



Public – To be published on the Trust external website

Title: Data Management Policy

Ref: IT-0030-v3

Status: Ratified

Document type: Policy

Contents

1	Introduction	4
2	Why we need this policy	5
2.1	Purpose	5
2.2	Objectives.....	5
3	Scope.....	6
3.1	Who this policy applies to	6
3.2	What this policy applies to	6
3.3	Roles and responsibilities.....	6
3.3.1	NHS Number Responsibilities	10
4	Policy.....	11
4.1	Legislation and data standards.....	12
4.1.1	Data Protection Act 2018 and UK GDPR.....	12
4.1.2	Confidentiality.....	12
4.1.3	Pseudonymisation/de-identification of patient data	12
4.1.4	Information standards notices	12
4.1.5	Clinical coding.....	13
4.1.6	Data Security and Protection Toolkit.....	13
4.1.7	Use of the NHS Number	13
4.2	Data quality	13
4.2.1	Information data quality assurance	13
4.2.2	Principles of good data quality	14
4.2.3	Risks of poor data quality	16
4.2.4	Professional obligations	17
4.2.5	Monitoring and Action on Data Quality.....	17
4.3	Pseudonymisation / de-identification of Patient Identifiable Information (PII)	18
4.3.1	National Data Opt-Out.....	21
4.4	Use of the Trust's file storage network	21
4.4.1	Accessing the network	21
4.4.2	Home (H:\) drives	22
4.4.3	Shared (S:\) drives	23
4.4.4	OneDrive/MS Teams/Sharepoint	24
4.4.5	Storage limits	24
4.4.6	Security	25
4.4.7	Maintenance and availability	25
4.5	Security of information, equipment, and computer media	26
4.5.1	Clear Desk	26
4.5.2	Electronic or computerised information and equipment	27

4.6	Reporting data management issues.....	27
5	Definitions.....	28
6	Related documents	31
7	How this policy will be implemented	31
7.1	Implementation action plan.....	32
7.2	Training needs analysis.....	32
8	How the implementation of this policy will be monitored.....	32
9	References	34
10	Document control (external).....	35
	Appendix 1 - Equality Analysis Screening Form	37
	Appendix 2 – Approval checklist.....	40

1 Introduction

This document explains the Trust’s policy for the access, use, storage and processing of information and data in all Trust systems. This document also describes the importance of data quality, and how this is monitored and improved in the organisation.

This policy aligns with the Data Protection Act 2018, and UK General Protection Regulation (01 January 2021).

“High quality data is important to the NHS as it can lead to improvements in patient care and patient safety. Quality data plays a role in improving services and decision making, as well as being able to identify trends and patterns, draw comparisons, predict future events and outcomes, and evaluate services.” *NHS England (2022), NHS England » Data quality Improvement*

This policy is critical to the delivery of Our Journey to Change and our ambition to co-create safe and personalised care that improves the lives of people with mental health needs, a learning disability or autism. It helps us deliver our three strategic goals as follows:

- This policy supports the trust to co-create a great experience for all patients, carers, and families from its diverse population by ensuring data is recorded securely, accurately, and timely.
- This policy supports the trust to co-create a great experience for our colleagues by ensuring there is clear guidance on how data is managed in the organisation. Good quality data will help inform good practice and data-driven decision making, improving the “Well led and managed” sub-goal.
- This policy supports the trust to be a great partner by ensuring that the data we share is well structured, of good quality and reliable.

2 Why we need this policy

2.1 Purpose

This policy ensures:

- Staff understand their responsibilities when using all Trust information systems especially in the areas of:
 - quality
 - confidentiality
 - security
 - appropriate access

in relation to data and information whether patient or staff

- Correct access is given to the information systems staff need to carry out their duties, along with the following policies/procedures:
 - IT-0011: Registration Authority Policy
 - IT-004: Network User Access Procedure
 - IT-0031: Access to Information Systems Policy
- Staff have clear guidance on Data Management principles
- Compliance with the relevant legislation.
 - The Data Protection Act 2018 and UK GDPR
 - The NHS Confidentiality Code of Practice 2003
 - The Eight Caldicott Principles
 - Information Commissioner's Office Anonymisation: managing data protection risk code of practice
 - NHS Number Operational Information Standards

2.2 Objectives

This policy aims to reinforce Tees, Esk and Wear Valleys NHS Foundation Trust's commitment to high standards in data management. The policy identifies roles and responsibilities for data quality, information security and confidentiality of all person identifiable data.

[Section 4](#) of this policy draws together the various areas of Data Management including:

- Data Quality
- Data / Information storage and Information Security
- De-identification (Pseudonymisation) of Patient Identifiable Information (PII)
- Best practice in Information Standards and coding including the use of NHS number and ICD10 clinical codes

3 Scope

3.1 Who this policy applies to

- All staff employed by, or seconded to, Tees Esk and Wear Valleys NHS Foundation Trust who use Trust information systems
- All staff employed by, or seconded to, Tees Esk and Wear Valleys NHS Foundation Trust who collect information for entry onto Trust information systems
- Staff of those organisations from whom we commission services

3.2 What this policy applies to

- All information that is entered onto a computerised system whether centrally or locally maintained.
- Any new systems implemented within the trust.
- Any paper-based systems held and maintained by 'staff' within the trust ([see 3.1 'Who this policy applies to'](#))
- All systems including:
 - clinical systems such as the Electronic Patient Record, and
 - non-clinical systems, including Finance, Human Resources, Facilities and Risk Management.

3.3 Roles and responsibilities

Role	Responsibility
Director of Finance, Information and Estates/Facilities	<ul style="list-style-type: none"> • Enforcing this policy

<p>Clinical Chief Information Officer</p>	<ul style="list-style-type: none"> • Ensuring the quality of clinical information
<p>Head of Business Intelligence and Reporting</p>	<ul style="list-style-type: none"> • Providing professional advice to the Trust about this policy. • Assessing any data quality issues identified and raising concerns with the Digital Performance and Assurance Group. • Advising further action if needed, e.g., escalating to the Caldicott Guardian. • Managing the Business Intelligence and Clinical Outcomes teams and monitoring the secondary use of patient data. • Reviewing and updating this policy.
<p>Head of Information Governance and Data Protection Officer</p>	<ul style="list-style-type: none"> • Informing and advising the Trust and employees whose tasks involve data processing regarding their statutory obligations • Provide advice regarding Data Protection Impact Assessments • Monitor compliance with the Data Protection Act 2018 and UK GDPR
<p>All staff</p>	<ul style="list-style-type: none"> • Ensuring that they understand this policy and its supporting standards and guidelines. • Building these standards and guidelines into local processes and ensuring ongoing daily compliance. • Reporting incidents relating to breaches or suspected breaches of confidentiality or information security on Trust incident reporting system and to the Information Governance Section within Digital and Data Services for immediate investigation. • Maintaining data standards in accordance with national developments • Maintaining confidentiality - staff must not pass on PII intended for secondary uses to each other (for definition of 'secondary use' see section 5). Data for secondary use must be sourced from the Trust's main Safe Haven or Local Safe Havens, where requests will be logged and data de-identified appropriately. For further detail, please consult the 'Records management and safe haven' procedure, Ref CORP-0026-007. • Ensuring the timely, accurate and complete input of their data onto the appropriate trust information system or onto data recording sheets • Ensuring that they have the appropriate level of knowledge and skills for using the information systems • If unable to enter the information themselves, providing input staff with full completed data sheets in a timely manner

	<ul style="list-style-type: none"> • Confirming that demographic and key personal data such as GP, ethnicity, etc, is accurate and up to date. • Monitoring the data held for any data quality issues and reporting any concerns to the appropriate System Owner or System Administrator
System Owners	<ul style="list-style-type: none"> • Monitoring and communicating changes implemented via Information Standards Notices (ISNs) • Ensuring that all systems including the Electronic Patient Record ensure the collection of high-quality data, in line with national standards • Establishing and disseminating monitoring reports from the system to the right staff and service, detailing key data quality issues • Reporting any concerns to the Service Manager with responsibility for the system • Following the System Specific Policy when introducing or upgrading an information system • Logging system security issues with the Information Security Officer • Maintaining systems following any concerns • Maintaining a list of the authorised users for each system containing PII. A full access list is maintained by the information service desk.
Information Asset Owners / Administrators	<ul style="list-style-type: none"> • Controlling system access to information assets for staff who need to use those systems to access patient data for secondary uses. Patient data intended for secondary use must be accessed via the Trust's New Safe Haven process for the secondary use of patient data, ideally the Main Safe Haven. • Regularly reviewing access to systems that contain person identifiable data via system maintenance. • Closing system accounts for those staff who no longer need access. • Disabling temporary access to systems when the task or project is complete. • Ensuring information sharing agreements and Data Protection Impact Assessments (DPIA) are approved and in place where partner agency access to Trust systems is required before any processing of PII takes place. • Ensuring DPIAs are reviewed when changes are proposed to processes that involve the use of person identifiable data.

<p>Business Intelligence and Clinical Outcomes Teams</p>	<ul style="list-style-type: none"> • Acting as the Trust’s main Safe Haven team for the secondary use of patient data. • De-identification or pseudonymisation of patient data before secondary use. • Converting pseudonymised or de-identified data back to its identifiable form if the data is subsequently required for primary use. • Supporting staff who need advice or help with any aspect of Data Management. • Maintaining, developing, and supporting the pseudonymisation of patient data within the Trust’s IIC reporting system.
<p>Caldicott Guardian</p>	<ul style="list-style-type: none"> • Approving all procedures that relate to the use of PII.
<p>Information Governance Team</p>	<ul style="list-style-type: none"> • Providing all staff with up-to-date guidance on information governance and data protection issues.
<p>Directors, Service Directors, Heads of Service</p>	<ul style="list-style-type: none"> • Ensuring staff are aware of and comply with Trust policies and procedures and that policy change is reflected in practice. • Ensuring that any breach of confidentiality or information security, whether actual or suspected, is reported on Datix and to the Information Governance Section within Digital and Data Services for immediate investigation. • Ensuring that, when staff use patient data for secondary uses, only authorised staff will have access to PII. Non-clinical staff who have not been identified and registered as Local Safe Haven staff for the secondary use of patient data must not have access to PII. • Escalating to Information Governance Section within Digital and Data Services when a need for ongoing access to PII for secondary use is identified. Approval will be made via the Information Governance Group. • Ensuring that staff are aware of their responsibilities. • Ensuring that support is provided to enable the timely, accurate and complete input of data onto the appropriate Trust information system. • Ensuring that all staff are aware of their responsibilities for checking and maintaining up-to-date demographic data. • Ensuring that any data quality issues are addressed quickly and reported to the System Owner or Administrator. • Ensuring that all working procedures are fully documented, regularly updated and available to all staff.

	<ul style="list-style-type: none"> Monitoring compliance with this policy and appropriate use of Information Systems as detailed in the System Specific Policy Ensuring that communication exists between the clinical and corporate services to resolve data quality issues. Ensuring that all job descriptions support and enforce the responsibilities within this policy.
--	--

3.3.1 NHS Number Responsibilities

Role	Responsibility
All Staff registering patients on a Clinical Information System	<ul style="list-style-type: none"> Following the NHS Number Procedure when NHS Number is input into a system. Ensuring the NHS number is obtained from the referrer and recorded on the system and all documentation. Where the NHS number is not available, undertaking a trace on the Demographic Batch Service or the Clinical Spine Application as appropriate. Ensuring that they have the appropriate training for the Demographic Batch Service or the Clinical Spine Applications. Ensuring that the demographic information for any patients currently registered is verified and up to date. Ensuring that the NHS number is documented on all clinical documentation in the paper record.
Service Managers/Modern Matrons/Team Leaders (with responsibility for staff collecting patient demographic data):	<ul style="list-style-type: none"> Ensuring that the NHS number is captured for all active patients within their service. Ensuring that all staff are aware of their responsibilities for capturing the NHS number for patients. Arranging training for any members of staff requiring access to the Demographic Batch Service of the Clinical Spine Application as appropriate. Ensuring that all working procedures are fully documented, regularly updated and available to all staff and that staff understand and comply with Trust policies and procedures. Ensuring that all working procedures provide contingency for staff absence. Monitoring compliance with this procedure and appropriate use of Clinical Information Systems.

	<ul style="list-style-type: none"> Ensuring staff are aware of appropriate Trust policies and procedures and changes within policies are reflected in practise.
System Owners	<ul style="list-style-type: none"> Monitoring and disseminating regular reports on missing NHS numbers to the clinical services. Reporting any concerns to the appropriate Service/General Manager and Information Manager. <p>NB: batch tracing is only undertaken for Paris and is the responsibility of the Paris System Owner or Administrator.</p>
Digital and Data Services	<ul style="list-style-type: none"> Providing training on the applications which access the National Clinical Spine

4 Policy

The Trust recognises that using information is essential in all aspects of our business, as is collecting data and information on the population that we serve. This allows us to effectively:

- treat our patients and provide continuity of care
- monitor and manage service level agreements
- develop commissioning plans
- monitor health improvement programmes
- support clinical governance
- understand the health needs of the population
- monitor the experience of our patients, carers, and staff

As NHS information systems have grown to accommodate the increasing levels of patient data, so too have concerns about the quality, security, and confidentiality of that data. This policy describes the Trust’s framework within which information is to be used, processed, and stored.

4.1 Legislation and data standards



Any breaches of Data Protection or confidentiality may lead to disciplinary action

4.1.1 Data Protection Act 2018 and UK GDPR

- Applies to computerised and manual records for living individuals - whenever the records were generated.
- Under the Act individuals have a right to access information about themselves and take steps to rectify or destroy inaccurate data.
- Article 5(d) of the Act states that “Personal data shall be accurate and ... kept up to date.” This means we have a legal duty to maintain and update all records (patient and staff), to ensure that they correctly reflect the demographic details and, in patient records, clinical care.

4.1.2 Confidentiality

- The HSCIC Code of Practice on Confidential Information emphasises the importance of identifying the purpose for the use of information in detail
- Where use of confidential data is essential, the minimum amount of personal confidential data should be transferred or accessible.
- When analysing data, “Quality should be monitored, assured and reported on, taking account of internationally agreed practices”¹

4.1.3 Pseudonymisation/de-identification of patient data

- See section 4.3 – [Pseudonymisation/De-identification of Patient Identifiable Information](#)

4.1.4 Information standards notices

- Issued on a regular basis to inform about and support changes to national standards.

¹ HSCIC Code of practice on confidential information, 2014



Information systems must support the definitions within the Data Dictionary and the Information Standards Notices and ensure these are also reflected within care pathways.

4.1.5 Clinical coding



Processes to support the standards of the NHS Clinical Coding Manual must be in place so that the coding of clinical data is accurate, complete, and timely. See [Clinical Coding Procedure](#) on Trust Intranet.

4.1.6 Data Security and Protection Toolkit

- A framework for assuring information quality.
- Requires key data items to be monitored against national definitions.

4.1.7 Use of the NHS Number

- Staff must use the NHS number accurately and record it where required in all information systems in use by the trust appropriately.
- See [3.3.1 – Roles and Responsibilities](#) for the use of the NHS number
- See [NHS Number Procedure](#), accessible on the Trust Intranet, for appropriate use of the NHS number

4.2 Data quality

4.2.1 Information data quality assurance

Who	What	When	Why
Digital Performance and Assurance Group	To monitor and oversee the data quality within the organisation, which covers all information systems managed by	Monthly	Provide strategic leadership, direction, and oversight

	Digital and Data Services		
Data Quality Working Group	To monitor Trust-wide data quality issues and develop action plans to take remedial action. The group will also take a proactive role in ensuring that existing systems are used to record information in line with agreed trust and National standards and use systems to proactively view, monitor and improve data quality on an ongoing basis.	Monthly	Develop action plans to improve the data quality of the organisation. Monitor improvements and report progress, escalating any areas of concern. Monitor nationally available data quality metrics. Raise any business/clinical processes that are leading to poor data quality.
NHS England	Assesses the completeness of data to make assessments for specific outcomes (i.e., employment) using MHSDS	Monthly	For monitoring compliance by NHS FTs with their terms of Authorisation

The trust has been subject to several audits in which data quality has been measured and targets established to improve the quality of the data captured on information systems.

4.2.2 Principles of good data quality


Data is an acceptable qualitative level when it is:

- ✓ valid
- ✓ complete
- ✓ consistent
- ✓ accurate and up to date
- ✓ relevant
- ✓ available when needed and
- ✓ secure; in compliance with Data Protection legislation and Caldicott guidelines.


Issue	Action
Trust systems must be kept up to date	<ul style="list-style-type: none"> • Ensure they accurately reflect changes to national standards and data definitions. • Communication must ensure that updates can be disseminated efficiently and effectively to all affected staff.
Standard operating procedures	<ul style="list-style-type: none"> • Must be developed to facilitate the capture of data.
Data must be valid	<ul style="list-style-type: none"> • Data must be clinically valid, i.e., the correct clinical information, such as the appropriate diagnoses, must be recorded within the patient's case notes and reflected on the system. • The correct coding structures must be used to record the data, i.e., all codes used within Trust systems must comply with national standards and guidelines.
Data must be complete	<ul style="list-style-type: none"> • Mandated data items must be collected and reviewed appropriately. • Default codes must not be used as an acceptable alternative to the correct information; they must only be used after all methods of obtaining the information have been exhausted.
Clinical data must be coded	<ul style="list-style-type: none"> • To input onto the Electronic Patient Record accurate and complete coded information within the designated time scales to support the information requirements and commissioning of the Trust. • To adhere to national standards and classification rules and conventions as set out in the WHO ICD-10 Volumes 1-3, Clinical Coding Instruction Manual ICD-10 and OPCS-4 and publications of the Coding Clinic
Consistency	<ul style="list-style-type: none"> • The information recorded must be consistent across data source.
Data must be accurate and up to date	<ul style="list-style-type: none"> • The system must accurately reflect the information that is maintained within other records/systems and be updated in a timely fashion.
Relevant level of data collected	<ul style="list-style-type: none"> • The level of data collected must be relevant to the purpose. Systems must not collect additional information that is not appropriate.
Data must be available in a timely manner	<ul style="list-style-type: none"> • All data must be recorded in a timely manner to ensure: <ul style="list-style-type: none"> ○ Information is available when required ○ To ensure patient safety

	<ul style="list-style-type: none"> ○ The quality of the information reports submitted to the Department of Health and Trust Commissioners is of a high standard.
Training	<ul style="list-style-type: none"> ● Staff must be trained on the importance of data quality, collection routines and data entry. ● Mechanisms must be established for the dissemination of updates to national standards.

4.2.3 Risks of poor data quality

 Information collected on the Trust’s information systems is used to inform clinical care, manage resources, for business and planning development, record financial flows and improve services within the Trust. If data is not collected efficiently and effectively several risks can occur.

Issue	Risk
Lack of demographic details	<ul style="list-style-type: none"> ● Misidentification of a patient which could lead to: <ul style="list-style-type: none"> ○ Misallocation of future appointments ○ Delay in providing follow-up care.
Inconsistent collection of key data items	<ul style="list-style-type: none"> ● Unsuccessful and ill-informed decisions for service improvement.
Inaccurate recording of contact information	<ul style="list-style-type: none"> ● Resource issues, as planning managers cannot make informed decisions on service use.
Poor data quality	<ul style="list-style-type: none"> ● Risk to planning and performance management
Failure to record key data items	<ul style="list-style-type: none"> ● Impact on commissioning data ● Lack of payment for services by commissioners ● Risk to Foundation Trust status and the Trust’s ability to obtain correct funding outside of Block Contracts.

 The above risks are examples and not an exhaustive list of the risks associated with poor data quality. All steps must be taken to ensure the data collected within Trust systems is robust enough to minimise any issues.

4.2.4 Professional obligations

Staff must follow their own professional body’s code of practice which details record keeping and data quality. This includes but is not limited to:-

Who	What
General Medical Council	“Documents you make (including clinical records) to formally record your work must be clear, accurate and legible. You should make records at the same time as the events you are recording or as soon as possible afterwards.”
Nursing and Midwifery Council	“demonstrate the ability to keep complete, clear, accurate and timely records” and “write accurate, clear, legible records and documentation”

4.2.5 Monitoring and Action on Data Quality

The Data Quality Working Group (DQWG) monitors Trust-wide data quality issues and develops action plans to take remedial action. The group takes a proactive role in ensuring that systems are used to record information in line with agreed Trust and National standards and use systems to proactively view, monitor and improve data quality on an ongoing basis.

The Data Quality Assessment Tool (DQAT) is a fundamental part of our “assurance” to Trust Board, providing confidence that we have clearly defined measures/key performance indicators, that are robust and fit for purpose and that our testing processes ensure that the measures remain accurate and up to date. The tool provides assurance on the quality of data being reported as part of our Integrated Performance Dashboard, focussing on our quality and confidence in:

- the source of the data
- the accuracy and consistency of the data
- the measure construction
- the assurance/audit testing undertaken

The results (scores) from the data quality assessment are reported to Trust Board within our Integrated Performance Report and are overseen by the DQWG to ensure that all improvement actions identified as part of the assessment are completed.

Strategic improvements in the monitoring and oversight of Data Quality are described and implemented within the Digital and Data Journey for Change.

The Trust's Business Intelligence (BI) system, the Integrated Information Centre (IIC) provides all Trust employees with access to data from multiple Trust systems, with data as little as one hour behind the operational systems. Data is available in the IIC in both transactional form and transformed to align with business processes to provide multi-layered visibility.

The quality of Clinical Coding undergoes an external audit annually, in line with the requirements of the Data Security and Protection Toolkit (DS&PT).

The Data Quality Maturity Index (DQMI) is a monthly publication about data quality in the NHS, which provides data submitters with timely and transparent information. DQMI performance is measured via the Digital and Data department measures and is reported into the Trust's governance structure.

Cito employs pathways which prompt the clinician to enter data in the correct place and in a timely manner. Care is created collaboratively with the Patient and Carer making the clinical record transparent (where appropriate and in accordance with law) and facts are verified thus improving the quality of the overall patient record. Key documents are shared with the ICS shared care records viewers and their patient portals. This visibility of records and data emphasis on the need for good data quality and supports the data quality agenda within the Trust.

The Trust's Business Intelligence Research and Statistics team provide bespoke data analysis and deep dives based upon the needs of the organisation. A key part of this work involves the assessment and portrayal of the quality of the data within the scope of the work, the impact this may be having on the performance of the organisation and any limitations data quality may have on data-driven decision making.

4.3 Pseudonymisation / de-identification of Patient Identifiable Information (PII)

It is NHS policy and a legal requirement that, when patient data is used for purposes not involving the direct care of the patient, (i.e., Secondary Use) the patient **must not** be identified **unless** other legal means hold, such as has the patient opted out via National

Data Opt-Out or Section 251 approval. See [Information Standard: DCB3058: Compliance with National Data Opt-outs](#).

It is important to understand:

- the difference between Primary and Secondary use; and
- data items that are Patient Identifiable.

Item	Description
Primary use	<ul style="list-style-type: none"> Information that is used for healthcare and medical purposes. This would directly contribute to the treatment, diagnosis, or the care of the individual. This also includes relevant supporting administrative processes and audit/assurance of the quality of healthcare service provided. Clinicians using PII for Healthcare Medical purposes must follow the guidelines laid down in the Data Protection Act, the Caldicott Guidelines and best practice regarding patient confidentiality always.
Secondary use	<ul style="list-style-type: none"> Information that is used for non-healthcare and medical purposes, e.g., research purposes, audits, service management, commissioning, contract monitoring or reporting. Secondary use PII must be limited and de-identified to maintain confidentiality. When PII is being shared for secondary use purposes by any member of staff you must refer to the Moving Records and Other Sensitive Information procedure (see hyperlink at section 6 'Related Documents' below). This must be done by Trust Safe Haven staff.
PII data items	<p>Information that, on its own or with other information, can identify a person.</p> <p>PII data items are:</p> <ul style="list-style-type: none"> Name - including last name and any forename or aliases Address – including any current or past address of residence Date of birth Postcode - including any current or past postcode of residence NHS number Ethnic category Local Patient identifier Hospital Spell number Patient pathway identifier SUS spell ID Unique booking reference number Social Service Client number Date of death

The above categorisation of data must be recorded in the relevant Information Flows register and reviewed annually by the relevant Information Asset Owner in line with Data Protection Act guidelines.

4.3.1 National Data Opt-Out

National Data Opt-Out is a single opt out model that allows patients to opt out of having their confidential patient information used for research and planning purposes.

The national data opt-out does **not apply** where:

- data is shared for individual care
- there is a risk to public health or data is required for monitoring and control of infectious diseases, for example during an epidemic
- there is an overriding public interest, for example:
 - reporting of gun wounds in line with GMC guidance
- there is a legal requirement to share information, for example:
 - investigations by regulators of professionals (e.g., General Medical Council investigating a registered doctor's fitness to practice)
 - NHS fraud investigations
- the patient has consented to take part in a specific project
- where anonymised data is used.

4.4 Use of the Trust's file storage network

4.4.1 Accessing the network



- Staff cannot access any of the Trust's information systems or resources until they have completed the Trust Network Security Course.
 - Staff must complete Data Security and Protection Training for New Starters within 5 days of starting employment with the Trust. Instructions for accessing and completing the training will be included with the new starter email sent to the new employee's line manager.

- For guidelines on how to obtain a network account, see the Network User Access Procedure on the Trust Intranet.

- Staff can only use the Trust's network file storage system for Trust business. (In normal circumstances, patient information must be stored within the appropriate patient system (e.g., PARIS, IAPTus, SsID) or the Trust's network drive.
- All files created and stored on the Trust's network file storage system, including back-up copies, are Trust property and are not to be considered private.
- The Trust retains the right to investigate and remove from its network file storage system any material it views as offensive or illegal.
- This policy recognises the value of electronic information to the Trust and its patients. Staff must treat the storage of such information with care and follow the principles of security, confidentiality, freedom of information, and corporate records management.
- Misuse of the Trust's network file system can create potential liability, compromise the trust's confidential information, and otherwise adversely affect the trust's interests and reputation.



No information of any kind is to be stored on the C drive (local hard disk) of any desktop PC.

4.4.2 Home (H:\) drives

Users of the Trust's computer network will have a home drive for storing 'work in progress' files or work-related information of a confidential nature. The following conditions apply to a user's home drive:



Do not share accounts and passwords under **any** circumstances.

- Access to a networked home drive is restricted to its associated user account.
- If there is a genuine business need, a manager may be given temporary access to an absent user's home drive. (Refer to Network Access Policy)
- Users are directly responsible for all content stored in their home drive and may be subject to disciplinary or legal action if any illegal or unauthorised content is found in a home drive.

- Users are responsible for managing data stored in their home drives. Remove data that is no longer needed and that is not classified as a corporate record. Data that needs to be stored for a specified retention period must be indexed and archived. (For advice contact information service desk or tewv.ig@nhs.net .

4.4.3 Shared (S:) drives

Users will also have access to a shared drive (Drive S:) for sharing files with colleagues within their directorate. The following conditions apply to such shared drives:



Do not share accounts and passwords under **any** circumstances.

- A shared drive is the best way to share common data files on the network file storage system.
- Each directorate has a shared drive with access restricted to staff of that directorate. The shared drive contains subfolders structured according to the Trust's corporate management approach.
- Folders can be setup so that access is only permitted to the respective group members. These will be strictly controlled so may not be the best approach to securing documents - please seek advice and guidance from the Service desk.
- Shared folder creation must be kept to a minimum – if possible, create a subfolder under an existing folder and password protect any confidential or sensitive documents.
- The creation of a new shared folder may be requested from the Information Service Desk (ONEform), who will ensure that the shared folder is appropriately named and can only be accessed by the required group members.
- Managers are directly responsible for all content stored on the shared drives by their staff.
- Managers are responsible for ensuring that data that is no longer needed is removed from their shared drives. If the data is classified as a corporate record, it must be archived and indexed appropriately.

4.4.4 OneDrive/MS Teams/Sharepoint

Users have access to store files online in the Microsoft Cloud through applications such as OneDrive, MS Teams and Sharepoint.



Do not share accounts and passwords under **any** circumstances.

- The creation of a MS Team site needs to be done by an administrator. Only requests that meet the following criteria will be approved:
 - A team that is for staff within a specific service within a locality / department / directorate.
 - A team that is for a cross functional piece of work involving staff from specific specialties, localities, or directorates.
 - A team that is for a trust wide group or meeting.
 - A team that is for a specific project involving staff from multiple localities / specialties / departments / teams.
 - A team that is created for trust wide professional groups.
 - A team that is created for staff across the organisation to network on a specific topic(s). MS Teams sites will follow a standard naming convention to ensure consistency and ease of use.
- To request the creation of a MS Team site you can log a call via the IT help page and select Applications Hardware and Infrastructure > Applications > Application – MS Teams.

4.4.5 Storage limits

- Quotas limit the number of files that can be stored in each area of the shared drive to help maintain the performance and availability of the network file storage system.

- Quotas are set and reviewed by the Digital and Data Services department and reflect the business needs of the Trust.
- Users are responsible for maintaining their home and shared drives and must either delete information that is not a Trust record or save the record in the appropriate filing system. If you have any doubt about the value of a document as a record, contact the Information Governance Team Mailbox via tewv.ig@nhs.net.

4.4.6 Security

- All data on the network file storage system is backed-up regularly by the Digital and Data Services department to mitigate the loss of electronic information through accidental or malicious acts.
- All back-up media is stored in a secure location and data which has been deleted or corrupted may be recoverable from it (contact the Information Service Desk).
- Digital and Data Services department will provide a reliable network file storage system. Nevertheless, users are ultimately responsible for the appropriate safeguarding of their own data.
- Users are responsible for the security of data they do not store on the network file system (e.g., files stored on Trust-issued encrypted memory sticks etc). You must store all original copies of files on networked home or shared drives (or appropriate specific system).
- Unless indicated otherwise, records may be deleted in line with the Trust's [record retention and disposition procedure](#). For further guidance contact the IG team via tewv.ig@nhs.net.

4.4.7 Maintenance and availability

- Digital and Data Services department monitor and maintain the availability of the network file storage system and develop it in accordance with the business needs of the Trust.
- Sometimes planned maintenance work is needed on the network file storage system. Any downtime is kept to a minimum and 5 days' notice of planned downtime will be

given. If emergency maintenance is needed, this will be undertaken with minimum disruption where possible.

- A log is kept of the network file storage system configuration. In the event of a system failure this information will be used to restore service as promptly as possible.
- Digital and Data Services department may search the network file storage system at any time for illegal, unauthorised, or pirated software (including personal movies and personal music files). If such content is found, it will be removed, and the user's account suspended pending further investigation.

4.5 Security of information, equipment, and computer media

4.5.1 Clear Desk



Clear Desk guidance is applicable in any environment where Trust duties are undertaken. This includes home/remote working outside of the Trust-owned office environments.




All information, electronic or paper, and other valuable resources **must** be secured appropriately when staff are absent from their workplace and at the end of each working day if not working within a 24-hour environment.




- **Do not** leave patient notes, personal files, or any other confidential records unattended on or around the work area. This includes handwritten telephone numbers, names etc. Do not leave adhesive notes (post its) with telephone numbers attached to the work area.
- At the end of each working day (excludes 24hr environments), clear your desk of any confidential or person identifiable information. Medical records must be locked securely in desks, filing cabinets or rooms at all times, unless they are currently in use.
- For security, lock your personal items away (i.e., keys, handbags, wallets etc).

- Store paper and computer media in suitable locked cupboards when not in use.

4.5.2 Electronic or computerised information and equipment

 Computing and all other equipment containing data will be treated with the same level of security as paper-based resources as they contain the same type of confidential and/or personal information.

-  **Do not** leave computers and laptops logged on when unattended. Security options will depend on the type of equipment. Raise any concerns with the Information Security Officer or Information Service Desk.
- Lock your screen when leaving the computer terminal, irrespective of the amount of time spent away from the unattended screen.
- Close, minimise or lock the screen when unauthorised persons are near it.
- Remove sensitive items such as personal identifiers from printers immediately on completion. If these are no longer required, shred the items, or send them for secure disposal.

4.6 Reporting data management issues

Any members of staff identifying a potential data management issue must inform the relevant Manager / Team as follows:

Issue	Who to contact
Data Quality	System Owner of the relevant system and appropriate Service Manager. NB: Care must always be taken when changing the data held within live systems to correct Data Quality issues. Data stored in systems must always be factual to events, and the integrity and accuracy of the record is the utmost

	importance. This is permissible in some systems and not in others. Please refer to the relevant System Specific Policy, System Owner, System Administrator, or support team if you require further guidance e.g., Patient Systems Team.
Confidentiality, Privacy and Sharing Information	The Information Governance Team tewv.ig@nhs.net
Security, Risk and Safe Ways of Working with Information	Digital and Data Services department's Compliance Team tewv.informationsecurity@nhs.net

5 Definitions

Term	Definition
Back-Up Media	Magnetic tapes or other electronic storage processes that contain copies of all electronic files from the network file storage system.
Business Intelligence and Clinical Outcomes teams	The section of the Digital and Data Services department responsible for the collation and submission of the trust's statutory and corporate reporting obligations.
Clinical Information system/Electronic Patient Record	The Trust currently uses PARIS as the primary electronic patient/Clinical Information System for the purpose of this document. This policy will be applicable to any other Clinical Information System that may be brought into the Trust.
Clinical Spine Application (CSA)	Web-based application used by healthcare professionals to gain controlled access to trace demographic information for patients within the NHS Care Records Service
Data Sets	Data sets detailing the trust's finished consultant episodes and mental health spells, and activity are submitted on a regular basis, for processing nationally and for visibility to the appropriate commissioners.
Data Protection Act 2018 and UK GDPR	The provisions detailed within the Act provide the statutory guidance for the protection and use of patient and staff information.
Demographic Batch Service	This facility allows controlled access to the Patient Demographics Service. It enables the Trust to securely

	submit and receive large electronic files providing verified patient demographic information.
Home Drive	A networked data storage area created for personal use only.
Information Centre	The national body responsible for the NHS Data Model and Dictionary Service that details the standard terms and definitions for key data items within the NHS.
Information Standards Notices (ISNs)	Used to enforce and control changes to the data standards that are embedded within the NHS Data Dictionary, ensuring the accurate and consistent interpretation and implementation of data standards throughout all NHS organisations. The ISNs include notifications of changes to the Commissioning Data Sets and are used as a basis for system amendments.
Information Systems	The information systems used for the capture of data within the trust.
Information Uses (Primary / Secondary)	<p>Primary Uses – is when information is used for healthcare and medical purposes. This would directly contribute to the treatment, diagnosis, or the care of the individual. This also includes relevant supporting administrative processes and audit/assurance of the quality of healthcare service provided.</p> <p>Secondary Uses – is for non-healthcare and medical purposes. Generally, this could be for research purposes, audits, service management, commissioning, contract monitoring and reporting facilities. When PII is used for secondary use, this must be limited and de-identified so that the secondary uses process is confidential.</p>
Network File Storage System	A hardware and software configuration designed primarily for the storage, retrieval, sharing, and printing of computer data files.
New Safe Havens	<p>A Safe Haven is a location or system within an organisation where personal information can be held, received, and communicated securely.</p> <p>The New Safe Haven principles restrict access to PII and apply to such information held in trust electronic systems. It supports the creation of safe haven teams (whether physically co-located or virtual) for the secure communication of PII. Patient information systems and databases must be used within the new safe haven</p>

	process whereby access is limited, and password controlled for each authorised user.
Paper Record (Patient)	Where paper records are kept, they must mirror the information that is held as part of the patient electronic record. All relevant clinical documentation in the paper record must include the NHS number. This includes correspondence, risk documentation, clinical notes, assessment, care planning etc.
Personal/Patient Identifiable Information (PII)	Information that can identify one person whether a single data item e.g., person's name, or a collection of data items for example name, address, Date of Birth.
Pseudonymisation / De-Identification	A group of techniques for de-identifying person identifiable data items. Some techniques are reversible, allowing identity to be re-established. It is also possible to produce consistent pseudonyms using techniques which do not allow the pseudonym to be reversed.
Printing Service	Means by which data files (e.g., Microsoft Word® documents) stored on the file storage system can be printed to any printer located on the computer network.
Pseudonymisation / De-Identification – Means of	De-identification of patient records all or a combination of: <ul style="list-style-type: none"> • Not displaying or outputting person identifier data items • Quarantining identifiers to organisations that have no ability to 'look-up' a person's identity in controlled circumstances. • Using derivations to systematically replace real values, e.g. <ul style="list-style-type: none"> ○ electoral ward instead of postcode, age instead of Date of Birth ○ Banding of values, (e.g., age 5-10) instead of Date of Birth ○ Post code sector (first 4 chars e.g., DE3 7) instead of full post code ○ Pseudonymisation techniques ○ Aggregation
Quotas (Network storage)	Constraints which limit the number of files that can be stored in a networked home or shared drive.
Record	Information created, received, and maintained as evidence and information by an organisation or person, in

	pursuance of legal obligations, or in the transaction of business (BS ISO 15489-1).
Shared Drive (Network)	A data storage area created for groups of people to access common files.
System Administrator	Individual who has responsibility for the Administration of a named information system within the trust. NB the roles of System owner and System Administrator can be combined in one person
System Owner	Individual who has overall responsibility within a given area for information systems in use in that area.
User Account	A name and password which is required to logon to the trust's computer network and electronic file storage system.

6 Related documents

CORP-0026: [Records Management Policy](#)

CORP-0026-007: [Records Management and Safe Haven procedure](#)

CORP-0026-005-v2: [Moving records and other sensitive information](#)

CORP-0026-002-v1.1 [Minimum standards for clinical record keeping](#)

CORP-0006: [Information Governance Policy](#)

IT-0011: [Registration Authority Policy](#)

IT-004: [Network User Access Procedure](#)

IT-0031: [Access to Information Systems Policy](#)

IT-0010: [Information Security and Risk Policy](#)

IT-0014: [NHS Number Procedure](#)

CLIN-0066: [Clinical Coding Procedure](#)

[Multiple]: System Specific Policies of those trust systems containing patient information

7 How this policy will be implemented

- This policy will be published on the Trust's intranet and external website.
- Line managers will disseminate this policy to all Trust employees through a line management briefing.

7.1 Implementation action plan

Activity	Expected outcome	Timescale	Responsibility	Means of verification/ measurement
Not applicable				

7.2 Training needs analysis

Staff/Professional Group	Type of Training	Duration	Frequency of Training
All Staff registering patients on a Clinical Information System	Training for the Demographic Batch Service or the Clinical Spine Applications	This is incorporated within a module in the Paris training appropriate to role.	On starting this job role (refresher required if access lapses the period defined in Paris Procedure)
All staff accessing electronic patient record systems	Paris User Training appropriate to their job role – Incl Data quality, collection routines and data entry	Approx 40 min – 4 hours appropriate to role	On starting job role (refresher if access lapses the period defined in Paris Procedure)
New starters to the Trust	Data Security and Protection Training for New Starters	Approx. 40 mins	On starting work with the Trust

8 How the implementation of this policy will be monitored

Number	Auditable Standard/Key Performance Indicators	Frequency/Method/Person Responsible	Where results and any Associate Action Plan will be reported to, implemented and monitored; (this will usually be via the relevant Governance Group).
1	A rolling programme of audits are commissioned via an external provider. These monitor the appropriate use, storage, security and processing of data and information in Trust systems.	This is a rolling programme, responsibility of the CIO/DCIO	Digital and Data Management Meeting
2	As specified in the DPIA for each system, there must be an access log maintained in relation to PII which must enable auditing of the access to identifiable data by individual users. The logging and audit facilities are required to ensure that only appropriate access to identifiable data has been undertaken. This log may take the form of an electronic access which forms part of electronic systems, and which can be used to monitor the access and use of PII for trust systems. Where such a facility is not available a manual log must be created	Privacy monitoring for Paris is a daily task of the Privacy Officer and	Action plans are reported to the staff member's line manager and managed via People and Culture
3	Data Security and Protection Toolkit	Annual, Online Self-Assessment, Digital and Data Services	Digital Performance and Assurance Group

9 References

ISB 0149 NHS Number - NHS Digital (accessed on 09 November 2022)

[Information Standard: DCB3058: Compliance with National Data Opt-outs](#) (NHS Digital, 25 May 2018)

Anonymisation: managing data protection risk code of practice (ico.org.uk) (ICO, November 2012)

Data Protection Act 2018 (GDPR)

The NHS Confidentiality Code of Practice

The Common Law Duty of Confidentiality

The Caldicott Report 1997

NHSX Records Management Code of Practice 2021

NHS England » Data quality Improvement (accessed on 09 November 2022)

[HSCIC Code of Practice on Confidential Information 2014](#)

[General Medical Council - Good medical practice Domain 1 - Knowledge skills and performance](#) (accessed 06 March 2023)

<https://www.nmc.org.uk/standards/standards-for-nurses/standards-of-proficiency-for-registered-nurses/> (accessed 06 March 2023)

10 Document control (external)

To be recorded on the policy register by Policy Coordinator

Date of approval	17 May 2023
Next review date	17 May 2026
This document replaces	Data Management Policy IT-0030-v2.1
This document was approved by	Digital and Data Management Meeting (25 April 2023) Digital Performance and Assurance Group (03 May 2023)
This document was approved	03 May 2023
This document was ratified by	Management Group
This document was ratified	17 May 2023 (MG inquorate – ratified pending full quorum) 21 June 2023 (full retrospective ratification - MG quorate)
An equality analysis was completed on this policy on	03 March 2023
Document type	Public
FOI Clause (Private documents only)	n/a

Change record

Version	Date	Amendment details	Status
1.0	04 May 2016	Policy underwent full review and no change required. Review date extended 3 years.	Withdrawn
2.0	23 Jul 2018	Full revision in line with GDPR and current Digital and Data Services department structure	Withdrawn
2.1	20 Jul 2020	Section 4.3 para added re: recording pseudonymised data flows on information flow mapping. 4.3.1 added re National Data Opt-Out	Withdrawn
2.1	15 June 2020	Review date extended to 08/02/2022	Withdrawn
2.1	20 Apr 2022	Review date extended to 31/10/2022	Withdrawn
2.1	18 Oct 2022	Review date extended to 31/01/2023	Withdrawn
3.0	17 May 2023	Full review with changes: <ul style="list-style-type: none"> • Outdated references to systems, process and documents removed and updated. • Minor changes to wording to aid clarity. • Section 4.2.5 <i>Monitoring and Action on Data Quality</i> added to incorporate elements of retired Data Quality Strategy • Alignment to Digital and Data Journey to Change. 	Published
3.0	21 Jun 2023	Document control amended to reflect MG on 17 May 2023 was inquorate – ratified pending full quorum. Full retrospective ratification at MG 21 June 2023 (quorate).	Ratified

Appendix 1 - Equality Analysis Screening Form

Please note: The Equality Analysis Policy and Equality Analysis Guidance can be found on the policy pages of the intranet

Section 1	Scope
Name of service area/directorate/department	Digital and Data Services
Title	Title: Data Management Policy Ref: IT-0030-v3.0
Type	Policy
Geographical area covered	Trust-wide
Aims and objectives	The Data Management Policy describes the importance of good data management and defines responsibilities of staff within the trust in helping to maintain these high standards.
Start date of Equality Analysis Screening	06 March 2023
End date of Equality Analysis Screening	10 March 2023

Section 2	Impacts
Who does the Policy, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan benefit?	Properly managed data will benefit the whole of the Trust as an organisation and enhance the Trust's ability to manage its work and workforce effectively at all levels. It will ensure that the information we hold is managed efficiently which adds to the quality of patient care and patient safety.
Will the Policy, Service, Function, Strategy, Code of practice, Guidance, Project or	<ul style="list-style-type: none"> • Race (including Gypsy and Traveller) NO

Business plan impact negatively on any of the protected characteristic groups?	<ul style="list-style-type: none"> • Disability (includes physical, learning, mental health, sensory and medical disabilities) NO • Sex (Men, women, and gender neutral etc.) NO • Gender reassignment (Transgender and gender identity) NO • Sexual Orientation (Lesbian, Gay, Bisexual and Heterosexual etc.) NO • Age (includes, young people, older people – people of all ages) NO • Religion or Belief (includes faith groups, atheism, and philosophical beliefs) NO • Pregnancy and Maternity (includes pregnancy, women who are breastfeeding and women on maternity leave) NO • Marriage and Civil Partnership (includes opposite and same sex couples who are married or civil partners) NO • Armed Forces (includes serving armed forces personnel, reservists, veterans, and their families) NO
Describe any negative impacts	None.
Describe any positive impacts	The policy describes the benefits of properly managed data which will enhance the security and confidentiality of all the information we hold in the Trust. This will be to the benefit of all staff and patients associated with the Trust.

Section 3	Research and involvement
What sources of information have you considered? (e.g., legislation, codes of practice, best practice, nice guidelines, CQC reports or feedback etc.)	National Guidance (NHS England/UK Government) Data Security & Protection Toolkit Statutory Dataset Requirements and Data Standards UK General Data Protection Regulation (UK GDPR)

Have you engaged or consulted with service users, carers, staff and other stakeholders including people from the protected groups?	Yes
If you answered Yes above, describe the engagement and involvement that has taken place	Trust-wide consultation – undertaken at this version.
If you answered No above, describe future plans that you may have to engage and involve people from different groups	

Section 4	Training needs
As part of this equality analysis have any training needs/service needs been identified?	No
Describe any training needs for Trust staff	n/a
Describe any training needs for patients	n/a
Describe any training needs for contractors or other outside agencies	n/a

Check the information you have provided and ensure additional evidence can be provided if asked

Appendix 2 – Approval checklist

To be completed by lead and attached to any document which guides practice when submitted to the appropriate committee/group for consideration and approval.

	Title of document being reviewed:	Yes / No / Not applicable	Comments
1.	Title		
	Is the title clear and unambiguous?	Y	
	Is it clear whether the document is a guideline, policy, protocol or standard?	Y	
2.	Rationale		
	Are reasons for development of the document stated?	Y	
3.	Development Process		
	Are people involved in the development identified?	Y	
	Has relevant expertise has been sought/used?	Y	
	Is there evidence of consultation with stakeholders and users?	Y	Trust wide consultation and through data quality working group.
	Have any related documents or documents that are impacted by this change been identified and updated?	Y	Removal of data quality strategy
4.	Content		
	Is the objective of the document clear?	Y	
	Is the target population clear and unambiguous?	Y	
	Are the intended outcomes described?	Y	
	Are the statements clear and unambiguous?	Y	
5.	Evidence Base		
	Is the type of evidence to support the document identified explicitly?	Y	
	Are key references cited?	Y	
	Are supporting documents referenced?	Y	
6.	Training		
	Have training needs been considered?	Y	
	Are training needs included in the document?	Y	
7.	Implementation and monitoring		

	Title of document being reviewed:	Yes / No / Not applicable	Comments
	Does the document identify how it will be implemented and monitored?	Y	
8.	Equality analysis		
	Has an equality analysis been completed for the document?	Y	
	Have Equality and Diversity reviewed and approved the equality analysis?	Y	
9.	Approval		
	Does the document identify which committee/group will approve it?	Y	
10.	Publication		
	Has the policy been reviewed for harm?	Y	No harm
	Does the document identify whether it is private or public?	Y	Public
	If private, does the document identify which clause of the Freedom of Information Act 2000 applies?	n/a	