act 2000.

Data Security and Protection Toolkit - is a mandatory online tool that enables organisations to measure their performance against the National Data Guardian Standards.

The description of the full definitions used in this policy are available in the Glossary of Terms available under the Information Governance section of the intranet.

6. Process

Northumbria Healthcare NHS Foundation Trust have developed a framework for their Information Governance Policy. This is supported by a set of Information Governance policies and related procedures to cover all aspects of Information Governance which are aligned with the NHS Operating Framework and the Data Security and Protection toolkit requirements.

The principles of Information Governance:

6.1 Information Governance Management

The Trust recognises the need for a balance between the need for transparency, openness and confidentiality in the management and use of information.

The Trust will establish and maintain robust operational and management accountability structures, assign appropriate resources and dedicated staff to ensure IG issues are dealt with appropriately, effectively and at levels within the Trust.

There will be proactive use of the information within the Trust, and other NHS partner organisations to support patient/service user care as determined by law, statute and best practice.

The Trust will establish, maintain and review procedures and arrangements for handling queries from patients and the public.

The Trust will establish, maintain and review a publication scheme for the Trust.

There is a commitment to improving staff understanding of their responsibilities around information governance at a level relevant to their role.

The Trust will consider information governance implications of any new or changed system service being implemented.

The Trust will establish and maintain policies and procedures to ensure compliance with the Data Protection Act, General Data Protection Regulations, Human Rights Act, the common law duty of confidentiality, the Freedom of Information Act and the Environmental Information Regulations.

6.2 Confidentiality and Data Protection Assurance

The Trust will share patient/service user information with other health organisations and other non-health agencies in a controlled manner consistent with the interests of the patient/service user and in some circumstances, the public interest.

The Trust will ensure there are effective arrangements in place to ensure confidentiality and security of personal and other sensitive information.

6.3 Information Security Assurance

The Trust will ensure the security of all personal information held by the Trust through the implementation of policies, procedures and processes to ensure the confidentiality, integrity and availability of information to maintain effective and secure management of its information assets and resources.

The Trust will undertake and commission audits to assess information and IT security resilience and arrangements on a regular basis.

6.4 Corporate Information Assurance

The Trust will ensure that policies and procedures are in place to ensure all corporate records are managed, stored and archived in line with governance standards and legislation.

There is a commitment to making non-confidential information widely available in line with responsibilities under the FOI Act 2000 to ensure openness.

The Trust will effectively manage all corporate records regardless of the medium.

6.5 Clinical Information Assurance

The Trust will maintain accurate, timely and relevant information in order to deliver the highest quality health and social care.

The Trust will produce and maintain policies and procedures for information quality assurance and the effective management of records.

The Trust will continually improve records management for care purposes in keeping with professional, legislative and statutory records management requirements.

6.6 Secondary Use Assurance

The Trust will continually develop quality data to support non-direct care related purposes (planning, commissioning, public health, finance) and improve data quality through the use of local and national benchmarking.

6.7 Information Risk

Information risk is inherent in all organisational activities and everyone working for or on behalf of the Trust. All Trust staff, both permanent and non-permanent, whom the Trust has legal responsibility for, has a responsibility to continuously manage information risk. The information risk policy defines how the Trust and its partners will manage information risk and how effectiveness will be assessed and measured.

7. Training and Support

The overriding critical success factor for effective Information Governance will be to develop a culture within the Trust whereby good management of information and associated records becomes second nature to staff. This can only be achieved by an effective programme of awareness and training provided to all Trust staff that use information. In order to achieve this, a staff training assessment will be carried out by the Information Governance department on an annual basis. Gaps in staff awareness will result in targeted training courses.

Information Governance is an item on the Trust Wide mandatory Induction Training Programme. Various training programmes are available.

One off training sessions are provided as requested by Managers/Department Heads where possible.

Mandatory Information Governance training provided via online e-learning tool and also via workbooks.

Work programmes will be developed, implemented, monitored and reviewed to ensure continued compliance and improvements of standards.

8. Process for Monitoring and Audit

Monitoring/audit arrangements	Methodology	Reporting		
		Source	Committee	Frequency
IG Audits	Review of processes to ensure comply with policy (System monitoring, Inappropriate Access Audits)	IG Team	Sub Groups/IG Group/IM&T Committee	Annually
External Assessment	Submission against IG Toolkit (Data Security & Protection Toolkit) and CQC standards	IG Team	Sub Groups/IG Group/IM&T Committee	Annually

Failure to follow this policy may lead to disciplinary action being taken against the member of staff and could potentially lead to criminal investigation and potential prosecution.

9. References

- The Copyright, designs and Patents Act 1990
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- Health and Social Care Act 2000
- Access to Health Records Act 1990
- The NHS Care Record Guarantee
- NHS Code of Practice: Confidentiality
- General Data Protection Regulations
- The Data Protection Act 2018

10. Associated Documentation

Information Governance Policies

- IG 02 Information Security Policy
- IG 03 AUP Network Services Policy
- IG 04 Network Access Policy
- IG 05 Confidentiality Code of Practice Policy
- IG 06 Data Protection Policy

- IG 07 Freedom of Information Policy
- IG 08 Information Risk Management Policy
- IG 09 Internet, Email & Instant Messenger Policy
- IG 10 Registration Authority Policy
- IG 11 Social Media Policy
- IG 12 Digital Forensics Policy
- IG 95 Copyright Law Policy
- IG104 Records Management Policy
- IG108 Use of Making and Using Visual and Audio Recordings
- IG109 Media Policy
- IG110 Use of Mobile Phones and Smart Devices Policy
- IG111 Accessible Information and Communication Support Policy

Data Quality Policies

- DGP01 Data Quality Policy
- DGP02 Operational Policy for Ethnic Monitoring
- DGP03 Trust Patient Identification and Use of NHS Number Policy
- DGP04 Trust Use of PAS Policy
- DGP06 Trust Data Standards Policy
- DGP08 Trust Patient Alerts Policy
- DGP14 PAS Document Management Policy
- DGP15 Policy on the responsibility of IT system owners for ensuring safe and appropriate use of systems by health and social care professionals
- DGP17 Access to SystmOne Policy
- DGP18 Policy on the use of test data on TEST and LIVE PAS

Information Governance Procedures

- Data Protection by Design and Default Procedure/ DPIA Procedure
  Data Subject Rights Procedure
- Data Flow Mapping, Safe Haven Transfers and Caldicott Approval Procedure
- Confidentiality Audit Procedure
  Inappropriate Access Audit Procedure
- Corporate Records Procedure
- Incident Reporting Procedure

Data Quality Procedure

- Health and Social Care Records Procedure

Appendix 1 – Equality Impact Assessment (EIA)

To be completed for all key policies. Cite specific data and consultation evidence wherever possible.

Duties which need to be considered:

- Eliminate unlawful discrimination, harassment and victimisation and other conduct prohibited by the Act
- Advance equality of opportunity between people who share a protected characteristic and those who do not
- Foster good relations between people who share a protected characteristic and those who do not

PART 1 – Overview

Date of equality impact assessment:

15/02/2022

Name(s) and role(s) of staff completing the assessment:

Scott Neal, IG Specialist

Overall, what are the outcomes of the policy?

Provide guidance, assistance and awareness for Northumbria Healthcare NHS Foundation Trust staff to ensure a standard, consistent compliance to Information Governance issues.

PART 2 – Relevance to different Protected Characteristics

Answer these questions both in relation to people who use services and employees as appropriate

Protected Characteristic	Does this characteristic have specific relevance to this policy?	If No –	If Yes –						
		Please state why:	What do you know about usage of the services affected by this policy by people in this protected group, about their experiences of it, and about any current barriers to access?	Could people in this protected group be disproportionately advantaged or disadvantaged by the policy?	Could the policy affect the ability of people in this protected group participate in public life? (E.g. by affecting their ability to go to meetings, take up public appointments etc.)	Could the policy affect public attitudes towards people in this protected group? (e.g. by increasing or reducing their presence in the community)	Could the policy, change make it more or less likely that people in this protected group will be at risk of harassment or victimisation?	If there are risks that people in this protected group could be disproportionately disadvantaged by the policy are there reasonable steps or adjustments that could be taken to reduce these risks?	Are there opportunities to create positive impacts for people in this protected group linked to this policy?
Disability *Note: "disabled people" includes people with physical, learning and sensory disabilities, people with a long-term illness, and people with mental health problems.*	No	N/A							
Sex	No	N/A							
Age	No	N/A							
Race *Note: For the purposes of the Act 'race' includes colour, nationality and ethnic or national origins.*	No	N/A							

Protected Characteristic	Does this characteristic have specific relevance to this policy?	If No –	If Yes –						
		Please state why:	What do you know about usage of the services affected by this policy by people in this protected group, about their experiences of it, and about any current barriers to access?	Could people in this protected group be disproportionately advantaged or disadvantaged by the policy?	Could the policy affect the ability of people in this protected group participate in public life? (E.g. by affecting their ability to go to meetings, take up public appointments etc.)	Could the policy affect public attitudes towards people in this protected group? (e.g. by increasing or reducing their presence in the community)	Could the policy, change make it more or less likely that people in this protected group will be at risk of harassment or victimisation?	If there are risks that people in this protected group could be disproportionately disadvantaged by the policy are there reasonable steps or adjustments that could be taken to reduce these risks?	Are there opportunities to create positive impacts for people in this protected group linked to this policy?
Religion or belief *Note: In the Equality Act, religion includes any religion. It also includes a lack of religion. Belief means any religious or philosophical belief or a lack of such belief.*	No	N/A							
Sexual Orientation *Note: The Act protects bisexual, gay, heterosexual and lesbian people.*	No	N/A							

Protected Characteristic	Does this characteristic have specific relevance to this policy?	If No –	If Yes –						
		Please state why:	What do you know about usage of the services affected by this policy by people in this protected group, about their experiences of it, and about any current barriers to access?	Could people in this protected group be disproportionately advantaged or disadvantaged by the policy?	Could the policy affect the ability of people in this protected group participate in public life? (E.g. by affecting their ability to go to meetings, take up public appointments etc.)	Could the policy affect public attitudes towards people in this protected group? (e.g. by increasing or reducing their presence in the community)	Could the policy, change make it more or less likely that people in this protected group will be at risk of harassment or victimisation?	If there are risks that people in this protected group could be disproportionately disadvantaged by the policy are there reasonable steps or adjustments that could be taken to reduce these risks?	Are there opportunities to create positive impacts for people in this protected group linked to this policy?
Gender Reassignment *Note: The Act provides protection for transsexual people. A transsexual person is someone who proposes to, starts or has completed a process to change their gender.*	No	N/A							
Pregnancy and Maternity *Note: the law covers people who are pregnant or those who have given birth within the last 26 weeks, and those who are breast feeding.*	No	N/A							

Protected Characteristic	Does this characteristic have specific relevance to this policy?	If No –	If Yes –						
		Please state why:	What do you know about usage of the services affected by this policy by people in this protected group, about their experiences of it, and about any current barriers to access?	Could people in this protected group be disproportionately advantaged or disadvantaged by the policy?	Could the policy affect the ability of people in this protected group participate in public life? (E.g. by affecting their ability to go to meetings, take up public appointments etc.)	Could the policy affect public attitudes towards people in this protected group? (e.g. by increasing or reducing their presence in the community)	Could the policy, change make it more or less likely that people in this protected group will be at risk of harassment or victimisation?	If there are risks that people in this protected group could be disproportionately disadvantaged by the policy are there reasonable steps or adjustments that could be taken to reduce these risks?	Are there opportunities to create positive impacts for people in this protected group linked to this policy?
Marriage and Civil Partnership *Note: This applies to changes, decisions or proposals impacting on employees only. The Act protects employees who are married or in a civil partnership.*	No	N/A							

	Could the policy impact on human rights? (e.g. the right to life, the right to respect for private and family life, the right to a fair hearing)
Human Rights	Yes – Article 8.

PART 3 - Course of Action

Based on a consideration of all the potential impacts, tick one of the following as an overall summary of the outcome of this assessment:

☒	The equality analysis has not identified any potential for discrimination or adverse impact and all opportunities to promote equality have been taken.
☐	The equality analysis has identified risks to equality which will not be eliminated, and/or opportunities to promote better equality which will not be taken. Acceptance of these is reasonable and proportionate, given the objectives of the policy and its overall financial and policy context.