Cumbria Partnership
NHS Foundation Trust

New Safe Haven and Effective Anonymisation Policy: POL/002/081 (CPFT)

Reference	POL/002/081
Version	2.0
Date Ratified	14/05/2019
Next Review Date	May 2022
Date Published	23/5/2019
Accountable Director	Director of Workforce/Organisational Development
Policy Author	Information Development Manager

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

What is this policy for?

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.

Ensure 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:

Mandatory IG training on an annual basis for all staff.

KEY REQUIREMENTS

Any disclosure of data must be in accordance with Article 5 of the General Data Protection Regulation (GDPR) (Data Protection principles) and the Caldecott 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

1. INTRODUCTION

The NHS has used the principle of safe havens for over 20 years to ensure the safety and secure handling of confidential patient identifiable information. It was first defined to ensure security when faxes were used to transmit patient data between providers and purchasers. In that case a physical location of a locked room was used to restrict access to fax machines and hence to patient identifiable information. Later safe haven principles defined secure conditions necessary for the handling of personally identifiable data in a wider context.

The term 'Safe Haven' is used within the NHS to denote either a secure physical location or the agreed set of administrative arrangements that are in place to ensure security classified, personal or other sensitive information is communicated safely and securely.

The New Safe Haven principles include the concept of restricting access to identifiable data which is required to support the anonymisation process of de-identifying records when required for secondary purposes use.

Safe Havens should be established, where:

- Information can be securely received and transferred.
- Paper-based information is stored securely in approved containers, as soon as practical.
- IT is not on view or accessible to unauthorised persons.
- All waste potentially containing security classified, personal or other sensitive information is securely retained until it can be securely disposed of or destroyed.
- Conversations discussing security classified, personal or other sensitive information can be held where they cannot be overhead by unauthorised persons.

The New Safe Haven requirements do not replace existing safe haven arrangements, there are however very specific requirements for managing the transformation of data from primary sources (such as patient records) into de-identified data for secondary purposes this also applies where controlled access to personal identifiable data is permitted by law.

New Safe Haven security must also conform to current legislation and in particular the Data Protection Act 1998 and NHS good practice policy and guidance concerning the handling of identifiable data as predicated by ISO 27001 and 27002. Adherence to relevant good practice is particularly important as the New Safe Haven may be virtual in nature and New Safe Haven staff may be distributed throughout the organization.

The New Safe Haven can be defined in terms of

- The activities to be undertaken
- The posts authorised to access identifiable data for the purpose of supporting de-identification. This will include Information Asset Owners and Information Asset Administrators, Data Quality team and the Business Intelligence team.

2. PURPOSE

This policy is concerned with the security of personal information, including patient information when used for purposes other than direct patient care. It applies to all staff involved in handling such data or are responsible for managing services which require access to de-identified information.

The New Safe Haven will exist to provide the means of restricting access to authorised users to identifiable data for the purposes of receiving and sending identifiable data that is expected to be used for secondary purposes and for supporting the de-identification of identifiable data.

Primary Use
Purposes that directly contribute to the safe care of the patient are classified as primary uses and include care, diagnosis, referral and treatment processes together with relevant supporting administrative processes, such as clinical letters and patient administration, patient management on a ward, managing appointments for care; as well as the audit or assurance of the quality of the healthcare provided.

Secondary Use
Secondary use is defined as
"*Any purpose which does not "directly contribute to the diagnosis, care and treatment of an individual and the audit/assurance of the quality of the healthcare provided" to the individual.*[1]
The health and social care has a system wide need to share secondary use information to facilitate improved outcomes for the patients and service users. This need will facilitate service and process redesign, service improvement, pathway planning, greater financial and process efficiency, ensuring the right services are available to the right patients in the right place, performance management, commissioning, contract monitoring; all of which do not require personal identifiable information such as the identity of patients.

3. POLICY DETAILS

Nature and Scope of Sharing
Each organisation is bound by the following legislation:
- General Data Protection Regulations 2016 (GDPR)
- Data Protection Act 2018 (DPA)
- Common Law Duty of Confidentiality (CLDC)

The Common Law Duty of Confidentiality is that if information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the data subject's consent, unless there is another legal basis or an overriding public interest.

Adherence to these and to other relevant legislation are captured and demonstration in the Information Sharing Gateway where organisations electronically sign based on assessment of risk via the Data Security and Protection Toolkit (DSPT) compliance level. In addition to these overarching principles, for each instance of sharing for a secondary use purpose a Record of the Processing

Activity / Data Mapping should be documented and where necessary a Data Protection Impact Assessment Completed.

Context of Sharing

The Data Subjects concerned are the citizens who have been treated by health and social care services within the STP or staff employed by respective organisations. By ensuring decisions are made at the most appropriate level and empowering local leads to plan long term needs of the people they serve, health and care systems can make simple practical improvements for local communities. Patients and staff must be informed via the organisational or staff privacy notices available on the Trust's website.

Compliance, Legality and Proportionality

Clauses within GDPR Articles 6 and 9 allow for the sharing of information for the provision of health and social care or treatment or the management of health and social care systems and services. Both Articles need to be met for sharing of special categories of data to be legitimate:

- 6(1)(e) – is that processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- 9(2)(h) - states that 'processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services'.

Whilst GDPR provides a legal Gateway, each organisation must be able to demonstrate that it is not breaching the Common Law Duty of Confidence with regard to individual patients – this can be achieved by:

- Meeting the requirements of the Caldicott principles
- Only sharing with Trusted parties
- Ensuring data minimisation
- Ensuring anonymisation at the point of use
- Ensuring appropriate security measures are in place
- Ensuring consistent privacy notices are in place
- Demonstrating a wider public interest.

The New Safe Haven will be defined in terms of a role given to members of staff approved for purposes by the Caldicott Guardian.

All patient information systems and databases must be within an electronic safe haven whereby access is limited AND password controlled for each authorised user.

When information is used for primary purposes the use requires knowing who the patient is. All primary purposes therefore require identifiable patient information to ensure patient safety.

All business processes, using patient level clinical data, within Cumbria Partnership NHS Foundation Trust must be documented. Business processes can include, but

are not limited to: the process for using patient data for secondary uses, the use of personal identifiable data for a combination of primary and secondary purposes.

Following assessment any processes that require de-identified data must be modified in line with this policy. Secondary use business processes should be initially documented and then reviewed regularly to assess any requirement to use de-identified data. Processing of data to enable data to be transformed into a suitable state for a secondary purpose is considered to be an additional purpose and as such constitutes a secondary use

All onward disclosure should be limited to anonymised data only

In order to be able to undertake processing these must be allowed under s.251 of the NHS Act 2006 to allow the access and use to proceed.

Certain data that may be held by the Trust is subject to legal requirements and NHS regulations that restrict any disclosure. These include:

- Procedures (abortions, neurosurgery for mental disorders, etc.)
- Diagnoses (AIDS / HIV, Abortions, STDs, IVF)

Recognition is also given to processing where there is no practical alternative to approval being given by Caldicott Guardian following a risk assessment

3.1 PRINCIPLES

3.1.1 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 public 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).

3.1.2 Caldicott Principles

The Caldicott Principles are:

- 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

3.2 NEW SAFE HAVEN SECURITY ACTIVITIES

The facilities can only be used by a small number of authorised staff sufficient to perform the functions and provide cover and back up to ensure continuity of service

- Authorisation of the staff performing roles in the New Safe Haven should be through the Caldicott Guardian and should be modelled on the local Registration Authority processes for accessing spine based applications in terms of the definition of positions, roles and permitted activities
- Where possible access to data which is required to be processed into a format suitable for secondary use must be password controlled by both individual user accounts AND passwords
- The systems used for the data transition processes must have appropriate access control mechanisms to restrict access to authorised users for the specific purpose of supporting de-identification processes
- The New Safe Haven may have a physical local if this involves paper based data flows such as faxes
- Access to physical safe haven areas should be restricted and equipment must have a coded password and be turned off during out of office hours.
- If there are paper based flows which involve patient identifiable data then post-delivery and equipment such as fax machines should be operated in secure areas in order to function effectively for New Safe Haven purposes

3.3 NEW SAFE HAVEN TECHNICAL PROCESSES

The New Safe Haven comprises the facilities to restrict access by authorised users to identifiable data for the purpose of supporting de-identification

The processes that are involved in transforming the data into an acceptable format for secondary use purposes include but may not be confined to:-

- Data quality checks: ensuring that the data contained within the record is accurate such as ensuring the patient's NHS number, PCT code and GP practice are correct
- Undertaking derivations of identifiable data items: for example deriving age at the start or end of an episode of care which relies on the patient's date of birth

- Undertaking record linkage: an example is to link records from different data sets or over time usually based on NHS number and cross checking dates of birth corroboration
- Pseudonymising personal data can reduce the risks to the data subjects and help you meet your data protection obligations but remains personal data within the scope of the GDPR.
- Applying de-identification processes such as redaction to anonymise data.
- Re-identification tests – can you re-identify the person? In order to be truly anonymised under the GDPR, you must strip personal data of sufficient elements that mean the individual can no longer be identified. If a motivated actor could use any reasonably available means to re-identify the individuals to which the data refers, that data will not have been effectively anonymised but will have merely been pseudonymised. This means that despite your attempt at anonymisation you will divulging personal data.
- Penetration Testing – identifying a level of risk to manage or address though testing

The Effective Anonymisation process is described in Appendix 1 and in the Effective Anonymisation guidance document.

3.4 SECONDARY USE OF PERSONAL DATA IN BUSINESS PROCESSES

Any secondary use data processing must only use de-identified data, all data processing activities must be regularly reviewed and assess if they are using personal data appropriately.

4. TRAINING AND SUPPORT

The Head of Information Governance and Data Protection Officer has overall responsibility for maintaining awareness of the New Safe Haven arrangements and how effective anonymisation will be implemented for all staff and to provide specific training where this is required.

This will be undertaken through mandatory induction, and annual refresher training as set out in the training needs analysis.

All staff working within the relevant teams will receive local training on the implementation of the New Safe Haven guidance and Effective Anonymisation procedures. This will be delivered by the Head of Information and Performance.

.

5. PROCESS FOR MONITORING COMPLIANCE

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

Aspect being monitored	Monitoring Methodology	Reporting		
		Presented by	Committee	Frequency
What	How	Who	Where	How often
Compliance with effective	Audit of data production processes	Head of Information	Information Governance Board	Annual

Aspect being monitored	Monitoring Methodology	Reporting		
		Presented by	Committee	Frequency
anonymisation procedures				
Compliance with safe haven guidance	Audit of data production processes	Head of Information	Information Governance Board	Annual

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

- Action plan
- Progress of action plan monitored by the Information Governance Board minutes
- Risks will be considered for inclusion in the appropriate risk registers

6. REFERENCES:

List any references for example national guidance or literature associated with this policy using Harvard referencing style.

Legislation.gov.uk. (2019). Data Protection Act 2018. [online] Available at: http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted [Accessed 9 Jan. 2019]

Digital.nhs.uk. (2019). Code of practice on confidential information. [online] Available at: https://digital.nhs.uk/binaries/content/assets/legacy/pdf/8/9/copconfidentialinformation.pdf [Accessed 9 Jan. 2019].

NHS Connecting for Health Pseudonymisation Implementation Project – Reference Paper 2 – Guidance on Business Processes and new safe havens.

NHS Connecting for Health Information Security Good Practice 2003 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/200506/Information_Security_Management_-_NHS_Code_of_Practice.pdf

BS ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements: This guidance is used to formulate an Information Security Management System (ISMS) (that is part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security) for those organisations wishing to fully comply with the standard.

BS ISO/IEC 27002:2013 Information technology - Security techniques - Code of practice for information security controls: This is the international standard for information security management. It provides a useful reference for those wishing to gain a greater understanding of the security controls, or those who wish to become fully compliant with the standard.

BS ISO/IEC 27005:2011 Information technology - Security techniques - Information security risk management: This International Standard provides guidelines for information

security risk management in an organisation, supporting in particular the requirements of an information security management (ISMS) according to ISO/IEC 27001.

NHS Digital. (2019). ISB1523: Anonymisation Standard for Publishing Health and Social Care Data - NHS Digital. [online] Available at: https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/standards-and-collections/isb1523-anonymisation-standard-for-publishing-health-and-social-care-data [Accessed 9 Jan. 2019].

NHS Digital. (2019). *ISB1523: Anonymisation Standard for Publishing Health and Social Care Data - NHS Digital*. [online] Available at: https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/standards-and-collections/isb1523-anonymisation-standard-for-publishing-health-and-social-care-data [Accessed 9 Jan. 2019].

Igt.hscic.gov.uk. (2019). [online] Available at: https://www.igt.hscic.gov.uk/KnowledgeBaseNew/NHS%20CFH_Pseudonymisation%20Implementation%20Project%20-%20Guidance%20on%20Business%20Processes%20and%20New%20Safe%20Havens.pdf [Accessed 9 Jan. 2019].

ico.org.uk. (2019). Anonymisation: managing data protection risk code of practice. [online] Available at: https://ico.org.uk/media/1061/anonymisation-code.pdf [Accessed 10 Jan. 2019].

Safe Haven Directory
https://digital.nhs.uk/services/organisation-data-service/services-provided-by-the-organisation-data-service/safe-haven-directory

The Information Commissioner's Office (ICO) – This is the regulatory body with responsibility for monitoring compliance with the Data Protection Act. The Trust is required to register with the ICO to define what personal data it processes and for what purpose. https://ico.org.uk/

7. ASSOCIATED DOCUMENTATION:

List any Trust policies (hyperlinked to the relevant policies on the policies web page) and procedures that link to this policy.

Confidentiality Policy – Joint POL/IG/005
Data Protection Act Policy – Joint POL/IG/001
Information Sharing (Disclosure) Policy - Joint POL/IG/003

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.

The Chief Executive has ultimate responsibility for ensuring that the appropriate systems and processes are in place to protect the collection, recording and use of person identifiable data or information.

8.2 Executive Director Responsibilities: Director of Workforce/OD

All policies have a designated Executive Director and it is their responsibility to be involved in the development and sign off of the policies, this should ensure that Trust policies meet statutory legislation and guidance where appropriate. They must ensure the policies are kept up to date by the relevant author and approved at the appropriate committee.

The **Senior Information Risk Owner (SIRO)** is responsible to the Chief Executive and the Board of Directors for the development and implementation of the information risk policy and risk assessment, act as an advocate for information risk on the board and in internal discussions, and provide written advice to the Chief Executive on the content of the Statement of Internal Control relating to information risk

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.

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.

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.

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.

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.

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.

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

8.3 Managers Responsibilities:

Head of Information Governance and Data Protection Officer is responsible to the SIRO for the operational management data protection, the confidentiality code of conduct, and information security and for ensuring that safe haven arrangements conform to NHS standards

Information Asset Administrators, Information Asset Owners and all processors of personal information, such as the Information Management teams are responsible for managing the New Safe Haven processes and applying the rules of de-identification, pseudonymisation or anonymisation to personal information within a New Safe Haven or any data process activity requiring de-identification. Other staff may be approved by the Caldicott Guardian to undertake Safe Haven processes on a case by case or exception basis.

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.

8.4 Staff Responsibilities:

All Trust Staff involved in the processing of person identifiable information and Managers who have responsibilities for those staff must ensure the information remains secure and confidential at all times.

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.

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.

8.5 Approving Committee Responsibilities: Joint Information Governance Board

The Chair of the approving committee 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.

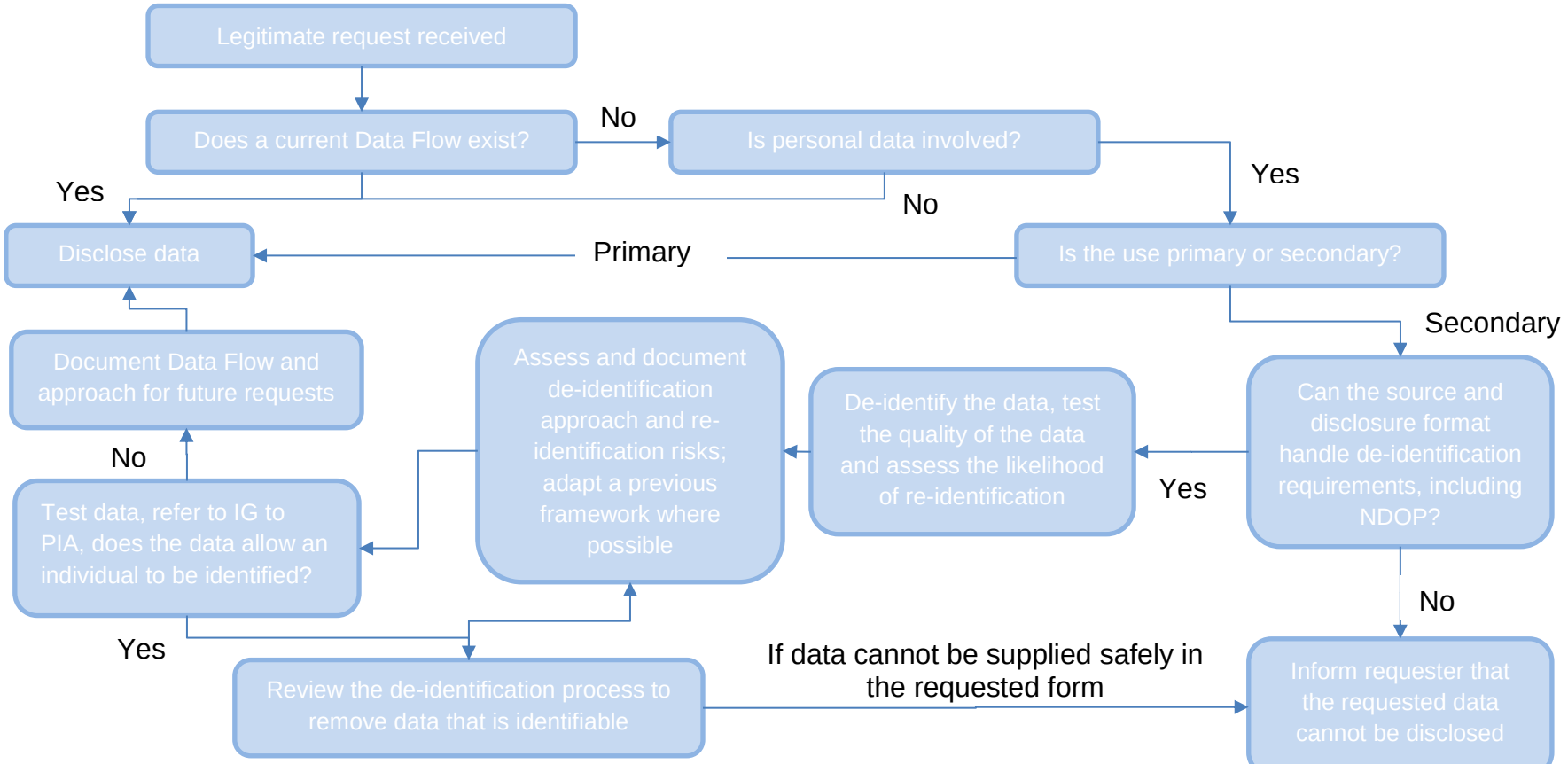
9. ABBREVIATIONS / DEFINITION OF TERMS USED

ABBREVIATION	DEFINITION
AHRA	Access to Health Records Act 1990
CEO	Chief Executive Officer
CPFT	Cumbria Partnership NHS Foundation Trust
DPA	Data Protection Act 2018
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DS&Ptk	Data Security and Protection Toolkit
FoIA	Freedom of Information Act 2000
GDPR	General Data Protection Regulation
ICO	Information Commissioner's Officer
NCUH	North Cumbria University Hospitals NHS Trust
NDOP	National Data Opt Out
PID	Personal Identifiable Data
PII	Personal Identifiable Information
SIRO	Senior Information Risk Owner

TERM USED	DEFINITION
Caldicott Guardian	The Caldicott Guardian is appointed by the Board of directors to oversee the safe and secure use and sharing of patient information.
Data Protection Act 2018 (DPA)	The DPA supplements the major reforms to data protection laws that are contained in the General Data Protection Regulation (GDPR). It regulates the processing of personal data by companies, public authorities, law enforcement and intelligence agencies.
Data Protection Officer	The Data Protection Officer (DPO) ensures, in an independent manner, that an organisation applies the laws protecting individuals' personal data.
General Data Protection Regulations	The General Data Protection Regulation (EU) 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA).
Information Asset Administrators	Information Asset Administrators ensure that policies and procedures are followed, recognise actual or potential security incidents, consult their IAO on incident

TERM USED	DEFINITION
	management, and ensure that information asset registers are accurate and up to date.
Information Asset Owners	Information Asset Owners are senior individuals involved in running the relevant business. Their role is to understand and address risks to the information assets they 'own' and to provide assurance to the SIRO on the security and use of those assets.
NHS Code of Practice: Confidentiality 2003	Annex A1 Project patient information "Care must be taken, particularly with confidential clinical information, to ensure that the means of transferring from one location to another is secure as they can be".
Pseudonymising	Pseudonymisation is a data management and de-identification procedure by which personally identifiable information fields within a data record are replaced by one or more artificial identifiers, or pseudonyms.
The Information Commissioner's Office (ICO)	This is the regulatory body with responsibility for monitoring compliance with the Data Protection Act. The Trust is required to register with the ICO to define what personal data it processes and for what purpose.

APPENDIX 1 - DATA DISCLOSURE PROCESS – WITH EFFECTIVE ANONYMISATION AND INFORMATION GOVERNANCE



PIA – Privacy Impact Assessment, IG - Information Governance, NDOP – National Data Opt Out

DOCUMENT CONTROL

Equality Impact Assessment Date	
Sub-Committee & Approval Date	*Joint Information Governance Board 17/05/2019*

History of previous published versions of this document:

Version	Ratified Date	Review Date	Date Published	Disposal Date
1.0	09/12/2014	01/05/2018	01/02/2014	

Statement of changes made from version

Version	Date	Section & Description
1.1	2019	• Reviewed, included GDPR and NDOP
1.2	15/05/2019	• General amendments
		•

List of Stakeholders who have reviewed the document

Name	Job Title	Date

[i] National Information Governance Board (2011), Information Governance for Transition, p.42