Northumbria Healthcare
NHS Foundation Trust

IG 06

Northumbria Healthcare NHS Foundation Trust

Information Governance Policies and Procedures

Data Protection Policy

Version	04
Sub Committee and Approval Date	Information Governance Group 24/05/2021
Date Ratified by Assurance Committee	20/07/2021
Name of Policy Author	Jonathan Walmsley Information Governance Manager
Date Issued	10/08/2021
Review Date	10/08/2024
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	Date Ratified by Assurance Policy Group	Version	Issue Date	Review Date	Policy Author
14/05/2018	29/05/2018	3.1	05/03/2021	29/05/2021	Tracey Best Head of Performance & Quality / DPO
14/05/2018	29/05/2018	3	29/05/2018	29/05/2021	Tracey Best Information Governance Manager
05/05/2015	10/11/2015	2	14/12/2015	14/12/2018	Tracey Best Information Governance Manager
27/03/2012	04/09/2012	1	12/09/2012	12/09/2015	Tracey Best Information Governance Manager

Statement of changes made from version 3.1

Version	Date	Description
04	May 2021	Full review of policy: Section 2: Removal of GDPR reference Section 4 – removal of COO and inclusion of IAO roles, minor changes. Definitions included in section 5 Section 6 – principles updated, Subject Rights section updated, Subject Access section updated. Inclusion of new sections for fees, incident reporting & DPIAs.

Contents

1. Operational Summary

Policy Aim

This Policy has been developed to provide guidance, assistance and awareness for Trust staff to ensure a standard, consistent compliance to processing (creation; storage; retention; accuracy; relevance; disclosure and disposal) of personal identifiable data.

Policy Summary

This policy applies to information, which relates to living individuals; processed by computer or held and stored manually in hard-copy as part of a 'relevant' filing system. Health and Social Care records are mentioned specifically in the Act and subject to secondary legislation.

This policy applies to all personal identifiable data which is received, created, processed or stored within the Trust regardless of the media the data is held.

What it Means for Staff

Policy Authors – Are responsible for providing good practice guidance and is responsible ensuring that this policy clearly outlines the steps required and remains up to date.

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

All Trust Employees – Are responsible for reading the new/revised policies to maintain current awareness of changes which impact on their roles

2. Introduction

The Trust is required by law to comply with the Data Protection Act 2018. It is the commitment of the Trust to ensure that every employee complies with this Act to ensure the confidentiality of any personal data processed by the Trust in whatever medium (i.e. electronic systems, manual filing system).

All legislation and common laws relevant to an individual's right of confidence and the ways in which that can be achieved and maintained are paramount to the Trust. This relates to roles that are reliant upon computer systems such as: patient administration, purchasing, invoicing and treatment planning. Recent legislation also regulates the use

of manual records relating to patients, staff and others whose information may be held within the Trust.

This Policy aims to detail how the Trust meets its legal obligations and NHS requirements concerning confidentiality and information security standards. The requirements within the policy are primarily based upon the Data Protection Act 2018 that is the key piece of legislation covering security and confidentiality of personal information.

The Trust needs to collect and use certain types of information about people with whom it deals in order to operate. These include current past and prospective patients/service users and employees, suppliers and others with whom it communicates. In addition, it may occasionally be required by law to collect and use certain types of information of this kind to comply with the requirements of government departments. This personal information must be dealt with properly however it is collected, recorded and used – whether on paper, in a computer, or recorded on other material – and there are safeguards to ensure this in the Data Protection Act 2018.

3. Purpose

The Trust needs to keep certain information about its employees and data subjects for reasons such as health and social care, research, performance, contractual arrangements and health and safety.

To comply with the law information must be collected and processed fairly and lawfully, stored safely and not disclosed to any other person unlawfully. To do this the Trust must comply with the Data Protection principles.

All staff or others who process or use personal information must ensure that they follow these principles at all times.

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/SIRO/Data Protection Officer

Caldicott Guardian – has 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.

SIRO – will act as an advocate for information risk on the board and during internal discussions in addition they will provide written advice to the accounting officer on the content of the annual statement of internal control in regards to information risk.

Data Protection Officer – will inform and advise the organisation in relation to data protection matters. They monitor compliance with the GDPR and other Data Protection laws, including managing internal data protection activities, advise on data protection impact assessments, train staff and conduct internal audits. They also act as a first point of contact for supervisory authorities and for individuals whose data is processed.

Information Governance Group – ensures the development and subsequently recommends approval of Information Governance policies as a delegated authority of the IM & T Committee.

Information Governance Manager –responsible for issuing guidance to support the implementation and compliance with this Policy:

- Acting as initial point of contact for any data protection issues which may arise within the Trust;
- Publicise and Promote this Policy;
- Ensuring training programme is in place to support the policy;
- Maintaining registration;
- Dealing with Subject Access Requests;
- Monitoring performance of this policy through Quality Control and Internal Audits.

Information Asset Owners (IAO's) – have responsibility for ensuring compliance within their own areas.

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.

5. Definitions of Terms Used

Personal Data – Data which relates to a living individual who can be identified from that data either directly or indirectly.

Processing – Means any operating or set of operations which is performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Special Categories of Personal Data

Data Controller – Means the individual or organisation, which alone or jointly with others, determines the purpose and means of the processing of personal data.

Data Processor - means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Data Subject – An individual who is the subject of personal data

Special Categories of personal data (Sensitive data) - Special category data is personal data which is more sensitive, and so needs more protection. It includes but is not limited to: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, processing of genetic data, biometric data for identification, data concerning health or a person's sex life or sexual orientation.

Data Protection Officer – an individual appointed for the Trust to assist in monitoring internal compliance, informing and advising on data protection obligations, provision of advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority.

Information Commissioners Office - an independent supervisory authority for Data Protection and Information laws.

Disclosure - The passing of personal data to a third party, either an individual or an organisation

Data Protection Registration - The means of updating the official public register for the purposes of keeping personal data in the Trust. It also includes descriptions of the data collected, the class of person the data relates to and to whom the personal data can be disclosed

Subject Access Request - The right of a data subject to have access to the information held about them

Third Party – Any person other than:

- The data subject;
- The data controller;
- Any data processor or other person authorised to process data for the data controller or processor. It does not include the employees of the controller.

6. Process

The following 6 principles must be applied to all processing of personal data.

6.1 Principle 1

Lawfulness, fairness and transparency - Processed lawfully, fairly and in a transparent manner in relation to individuals

There is a requirement to make the general public, who may use the services of the NHS, aware of why the Trust needs information about them, how this is used and to whom it may be disclosed.

The Trust is obliged under the Data Protection requirements and Caldicott recommendations to produce patient/staff/service user information leaflets and posters (privacy notices) which explain to individuals how their information may be used.

In order for processing of personal data to be lawful the Trust must have an appropriate lawful basis under data protection legislation.

In some cases, if the data is sensitive (special category) processing is only permitted if a further condition is present under data protection legislation or the data subject has given consent. Further guidance on obtaining consent can be found in the NHS Confidentiality: NHS Code of Practice and the Trust's Confidentiality Code of Conduct Policy (IG05).

6.2 Principle 2

Purpose Limitation - collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes

The Trust must ensure that all processing of personal data is carried out for predefined purposes or remains in line with the original purposes intended i.e provision of healthcare.

6.3 Principle 3

Data Minimisation - Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

6.4 Principle 4

Accuracy - accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

6.5 Principle 5

Storage limitation - kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals

Records must be retained in accordance with guidance on retention periods for clinical and corporate records. Further information can be found in the Trust Record Management Policy IG104.

6.6 Principle 6

Integrity and confidentiality - processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

6.7 Accountability

The Trust shall be responsible for, and be able to demonstrate compliance with the above principles.

6.8 Rights of the data subject

Under the Data Protection Act individuals have a number of different rights in respect of personal data held about them, these are:

- Right to Information
- Right to access
- Right to rectification
- Right to be forgotten
- Right to restriction of processing
- Right to object
- Rights in appropriate decision making (Automated)
- Right to data portability
- Right to notification

The Trust must ensure an up to date procedure is in place to deal with Data Subject Rights requests. Refer to the Data Subjects Rights Procedure, Access to Health and Social Care Records Procedure and guidance on disclosure to the Police.

Individuals have a right to seek compensation for any breach of the Act which may cause them damage and/or distress.

Further guidance can be sought from the Trust Information Governance Team or Trust Data Protection Officer.

6.9 Rights of Subject Access

All individuals have the right upon making a request and providing the necessary identification documents, whether the individual or someone else on their behalf is processing personal data relating to that individual.

Individuals have the right to be given:

- A description of the personal data the Trust holds
- The purposes for which it is being processed
- The categories of data being processed
- Those to whom it is, or may be, disclosed
- A copy of the information about them held by the Trust, except where the supply of such a copy is not possible or would involve disproportionate effort, or the individual agrees otherwise.

- A copy of the information provided should be provided in the format in which it is requested i.e. if it is requested electronically then it should be provided in this way.
- information as to the source of the personal data if available, except where this would involve the disclosure of information relating to an individual other than the subject of the information (a third party), including the fact that they were the source of the information. a disclosure of this nature may only take place where:
  - The other individual has consented to the disclosure of the information, or
  - Where it is reasonable in all the circumstances to comply with the request without the consent of the other individual.

Procedures are in place across the Trust to ensure subject access requests are responded to effectively. All requests must be dealt with promptly and within 1 month following receipt of a valid request.

The Access to Health Records Act 1990 will remain to provide access rights to the patient's personal representative, next of kin, or those who may have a claim arising out of the death of the individual, to deceased patient's records. Refer to the Data Subject Rights procedure & Access to Health and Social Care Records procedure (for further information.

The Data Protection Act 2018 will provide access rights under Schedule 2, S2(1) for personal data processed for the following purposes:

- The prevention or detection of crime
- The apprehension or prosecution of offenders, or
- The assessment or collection of any tax or duty or of any imposition of a similar nature.

6.10 Charges and fees

The Trust do not charge a fee for providing information to requestors.

The Trust may charge a fee where a duplicate copy of information has been requested:

- £10 for an additional copy of computer records.
- Maximum fee of £50 for additional copies of manual records.

6.11 Incident reporting

All incidents involving confidentiality, availability and integrity of personal data must be reported immediately to the information governance team and dealt in accordance to the Trust incident reporting procedure.

6.12 Data Protection Impact Assessments (DPIA)

DPIA's are a process designed to help systematically analyse, identify and minimise data protection risks. They are key part of the Trusts accountability obligations under the Data Protection Act. The Trust has a Data Protection Impact Procedure that must be considered for any proposed, new or change in process, service, technology or project which pertains to utilise personal information.

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.

Training is provided in response to Audits or Incidents.

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
Audit	Review of processes to ensure comply with policy	Internal Auditors	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

Wherever the monitoring has identified deficiencies, the following should be in place:

- Action plan
- Progress of action plan monitored by the appropriate Committee (minutes)
- Risks will be considered for inclusion in the appropriate risk registers
- 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

- Access to Health Records 1990
- Regulation of Investigatory Powers Act 2000
- Human Rights Act 1998
- Freedom of Information Act 2000
- Crime and Disorder Act 1998
- Data Protection Act 2018
- General Data Protection Regulations

10. Associated Documentation

- IG 05 Confidentiality Code of Conduct Policy
- Access to Records Procedure
- Corporate Records Procedure
- Disclosure of information to the Police
- Guidance for sending personal information by post
- Third Party Procedure
- Secure Email Matrix
- Records Management Code of Practice for Health and Social Care 2016

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:

25/06/2021

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

Tracey Best, Head of Performance & Quality / Data Protection Officer

Overall, what are the outcomes of the policy?

To be compliant with the data protection changes (GDPR & DP Act 2018)

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	No affected with changes applied							
Sex	No	No affected with changes applied							
Age	No	No affected with changes applied							
Race *Note: For the purposes of the Act 'race' includes colour, nationality and ethnic or national origins.*	No	No affected with changes applied							

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	No affected with changes applied							
Sexual Orientation *Note: The Act protects bisexual, gay, heterosexual and lesbian people and asexual people*	No	No affected with changes applied							

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 trans people. A transperson is someone who proposes to, starts or has completed a process to change his or her gender.*	No	No affected with changes applied							
Pregnancy and Maternity *Note: the law covers pregnant women or those who have given birth within the last 26 weeks, and those who are breast feeding.*	No	No affected with changes applied							
Marriage and Civil Partnership *Note: This applies to changes, decisions or proposals impacting on employees only. The Act protects employees who are*	No	No affected with changes applied							

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?
married or in a civil partnership regardless of gender .									
Human Rights	**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)**								

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.