Trust Standard Operating Procedure

University Hospitals Plymouth NHS Trust

Management of Records on IT Network Shares SOP

Issue Date	Review Date	Version
May 2019	May 2024	V1.1

Purpose

To explain how to manage records saved on shared folders on the Trust's electronic IT network.

Who should read this document?

All staff who use computers

Key Messages

There are two main areas for storing your information on the Trust's computer network;

- Home (H:) Drive; only available to you to use for your personal work
- Groups (G:) Drive; known as network shares or shared folders

Most work should be saved on the (G:) Drive;

- Secure and with appropriate management, confidential
- Allows for appropriate collaboration and business continuity

This SOP provides staff with general principles to follow for:

- Folder structure
- Naming Conventions
- Access and Security
- Maintenance and Records Management

It also identifies key individual's roles and responsibilities in maintaining/management of a network share.

Further information can be found on the IT intranet pages;
http://nww.plymouthict.nhs.uk/HelpGuidance/SavingAccessingFiles.aspx

Core accountabilities	
Owner	Head of Information Governance/Data Protection Officer
Review	Caldicott and Information Governance Assurance Committee
Ratification	Director of Corporate Business/Senior Information Risk Owner
Dissemination (Raising Awareness)	Head of Information Governance/Data Protection Officer
Compliance	Head of Information Governance/Data Protection Officer

Links to other policies and procedures

Information Governance Policy
Data Protection SOP (in production)
Subject Access Request (SAR) Policy
Management of Freedom of Information Requests SOP

Version History		
1.0	March 2019	Initial Document (Merging of four APNs into one SOP)
1.0	May 2019	Reviewed following consultation period

The Trust is committed to creating a fully inclusive and accessible service. Making equality and diversity an integral part of the business will enable us to enhance the services we deliver and better meet the needs of patients and staff. We will treat people with dignity and respect, promote equality and diversity and eliminate all forms of discrimination, regardless of (but not limited to) age, disability, gender reassignment, race, religion or belief, sex, sexual orientation, marriage/civil partnership and pregnancy/maternity.

An electronic version of this document is available in Document Library – UHPT Trust Documents. Larger text, Braille and Audio versions can be made available upon request.

Standard Operating Procedures are designed to promote consistency in delivery, to the required quality standards, across the Trust. They should be regarded as a key element of the training provision for staff to help them to deliver their roles and responsibilities.

Standard Operating Procedure (SOP)

Management of Records on IT Network Shares SOP

1 Introduction

This procedure has been developed to ensure that electronic records held on network share folders are stored and managed appropriately.

2 Definitions

Types of Drives

There are two types of drives:

- **Home (H:)** drive; only accessible to the individual who is logged onto the computer. It is held on the network but is not accessible to other users.
- **Groups (G:)** drive; gives access to network share folders. The vast majority of electronic records should be stored on the network share folders. This is because NHS work records are 'public records' and colleagues need to be able to access the work of others to fulfil their own duties and to cover for absence.

  Folders can be accessible to everyone or restricted to individuals or teams.

Network Share Folder

A network share folder is classed as an information asset. Each folder is owned by an Information Asset Owner who has assigned an Information Asset Administrator to take responsibility for managing and organising the folder.

3 Regulation and Legislation

Records Management Code of Practice for Health and Social Care 2016

This sets out what people working with or in NHS organisations in England need to do to manage records correctly. It is based on current legal requirements and professional best practice and was published by the Information Governance Alliance (IGA).

Appendix 3 of the Code contains the detailed retention schedules. It sets out how long records should be retained, either due to their ongoing administrative value or as a result of statutory requirement.

Data Protection Legislation
The following sets out the way organisations should process personal data of living individuals:

- EU General Data Protection Regulation (GDPR)
- UK Data Protection Act 2018

It also gives people the right to see information held about them.

Common Law Duty of Confidentiality
Information is only disclosed to individuals who are authorised to receive it by individuals who are authorised to release it. Disclosure is determined on a need to know basis.

Caldicott Report
The seven Caldicott Principles when using patient information are:

- Justify the purpose
- Only use if absolutely necessary
- Use the minimum required
- Access on a need to know basis
- Everyone must understand their responsibilities
- Understand and comply with the law
- The duty to share information can be as important as the duty to protect confidentiality.

Freedom of Information Act 2000
The Freedom of Information Act 2000 provides public access to corporate information held by public authorities.

4 Key Duties

An Information Asset Owner is a named Director or Senior Manager who has ultimate accountability for the records contained within the network share folder(s) that they own. They are responsible for ensuring that each share has an **Information Asset Administrator** who is responsible for:

- Granting and removing permissions to network share folders ensuring access is on a need to know basis.
- Amending permissions when staff leave or transfer department.
- Maintaining a logical and controlled folder structure.
- Ensuring names of folders and documents comply with naming convention.
- Encouraging regular deletion of unnecessary/old or duplicate records.
- Liaising with the IM&T Service Desk and user line managers where appropriate.
- Working with staff to ensure that folders are clear, well-structured and free from duplication.

- Working with staff to ensure that all users are made aware of their responsibilities and naming conventions.

IAO's and IAA's are listed on;

http://nww.plymouthict.nhs.uk/HelpGuidance/NetworkShares.aspx

The department's **Local Records Lead** should identify all the network share folders used in their area and keep a record of these on their local records inventory.

All Staff should:

- Understand how network share folders should be structured.
- Raise any concerns about information held within a network share folder with the Information Asset Administrator.

Information Governance Team
Oversees the records management process and reports exceptions to the Caldicott and Information Governance Assurance Committee chaired by the Senior Information Risk Owner (SIRO).

5 Procedure to Follow

Network Share Folder Structure
Organise folders according to functions/activities, not individual staff
- Functions tend to remain the same, even if teams change.
- Similar files owned by different employees causing of duplication should be avoided.

Organise folders according to functions / activities, not file format.
- E.g. Store spreadsheets in an activity folder, not in a folder called 'Spreadsheets'.

Keep it simple and think before creating new folders
- Creating a complex folder structure can make it more difficult to find information.
- Use subfolders only if needed to further categorise the records.

Routine information should be organised by year (either calendar or financial)
- Continue to month/week level if large volumes
- Ensures records can be easily found.
- Aids the identification of older records which should be archived/deleted.

All documents should be saved within a named folder
- Documents should not be saved in the top level folders as they can become lost – this is like putting loose papers into a filing cabinet without first putting into a file.

Naming Conventions for Folders and Documents
Folder/file names should be meaningful so they may be easily found:

- Name documents consistently and logically.
- Keep name to a manageable length
- Do not use;
    - ‘general’ or ‘miscellaneous’.
    - words such as ‘folder’, ‘letter’, ‘word document’ etc.
    - personal names unless absolutely necessary.
- If you are using numbers in titles, use at least two numbers so that documents stay in sequence (i.e. 01 – 99) unless you are including the year.
- Record dates ‘back to front’ to maintain a logical sequence i.e. 2019.01.27. Dates also help with version control
- Avoid using abbreviations unless well known.
- For drafts or minor updates to documents use the second decimal point. For final versions or major updates use the first decimal point:
    - Management of Records on IT Network Shares SOP v0.1 (Draft)
    - Management of Records on IT Network Shares SOP v1.0 (Final Version)
    - Management of Records on IT Network Shares SOP v1.1 (Minor Update)

Records Transfer
To prevent unnecessary duplicates, hyperlinks should be circulated by email whenever possible.

Access and Security
It is important to ensure that user permissions and folder contents are appropriately matched. It is only appropriate to share work records if colleagues have a legitimate need of access for their work.

Review the contents of the network share folders and check for potentially sensitive information (this can mean sensitive patient, personal or business information).

- Determine whether sensitive contents need access restriction.
- IAO’s should advise on alternative options for restricting access, such as saving sensitive documents in alternative locations – eg, other more restricted network share folders. The IAA/IAO should contact the IM&T Service Desk if they consider the creation of a new network share folder to be necessary.
- Ensure that staff are trained on the use of folders. This should be part of local induction for new staff.

Access Control
If access is required to a network share folder, then the relevant IAO must be contacted who will approve the application and forward to the IAA who will arrange access.

If a staff member needs routine access to information held on a network share then it is more appropriate to allow them access to the share rather than continually share information by email.

Maintenance and Records Management
Even when network share folders are well maintained, as time goes by, the amount of data stored will grow which makes it more difficult to find information.

Trust records must be retained for a minimum period of time for legal, operational, research and safety reasons. When the minimum period has expired, records should be considered for deletion. The Records Management Code of Practice for Health and Social Care 2016 details minimum retention schedules for electronic and paper records.

Network Share Folders should be continuously maintained and annually 'spring-cleaned'

- IAA's should inform all staff of any impending "spring clean".
- Delete records that are no longer relevant and that have exceeded their retention period.

To find out the size and number of items in a folder using My Computer/Windows Explorer:

- Right click on the folder and choose properties. This will bring up a box showing the size in kilobytes, the total number of items in the folder and sub-folders, and the number of folders within. This can help to identify which folders are largest and prioritise accordingly.
- Change the view to Details view (right click and select **View – Details**)
- Sort by Size (by right clicking and selecting **Sort by** - **Size**)

If searching an individual folder, the above process can be followed but click on **Date Modified** when in Detail view.

- Common large items include:
    - Bitmap images (.bmp). These should be saved as (.jpeg) files ('Paint' is on all PCs – Start – Programs – Accessories). The (.bmp) files should be deleted.
    - PowerPoint Presentations and Access databases
    - Audio/video files – (.wav) (.mp3) etc

To identify old/out-of-date items select the folder, right-click and choose search. In the search box, choose to search for items by date and search for files modified between certain dates (e.g. between 2000 and 2004). The search results can be ordered by date, by clicking on the date modified tab, to immediately identify the oldest items in the folder. Items which have not been modified for a long time may be likely candidates for deletion.

Benefits for Staff

- Filing systems will be well organised and reduce the time spent searching for information
- Records stored within the network share folders are accurate, relevant and up-to-date
- Common naming conventions are used
- Information shared as appropriate

- Improved ability to cover for absent colleagues
- Reduction in unnecessary duplicates consuming storage space
- Less email attachments sent/received thereby improving mailbox capacity

Removable media
Use of removable media should be avoided unless essential to a role. Where this is the case, devices should be encrypted in line with the Information Security Policy.

Records stored on encrypted removable devices are protected from unauthorised access if the device becomes lost. Nevertheless, it is important that records stored on removable devices be backed up on the appropriate network share folder to prevent permanent loss of work.

Email folders
Email folders should not be used to store records on an ongoing basis or be used as a personal filing structure/system. Emails should be deleted when actioned or, if the email/attachments have continuing work value, they should be saved into the appropriate network share folder then deleted from Microsoft Outlook folders.

6 Document Ratification Process

The design and process of review and revision of this procedural document will comply with The Development and Management of Formal Documents.

The review period for this document is set as default of five years from the date it was last ratified, or earlier if developments within or external to the Trust indicate the need for a significant revision to the procedures described.

This document will be reviewed by the Caldicott and Information Governance Assurance Committee and ratified by the Director of Corporate Business.
Non-significant amendments to this document may be made, under delegated authority from the Director of Corporate Business, by the nominated author. These must be ratified by the Director of Corporate Business and should be reported, retrospectively, to the Caldicott and Information Governance Assurance Committee.

Significant reviews and revisions to this document will include a consultation with named groups, or grades across the Trust. For non-significant amendments, informal consultation will be restricted to named groups, or grades who are directly affected by the proposed changes.

7 Dissemination and Implementation

Following approval and ratification, this procedural document will be published in the Trust's formal documents library and all staff will be notified through the Trust's normal notification process, currently the 'Vital Signs' electronic newsletter.

Document control arrangements will be in accordance with The Development and Management of Formal Documents.

The document author(s) will be responsible for agreeing the training requirements associated with the newly ratified document with the Director of Corporate Business and for working with the Trust's training function, if required, to arrange for the required training to be delivered.

8 Monitoring and Assurance

This procedure is underpinned by the Information Governance Policy.

All breaches of confidentiality must be reported on the Trust Incident Reporting System, Datix. Staff should also notify their Line Manager and the Information Governance Team.

Incidents will be managed in line with the Guide to the Notification of Data Security and Protection Incidents produced by NHS Digital and the Trust's Information Governance Incident Handling SOP.

Staff that breach confidentiality may be subject to disciplinary action in line with the Trust Performance and Conduct Policy.

9 Reference Material

- http://nww.plymouthict.nhs.uk/HelpGuidance/SavingAccessingFiles.aspx
- Data Protection Act 2018
- EU General Data Protection Regulation (GDPR)
- Records Management Code of Practice for Health and Social Care 2016
- Information Commissioners Office (ICO) Website

This SOP forms part of the Information Governance suite of formal documents which can be found on in the Document Library – UHPT Trust Documents.