Joint Policy for Cumbria Partnership Foundation Trust & North Cumbria University Hospital NHS Trust

Information Sharing (Disclosure) Policy

Reference	POL/IG/003
Version	1.0
Date Ratified	25 May 2018
Next Review Date	May 2021
Accountable Director	Director of Finance, and Joint Director of Strategy and Support Services
Policy Author	Head of Information Governance

Please note that the Intranet / internet Policy web page version of this document is the only version that is maintained.

Any printed copies or copies held on any other web page should therefore be viewed as "uncontrolled" and as such, may not necessarily contain the latest updates and amendments.

Policy On A Page

SUMMARY & AIM

This policy covers the issues of confidentiality and security relating to the transfer, disclosure / sharing of information. It is essential that transfers meet legal and ethical standards demanded.

The aim of the policy is to:

Promote good practice around the transfer of person identifiable information using the Information Sharing Gateway as the tool for creating and managing information sharing agreements;

Ensure that that common legal and ethical standards are applied in order to meet Data Protection, professional codes and Caldicott standards;

Ensure that any use of data is lawful, and properly controlled;

Guarantee that the data protection rights of individuals are respected; and

Comply with the Law in terms of information sharing and providing reasonable ethical justifications for sharing in all circumstances in order for the Trust to meet its statutory obligations.

TARGET AUDIENCE:

All employees who process personal data on behalf of the organisations covered by this policy.

TRAINING:

Annual mandatory Information Governance training includes information sharing.

KEY REQUIREMENTS

Any disclosure of data must be in accordance with Article 5 of the GDPR (Data Protection principles) and the Caldicott principles.

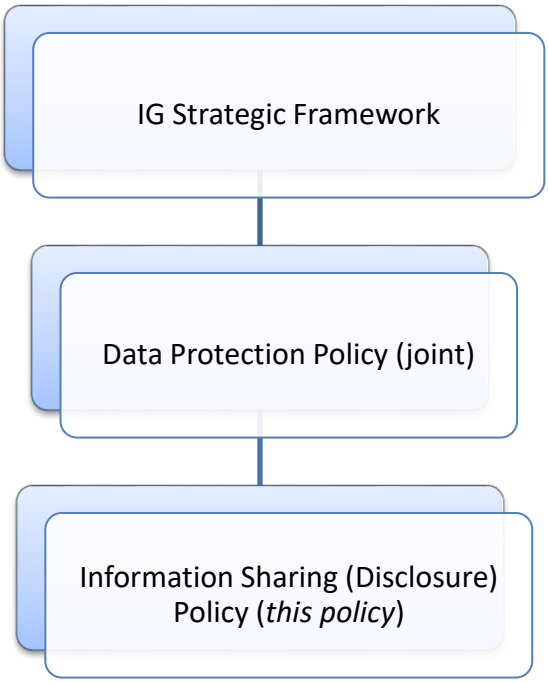
The Information Commissioner has indicated that in order to comply with Fair Processing the Trust will be transparent – clear and open with individuals about how their information will be used.

Transparency is always important, but especially so in situations where individuals have a choice about whether they wish to enter into a relationship with you. If individuals know at the outset what their information will be used for, they will be able to make an informed decision about whether to enter into a relationship or perhaps to try to renegotiate the terms of that relationship.

Assessing whether information is being processed fairly depends partly on how it is obtained. In particular, if anyone is deceived or misled when the information is obtained, then this is unlikely to be fair.

TABLE OF CONTENTS

SUMMARY FLOWCHART:



1. INTRODUCTION

There are a range of statutory provisions that limit, prohibit or set conditions in respect of the disclosure of records to third parties, and similarly, a range of provisions that require or permit disclosure. The key statutory requirements can be found in the Records Management Code of Practice for Health and Social Care 2016.

The organisations covered by this policy are committed to working in partnership with other agencies involved in providing services to its patients / service users. It is recognised that the exchange of relevant information between partners is fundamental to the provision of safe and effective service delivery. Such exchanges must meet required legal and ethical standards.

When patients are referred to our services it is understood that, under common law, they have consented to the referral being made and to the processing of information relevant to that referral. The Trust will not routinely request permission to view a shared record and, under the General Data Protection Regulation (GDPR), the will process information under Article 6(1)(e) and, where the information is sensitive, Article 9 (2)(h).

- *Article 6(1)(e)* – to carry out a public function or a task in the public interest or exercise official authority
- *Article 9(2)(h)* – Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional

However, it remains good practice to tell the patient that their information is being shared **unless** there is a specific public interest requirement preventing informing the patient (e.g. in criminal proceedings).

The partners covered by this policy have signed up to a common information sharing memorandum of understanding contained within the Information Sharing Gateway (ISG). This sets out high level principles for information sharing (disclosure) across key partner organisations (i.e. abiding by Data Protection 2018 and Caldicott 3, staff training, retention, documenting and risk assessing data flows and appointing an accountable senior officer responsible for the protection of personal information).

The ISG has been developed by a sub-group of organisations from the Lancashire and Cumbria IG Group in order to improve and modernise the administration and risk assessment of information sharing in the public sector.

The partners support this as the only tool to be used for storing information sharing agreements from 1 October 2015 (CPFT) and 27 June 2017 (NCUHT).

More information on the Information Sharing Gateway can be found here.

2. PURPOSE

This policy covers the issues of confidentiality and security relating to the transfer, disclosure / sharing of information. It is essential that transfers meet legal and ethical standards demanded.

This policy applies to all personal information (including anonymised and pseudonymised records) processed by North Cumbria University Hospitals NHS Trust and Cumbria Partnership NHS Foundation Trust relating to services users, their families and carers and members of staff. In particular the policy includes both clinical (i.e. clinical records) and corporate information (personnel and payroll information). It also covers all mediums of information, i.e. electronic, paper, verbal etc.

This policy equally applies to any organisation covered by the IG Service Level Agreement (i.e. North Cumbria Clinical Commissioning Group).

3. POLICY DETAILS:

Disclosure of personal information between partner agencies is vital to the provision of co-ordinated care for patients. There are however, rules that need to be maintained to meet the ethical and legal requirements around the sharing of personal information particularly with regard to security and confidentiality.

Any request to disclose personal data of any individual whose data is held by the Trust(s) will be considered carefully. Disclosures will only be permitted if an appropriate and necessary justification is established, in line with the requirements for lawful processing defined in data protection legislation. Any such disclosure will be recorded along with the reasons and justifications established to permit the disclosure. If a request to disclose is received, but no justification for disclosure other than consent would permit the disclosure, then disclosure will only be with the informed, explicit, recorded consent of the data subject.

Regardless of the justification for any disclosure, the data subject will be informed about the request and potential disclosure, unless to do so would prejudice any reasons for the request being made (such as prejudicing a police investigation or legal case). If the decision is taken not to inform the subject the relevant justifications as defined in legislation will be noted.

We process personal information to enable us to provide healthcare services for patients, data matching under the national fraud initiative; research; supporting and managing our employees, maintaining our accounts and records and the use of CCTV systems for crime prevention.

The data will be shared with health and care professionals and support staff in the Trust and at hospitals, diagnostic and treatment centers who contribute to your personal care for direct care purposes. This will include your GP.

Where necessary or required we may consider sharing information with any other categories of recipients. Please refer to the following privacy notices for details.

NCUH	http://www.ncuh.nhs.uk/about-us/fair-processing/index.aspx
CPFT	https://www.cumbriapartnership.nhs.uk/the-trust/access-to-records/how-the-trust-manages-your-information
NC CCG	http://www.northcumbriaccg.nhs.uk/about-us/fair-processing-notice.aspx

Any disclosure of data must be in accordance with Article 5 of the GDPR (Data Protection principles) and the Caldicott principles (see below). The Information Commissioner has indicated that in order to comply with Fair Processing the Trust will be transparent – clear and open with individuals about how their information will be used.

3.1 Data Protection Principles

The principles are:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals
(b) 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 and in the publice interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes
(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
(d) 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 ratified without delay
(e) 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 GDPR in order to safeguard the rights and freedoms of individuals
(f) 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.

Article 5(2) of the GDPR requires that

“the controller shall be responsible for, and be able to demonstrate, compliance with the principles” (accountability).

3.2 Caldicott Principles

- Justify the purpose
- Only use patient identifiable information if it is absolutely necessary
- Use the minimum amount for the purpose required
- Access to the data must be on a strict need to know basis
- All staff must be aware of their responsibilities and understand and comply with the law
- Understand and comply with the law
- The duty to share information can be as important as the duty to protect patient confidentiality

3.3 Safeguarding

Information sharing is vital to safeguarding and promoting the welfare of children and young people. A key factor in many serious case reviews has been a failure to record information, to share it, to understand its significance and then take appropriate action.

Good practice requires that concerns and proposed action are sensitively shared with parents/carers (and where age appropriate, with children and young people), unless this is likely to place the children or adults at risk in greater danger, e.g. in the case of fabricated or induced illness, (FII) or in the case of sexual abuse where criminal evidence may be tampered with or destroyed.

Although sharing concerns and proposing a referral to the local authority may cause distress and anger initially, in the long term, openness can be appreciated and professional relationships strengthened with families. It should be acknowledged that, in some instances, the relationship may be damaged and an alternative worker will need to be identified.

Working Together (2013) states: “Early sharing of information is the key to providing effective early help where there are emerging problems. At the other end of the continuum, sharing information can be essential to put in place effective child protection services. Serious Case Reviews (SCRs) have shown how poor information sharing has contributed to the deaths or serious injuries of children.

More information can be found here:

NCUH – staff web only	http://nww.staffweb.cumbria.nhs.uk/services-and-departments/safeguarding/safeguarding.aspx
CPFT – public website	https://www.cumbriapartnership.nhs.uk/the-trust/safeguarding-children-and-adults
NC CCG – public website	http://www.northcumbriaccg.nhs.uk/about-us/safeguarding/index.aspx

3.4 Sharing for research

The function of the Research and Development department is to approve and facilitate clinical research whilst ensuring that we comply with all legal, regulatory and ethical requirements within the healthcare research process.

The Research and Development department operates within the national strategies set out by the Heath Research Authority and adopt best practice guidance issued by the National Institute for Health Research. More information can be found here:

NCUH	http://www.ncuh.nhs.uk/about-us/research-and-development/research-and-development.aspx
CPFT	https://www.cumbriapartnership.nhs.uk/the-trust/the-trust-research-and-development
Heath Research Authority	https://www.hra.nhs.uk/
National Institute for Health Research	https://www.nihr.ac.uk/

Note: the NCUH and CPFT research departments are due to work in partnership in 2018.

3.5 Recording Sharing

Ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those who need to have it, is accurate and up to date, is shared in a timely fashion, and is shared securely.

Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

3.6 Managing objections to Information Sharing

The Trust will not routinely request the permission of the patient to view a shared record. However, there are a number of safeguards in place for patients regarding this:

- It should be possible for a patient to prevent disclosure of their medical data if they choose to. This is subject to the patient having capacity to make an informed decision and understand the full consequences of refusing to share any information
- Only those health professionals (or authorised personnel) that are presently involved in the patient's treatment may have access. There must be actual and current treatment between the professional and the patient, and reliable controls must be in place to identify and authenticate these therapeutic relationships
- Privacy by design has been put into our EPRs - modular presentation of the contents supported by access controls - so that access is only given to relevant parts of the record (**not applicable to NCUH or NC CCG**)

- All staff undertake mandatory IG training to ensure that they understand the rights of patients with regards to privacy and confidentiality, and that they aware of how to escalate objections from patients in the use of their information
- Patients can be provided with audit logs as to who has accessed their data via the subject access process (**not applicable to NCUH or NC CCG**).

4. TRAINING AND SUPPORT

Employees will be made aware of their responsibilities under this policy through:

- Effective induction
- Circulation of this policy via the intranet and employee noticeboards
- Mandatory annual training.

More in-depth training will be undertaken by Information Asset Owners, Information Asset Administrators, SIRO, Caldicott Guardian.

5. MONITORING COMPLIANCE WITH THIS FRAMEWORK

The process for monitoring compliance with the effectiveness of this policy is as follows:

Aspect being monitored	Monitoring Methodology	Reporting		
		Presented by	Committee	Frequency
Standard reports in the Information Sharing Gateway will be shared with the IG Board (unsigned data flows etc).	Dashboard via Information Sharing Gateway	Head of IG	Joint Information Governance Board	Quarterly

6. REFERENCES AND BIBLIOGRAPHY:

The General Data Protection Regulation – Guidance on the role of the Data Protection Officer (Information Governance Alliance)
https://digital.nhs.uk/information-governance-alliance/General-Data-Protection-Regulation-guidance

The General Data Protection Regulation – Guidance on Accountability and organisational priorities (Information Governance Alliance)
https://digital.nhs.uk/information-governance-alliance/General-Data-Protection-Regulation-guidance

The General Data Protection Regulation – Guidance on lawful processing (Information Governance Alliance)

https://digital.nhs.uk/information-governance-alliance/General-Data-Protection-Regulation-guidance

Overview of the GDPR (Information Commissioner's Office)
https://ico.org.uk/for-organisations/data-protection-reform

Preparing for the General Data Protection Regulation (GDPR): 12 steps to take now (Information Commissioner's Office)

https://ico.org.uk/for-organisations/data-protection-reform

National Data Opt Out (NHS Digital)
https://www.digital.nhs.uk/national-data-opt-out

Crime and Disorder Act 1998
http://www.legislation.gov.uk/ukpga/1998/37/contents

Children and Young Person's Act 2008
http://www.legislation.gov.uk/ukpga/2008/23/contents

Criminal Justice Act 2003 http://www.legislation.gov.uk/ukpga/2003/44/contents

Health and Social Care Act 2012
http://www.legislation.gov.uk/ukpga/2012/7/contents

7. ASSOCIATED DOCUMENTATION:

IG Strategic Framework
Data Protection Policy (joint)

8. DUTIES (ROLES & RESPONSIBILITIES):

8.1 Chief Executive / Trust Board Responsibilities:

The Chief Executive and Trust Board jointly have overall responsibility for the strategic and operational management of the Trust, including ensuring that Trust policies comply with all legal, statutory and good practice requirements. Data Protection compliance responsibilities have been delegated to the Executive Director of Finance, Strategy and Support Services.

8.2 Director of Finance, and Joint Director of Strategy and Support Services

The Executive Director is responsible for ensuring that the Trust has systems and policies in place to ensure data protection compliance.

8.3 Caldicott Guardian

The Caldicott Guardian role:

- Is advisory
- Is the conscience of the organisation
- Provides a focal point for patient confidentiality and information sharing issues
- Is concerned with the management of patient information.

The Caldicott Guardian is the person with overall responsibility for ensuring the Trusts have in place the appropriate security and processes to protect person identifiable data (PID). The Caldicott Guardian plays a key role in ensuring that the organisation and partner organisations abide by the highest level for standards for handling PID and adherence to the Caldicott Principles. It is the responsibility of the Caldicott Guardian to feedback any IG issues to the Executive Senior Management Team. The Caldicott Guardian (or designated individual) is a member of the Information Governance Board. The Caldicott Guardian has a responsibility to keep up to date with developments.

8.4 Senior Information Risk Owner (SIRO)

The Senior Information Risk Officer role:

- Is accountable
- Fosters a culture for protecting and using data
- Provides a focal point for managing information risk and incidents
- Is concerned with the management of all information assets.

The SIRO is an Executive Board member with allocated lead responsibility for the Trust's information risks and provides a focus for the management of information risk at Board level. The SIRO chairs the Information Governance Board. The SIRO has a responsibility to keep up to date with developments.

8.5 Designated Data Protection Officer (DPO)

The Trust's Data Protection Officer role:

- Has a level of autonomy to pursue their duties with the full support of the controller and / or processor
- The Data Protection Officer needs to be involved properly and in a timely manner in all issues which relate to the protection of personal data. The Trust / Processor shall support the Data Protection Officer in completion of the tasks required
- The DPO has a specific relationship with the Trust(s), it also has a specific relationship with the supervisory authority (the Information Commissioner). The DPO operations as a kind of intermediary in many instances providing a single point of contact, and ensuring that any communication with the supervisory authority and the Data Controller (the Trust(s)) / data processors (i.e. contractors) are clearly understood
- The Data Protection Officer is the single point of contact for the public for any queries relating to information about any data subject

- To inform and advise the controller or the processor and the employees who carry out tasks of their obligations
- To monitor compliance, including the assignment of responsibilities, awareness raising and training of staff and related audits
- To provide advice with regards to Data Protection Impact Assessments
- Have due regard to the risks associated with processing operations.

8.6 Information Asset Owners (IAO)

IAOs are senior / responsible individuals working in a relevant business area. Their role is to understand what information is held, what is added and what is removed, how information is moved, who has access and why. As a result they are able to understand and address risks to the information and ensure that information is fully used within the Law for the public good, and provider written input to the SRIO annually on the security and use of their assets.

An IAO will be responsible for an information asset in terms of:

- Identifying risks associated with the information asset
- Managing and operating the asset in compliance with policies and standards
- Ensuring controls manage all risks appropriately
- Approve access to the system.

8.7 Information Asset Administrators (IAAs)

Information Asset Administrators (IAA's) have responsibility for ensuring that information asset specific policies, procedures and standard operating procedures are followed by staff and recognise actual or potential security incidents, and consult their IAO on incident management. The IAAs are senior individuals and are usually head of department or with ultimate responsibility for the information asset.

8.8 Information Security Managers

The Information Security Managers are responsible for the provision and management of a high quality, customer focussed, Information Technology Security Advisory Service using expertise to manage security issues, identifying best practice and making recommendations for local implementation.

8.9 Information Governance Team

The Information Governance Team provides advice and guidance on all aspects of data protection compliance.

8.10 Human Resource Department

The Human Resources Department as responsible for compliance under this policy with all matters affecting staff compliance (i.e. fair processing notice for staff).

8.11 Managers

Managers are responsible for ensuring departmental record-keeping processes and all other departmental procedures adhere to this policy and that their teams adhere to the principles within this policy. Managers must ensure:

- Staff complete training in information governance
- Ensure that data protection incidents are reported by individual and investigate where appropriate
- Ensure processes are maintaining the rights of data subject
- Ensure any change in process has a data protection assessment completed
- Ensure that data flows are appropriately mapped.

8.12 All staff

All staff are responsible for ensuring that:

- Keep up to date with IG training
- any personal or sensitive personal data that they hold is kept securely and only used for legitimate business of the Trust(s)
- Personal, sensitive personal data and or any other restricted data is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party
- Reporting any near misses or incidents related to personal data, so they can be investigated and managed.

All staff are additionally responsible for:

- checking that any information that they provide to the Trust(s) in connection with their employment is accurate and up to date
- informing the Trust(s) of any changes to information that they have provided, including but not limited to changes of address, either at the time of appointment or subsequently. The Trust(s) cannot be held responsible for any errors unless the employee has informed it of such changes.

Any member of staff, or other individuals who considers that the policy has not been followed in respect of personal data about himself or herself, should raise the matter with his or her line manager in the first instance and then to the Trust(s) Data Protection Officer.

Staff should note that unauthorised disclosure of data deemed, personal, sensitive (special category) personal, confidential and restricted under the definitions in this policy will usually be a disciplinary matter, and may be considered gross misconduct in some cases. Therefore it is essential, if unsure, to check whether the disclosure is necessary or legally permissible by checking with the Data Protection Officer.

Staff should also follow the requirements of the Information and Cyber Security policy to ensure that all data in all formats/media is managed securely in line with its classification under the handling guidelines.

Staff will be required to report any incident related to data via the incident management system (Ulysses) so that swift remedial and containment action can be applied.

8.12.1 Other key responsibilities in relation to the sharing and disclosure of information - Knowledge

- Meet standards outlined in this and other related policies as well as in their terms of employment (or other engagement agreements)
- Be aware of and fully understand their legal and ethical obligations to keep personal information obtained through their work confidential
- Participate in induction, mandatory IG training and awareness raising sessions carried out to inform / update staff on information sharing issues
- Be aware of the nominated Senior Information Risk Owner, Caldicott Guardian and Data Protection lead in the Trust whom they should liaise with regard to information disclosure issues
- Health professionals must be aware of patients' and staff's rights about the information they wish to disclose to others, except where legally required to disclose in case of a Court Order

8.12.2 Putting Knowledge into practice

- Challenge and verify where necessary the identity of any person who is making a request for confidential information and determine the validity of their reason for requiring that information
- Report any actual or suspected breaches of disclosure to their line manager and via the incident reporting system
- Participate in audit / reviews of working practices to identify areas of improvement with regard to disclosure of information and to implement any measures identified
- Ensure data is recorded accurately, in a legible manner and signed clearly in accordance with the Trust policy on record keeping

8.12.3 Respect for patients

- Ensure that patients have been informed how the Trust will look after their information by providing leaflets and ensuring that the information is understood
- Inform patients when information is or may be disclosed to others. This includes situations where patients may seek advice from the Trust
- Provide patients with the opportunity to consent to how their information will be used and shared
- Provide patients with choice and respect and record their decisions to restrict disclosure or use of their information
- Continually strive to improve practice

8.13 Approving Committee Responsibilities:

The Chair of the Joint Information Governance Board will ensure the policy approval is documented in the final section of the Checklist for Policy Changes. The committee will agree the approval of the final draft of the policy.

9. ABBREVIATIONS / DEFINITION OF TERMS USED

Keep lists in alphabetical order

ABBREVIATION	DEFINITION
AHRA	Access to Health Records Act 1990
CEO	Chief Executive Officer
CPFT	Cumbria Partnership NHS Foundation Trust
DPA	Data Protection Act 1998
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DS&Ptk	Data Security and Protection Toolkit
GDPR	General Data Protection Regulation
HSCIC	Health and Social Care Information Centre
ICO	Information Commissioner's Office
IAA	Information Asset Administrator
IAO	Information Asset Owner
IG	Information Governance
IGtk	Information Governance Toolkit
ISG	Information Sharing Gateway
MoU	Memorandum of Understanding
NCUH	North Cumbria University Hospitals NHS Trust
PID	Personal Identifiable Data
SAR	Subject Access Request
SIRO	Senior Information Risk Owner
SOP	Standard Operating Procedure
ToR	Terms of Reference

TERM USED	DEFINITION
Anonymised Information	This is information which does not identify an individual directly, and which cannot reasonably be used to determine identity. Anonymisation requires the removal of name, address, full postcode and any other detail or combination of details that might support identification.
Confidentiality	A duty of confidence arises when one person discloses information to another person, where it is reasonable to expect that information is to be held in confidence.
Data Controller	A Data Controller is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are to be processed. By person it does not necessarily mean a living individual but refers to legal entity (i.e. organisation).

Data Erasure	**A**lso known as the Right to be Forgotten, it entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties cease processing of the data
Data Portability	The requirement for controllers to provide the data subject with a copy of his or her data in a format that allows for easy use with another controller
Data Processor	Any person (other than an employee of the data controller) who processes the data on behalf of the Data Controller.
Data Recipient	A recipient is any person who obtains a disclosure of data, this includes employees or agents who would not be regarded as third parties.
Data Subject	A natural person whose personal data is processed by a controller or processor
Disclosure	This is the divulging or provision of access to data.
Encrypted Data	**P**ersonal data that is protected through technological measures to ensure that the data is only accessible/readable by those with specified access
Health Record	Information about the physical or mental health or condition of an individual, made by or on behalf of a health professional in connection with the care of that individual.
Healthcare Purposes	These include all activities that directly contribute to the diagnosis, care and treatment of an individual and the audit/assurance of the quality of the healthcare provided. They do not include research, teaching, financial audit and other management activities.
Information Asset Administrator	Primary role is to support the IAO to fulfill their responsibilities. IAAs will ensure that policies and procedures are followed, recognise actual or potential security incidents, consult with their IAO on incident management and ensure that information asset registers are accurate and up to date.
Information Asset Owners	Senior members of staff who take responsibility for Information Assets such as information systems - further defined in the Trust's Information Risk Policy.
Information Sharing Protocols	Documented rules and procedures for the disclosure and use of patient information, which specifically relates to security, confidentiality and data destruction, between two or more organisations or agencies.
Medical Purposes	As defined in the Data Protection Act 1998, medical purposes include but are wider than healthcare purposes. They include preventative medicine, medical research, financial audit and management of healthcare services. The Health and Social Care Act 2001explicitly broadened the definition to include social care.
Personal Identifiable Data	Data that relate to a living individual who can be identified either from the data alone, or from combining the data with other information held by the data controller. It includes any recorded expression of opinion by or about the individual. Personal data may be held in electronic or manual form, or both.
Processing	Any activity that can be carried out concerning personal data.

Profiling	**A**ny automated processing of personal data intended to evaluate, analyse, or predict data subject behavior
Pseudonymised Information	This is like anonymised information in that in the possession of the holder it cannot reasonably be used by the holder to identify an individual. However it differs in that the original provider of the information may retain a means of identifying individuals. This will often be achieved by attaching codes or other unique references to information so that the data will only be identifiable to those who have access to the key or index. Pseudonymisation allows information about the same individual to be linked in a way that true anonymisation does not.
Sensitive Personal Data / Special categories of personal data	**Under GDPR (article 9) "special categories of personal data" means personal data consisting of information such as -** a) racial or ethnic origin b) political opinions, c) religious or philosophical beliefs d) trade union membership, e) genetic data f) biometric data g) health data h) sex life i) sexual orientation The presumption is that, because information about these matters could be used in a discriminatory way, and is likely to be of a private nature, it needs to be treated with greater care than other personal data. The nature of the data is also a factor in deciding what security is appropriate
Third Party Information	Information relating to any person other than the data subject, the Data Controller or any data processor or other person authorised to process data for the controller or processor. Generally this would be one of the following: 1) Any individual who is identifiable from the records who is not the applicant. Note that this does not apply to healthcare professionals. 2) In an organisation context, a third party is any organisation / agency which is not the Trust, i.e. where the Trust holds information from other organisations, those other organisations remain organisationally responsible for their own records as the "data controller" and constitute third parties

DOCUMENT CONTROL

Equality Impact Assessment Date	n/a
Sub-Committee & Approval Date	*Joint IG Board.*

History of previous published versions of this document:

Version	Ratified Date	Review Date	Date Published	Disposal Date
1.0	25/5/18	31/5/18	29/6/18	25/5/2038

Statement of changes made from previous version

Version	Date	Section & Description of change
0.3	30/05/2018	• 3.6 – correction of grammar - *"Patients can be provided with audit logs as to who has access their data via the subject access processes"* changed to *"Patients can be provided with audit logs as to who has accessed their data via the subject access process"*
1.0	29/06/2018	• First Issue

List of Stakeholders who have reviewed the document

Name	Job Title	Date
Yvonne Salkeld	Head of Information Governance	03/11/2017 25/01/2018 16/03/2018 15/05/2018
Anne Gadsden	Information Governance Officer and Freedom of Information Lead	25/01/2018 14/05/2018
Paul Corrie	Information Governance Compliance Manager	14/05/2018
Justine Gatehouse	Information Rights Co-ordinator	14/05/2018
Helen Charnley	Health Records Manager	14/05/2018
Gillian Coward	Data Quality Manager	14/05/2018
Graham Putnam	Caldicott Guardian (NCUH)	21/05/2018
Andrew Brittlebank	Caldicott Guardian (CPFT)	21/05/2018
David Rogers	Caldicott Guardian (NC CCG)	21/05/2018
Julie Thompson	Head of Workforce Services	21/05/2018
Lorraine Gray	Head of Information	21/05/2018
Esther Kirby	Chief Nurse	21/05/2018
Farouq Din	Interim Associate Director of E-Health	21/05/2018
Jemma Barton	Head of Clinical Governance	21/05/2018
Mandy Annis	Employment Services Bureau Manager	21/05/2018

Ian Pearson	Pathology Information & Performance Manager	21/05/2018
Micheal Smillie	Director of Finance, and Joint Director of Strategy and Support Services	25/05/2018 (IG Board)