Overview

This standard operating procedure (SOP) chapter contains information about records stored in central files and field offices. The content is relevant to Residential Care Services (RCS) staff, as well as anyone seeking to understand how RCS files are stored, retained, and destroyed.

Records Management is the responsibility of every person in RCS. Ensuring that we have complete and accurate records:

- Enables DSHS to fulfill its mission by giving timely access to information necessary to help our clients.
- Ensures open and accountable government.
- Promotes cost-effective use of agency resources by maintaining continuity in the event of staff turn-over, avoiding storage costs and purchasing.
- Minimizes risks and associated costs by being able to readily locate records in response to litigation, discovery, public records requests, and audits.

RCS record management procedures include paper files, shared files, scan procedures, perceptive content (the RCS Record Management Tool [RMT]), record verification and destruction procedures and electronic packet procedures.

Authority

- Chapter 40.14 RCW – Preservation and Destruction of Public Records
- Chapter 42.56 RCW – Public Records Act
- Chapter 434-662 WAC – Preservation of Electronic Records
- Chapter 434-663 WAC – Imaging Systems, Standards for Accuracy and Durability
- DSHS Administrative Policy 5.04 – Records Retention
- DSHS Administrative Policy 5.05 – Management of the Litigation Discovery Process
- DSHS Administrative Policy 5.06 – Use and Destruction of Health Care Information
- DSHS Administrative Policy 5.07 – Employee Response to Litigation Related Documents
- DSHS Administrative Policy 5.08 – DSHS Minimum Physical Security Standards for Confidential Information and Financial Instruments
- DSHS Administrative Policy 15.15 – Use of Electronic Messaging Systems and the Internet
- Washington State Records Retention Schedules

These procedures are not covered by DSHS Administrative Policies as they are specific to Residential Care Services. These procedures will be reviewed for accuracy and compliance at least every five years.

Contacts

- RCS Central Files General Contact: RCSCentralFiles@dshs.wa.gov
- RCS Policy Unit General Contact: RCSPolicy@dshs.wa.gov
- RCS Quality Improvement Unit General Contact: ImproveRCS@dshs.wa.gov

Table of Contents

Part I: Records Management

A. Shared Files

Background

Electronic file sharing simplifies administration, centralizes files for consistency, and keeps files organized and maintained. It is the electronic version of paper file sharing. Until the time that Perceptive Content is fully functional for all RCS documents, staff must use shared files to store and retrieve electronic documents relating to inspections, investigations, and certification work in LTC settings or other RCS work.

File sharing allows staff to retrieve the same file for view or modification. Information Technology (IT) staff are the RCS file sharing system administrators. RCS staff have a varying amount of access to these shared files and the permissions set by IT are based on the type of file being accessed.

The best practices for shared files include:

- Having a well-planned folder structure;
- Naming files and folders based on search intent; and
- Documenting and following a process to backup shared files.

File sharing standards protect and preserve electronic data and these procedures give direction and awareness to staff using shared files.

1. Shared File Saving

Saving documents in shared files requires that RCS staff:

a. Follow standard RCS document naming and saving conventions and folder structure for all shared files.
b. Save electronic documents pertaining to RCS inspection, investigation, and certification or other RCS work in shared files or designated applications, not on personal drives, One Drive, or desktop.
c. Staff have the option to save working papers and documents to their desktop or personal files while conducting inspection, investigation, certification, or other RCS work. Staff will remove the documents from the desktop, One Drive, or personal files once the inspection, investigation or certification or other RCS work is closed or completed.
d. Save all Word documents in PDF (portable document file) format.

2. Shared File Management

Regulatory Operations - Designated RCS staff must:

a. Conduct a monthly audit of two visits per staff person for the previous month.
   1) If a staff did not conduct two visits, the designated staff will note in the spreadsheet “Nothing to audit.”
   2) If staff did conduct two visits in the previous month, select two visits to review. If there are no documents in the Shared Drive for the two visits selected, check with the staff to ensure they did not have any visits in that month.
   3) Remind staff to store documents in the shared folder if they have saved them elsewhere.

b. Use the “eDoc Audit Spreadsheet” to track each unit’s folder usage by recording the following information:
   1) Audit date;
   2) Brief description of any errors found; and
   3) The outcome of the audit in the notes section.

> Example: “completed according to procedure” or “event ID and document description interchanged.”

c. Send e-mails to staff with the outcome of the audit using standard messaging that includes:
   1) Subject Line: eDoc Naming and Saving Review
   2) No Error Message: On conducting an internal review of the electronic documents saved to the Shared Drive, no errors were found among the files you saved. The files use the correct document naming and saving standard and are saved in the correct folder. Thank you.
   3) Error Message: On conducting an internal review of the electronic documents saved to the Shared Drive, the files you have saved include errors. Then, list the examples, using the following example:

> Example:
> 1) For facility XYZ intake #1234567, documents were in the correct folder, but they were not named according to the standard.
> 2) For facility XYZ intake #7654321, the documents were in the “Full” folder rather than the “Complaints” folder.
> 3) Please make the corrections by date and let me and your immediate supervisor know when corrections have been made. Thank you!

   4) RCS staff must respond to an error message. If staff do not respond to an error message within a week, request for the immediate supervisor to follow up.
   5) Refer staff to their supervisors for additional information about the naming and saving standard or the purpose of the audit.

Non-Regulatory Operations - Designated RCS staff must:

a. Conduct a monthly audit of shared file folders

b. Use an "eDoc Audit Spreadsheet" to track folder usage

c. Send emails to staff with the outcome of the audit using standard messaging that includes:

   1) Subject Line: eDoc Naming and Saving Review

   2) No Error Message: On conducting an internal review of the electronic documents saved to the Shared Drive, no errors were found among the files you saved. The files use the correct document naming and saving standard and are saved in the correct folder. Thank you.

   3) Error Message: On conducting an internal review of the electronic documents saved to the Shared Drive, the files you have saved include errors. Then, list the examples.

d. RCS staff must respond to an error message. If staff do not respond to an error message within a week, request for the immediate supervisor to follow up.

e. Refer staff to their supervisors for additional information about the naming and saving standard or the purpose of the audit.

Field Managers, Program Managers, and Supervisors must:

a. Ensure staff receive training in shared file naming, saving, and auditing.

b. Designate staff to conduct monthly Shared File Audits.

c. Provide training and mentoring to staff who are having difficulty following shared file system naming and saving conventions, and to staff who do not respond to an audit error message.

B. Scanners and Scan Procedures

Background

Many Long-term care (LTC) settings document on paper. RCS staff collect copies of facility documents to support inspection findings. Scanners are a device that captures an electronic image of a paper document. RCS field staff carry portable scanners as a tool for electronic document collection if the LTC setting does not have the means to provide documents in an electronic format. Scanner use contributes to the RCS goal of paperless work.

Scanner Procedure

RCS Staff will:

1. Learn how the scanner works including how to use the scanner and document storage prior to using the scanner.
2. Establish scanner support.
   a. Verify that CaptureOnTouch software is installed on the state-issued laptop.
   b. Create a scanner support folder on the laptop desktop with the scanner user’s manual, instructions, trouble shooting and document naming and saving key.
   c. Identify and carry the local office information technology (IT) support staff telephone number.
3. Prepare for scanner use in the field.
   a. Turn on laptop and allow all software updates to install.
   b. If planning to work without an internet connection, create a folder on the laptop desktop to store scanned documents.
      1) Name the folder with LTC setting name and license number.
      2) There should be a separate folder for each LTC setting.
   c. If using the Canon p-215ii Scanner - Check to ensure the Auto Start switch on the rear of the scanner is in OFF mode
   d. Label or attach a business card to the scanner and USB scanner cable.
4. Gather the following equipment:
   a. Laptop and Power Supply.
   b. Scanner and USB connector cable.
   c. Scanner carry bag.
   d. Optional: USB data hub.
5. When using the scanner in the field:
   a. Place the scanner on a level, stable surface with enough room for scanned documents to exit the scanner freely onto the flat surface. Inadequate room will result in scanned documents jamming the scanner, becoming crumpled or landing on the floor.
   b. Review scanned document image before finishing a scan to be sure that information is captured correctly. Rescan as needed.
   c. Return paper documents to the original location, in the original condition after scanning.

   d. Collect scanner, scanner cable, laptop, laptop cord and carry bags prior to leaving the LTC setting.
6. Scanned document saving:
   a. Save all scanned documents in a designated desktop folder or shared file or upload into electronic working papers.
   b. Label each scanned document following the RCS document naming convention when saving in a shared file during an inspection.
   c. If scanned documents are saved in a designated desktop folder during inspection:
      1) Label each scanned document following the RCS document naming convention.
      2) Transfer scanned documents to a shared folder or upload to electronic working papers once connected to an internet source.
      3) Delete desktop folder with scanned documents after confirming that scanned documents are stored in their final electronic destination.
         a) Scanned documents must be centered, without blurring or defect, in order to be an adequate record for RCS work.
7. For difficulties when using a portable scanner in the field:
   a. Refer to the scanner user’s manual and troubleshooting documents in the laptop desktop folder.
   b. Call the local IT support person.
   c. RCS staff may ask to use LTC setting scanners or ask that documents are emailed.
   d. RCS staff may not: take a cell phone photo of a document that has protected health information or any resident/client identifying information in lieu of scanning.

C. Record Scanning, Verification, and Destruction

Procedures

Perceptive Content has been authorized by the Washington Secretary of State as a records management tool that allows RCS to destroy non-archival records once that record has been imported into Perceptive Content and **verified to be complete and accurate**. The process for destroying records after their successful import into Perceptive Content is commonly referred to as *Scan and Toss*. It is a policy that is compliant with WA state records management standards with Washington State Archives.

1. Scanning

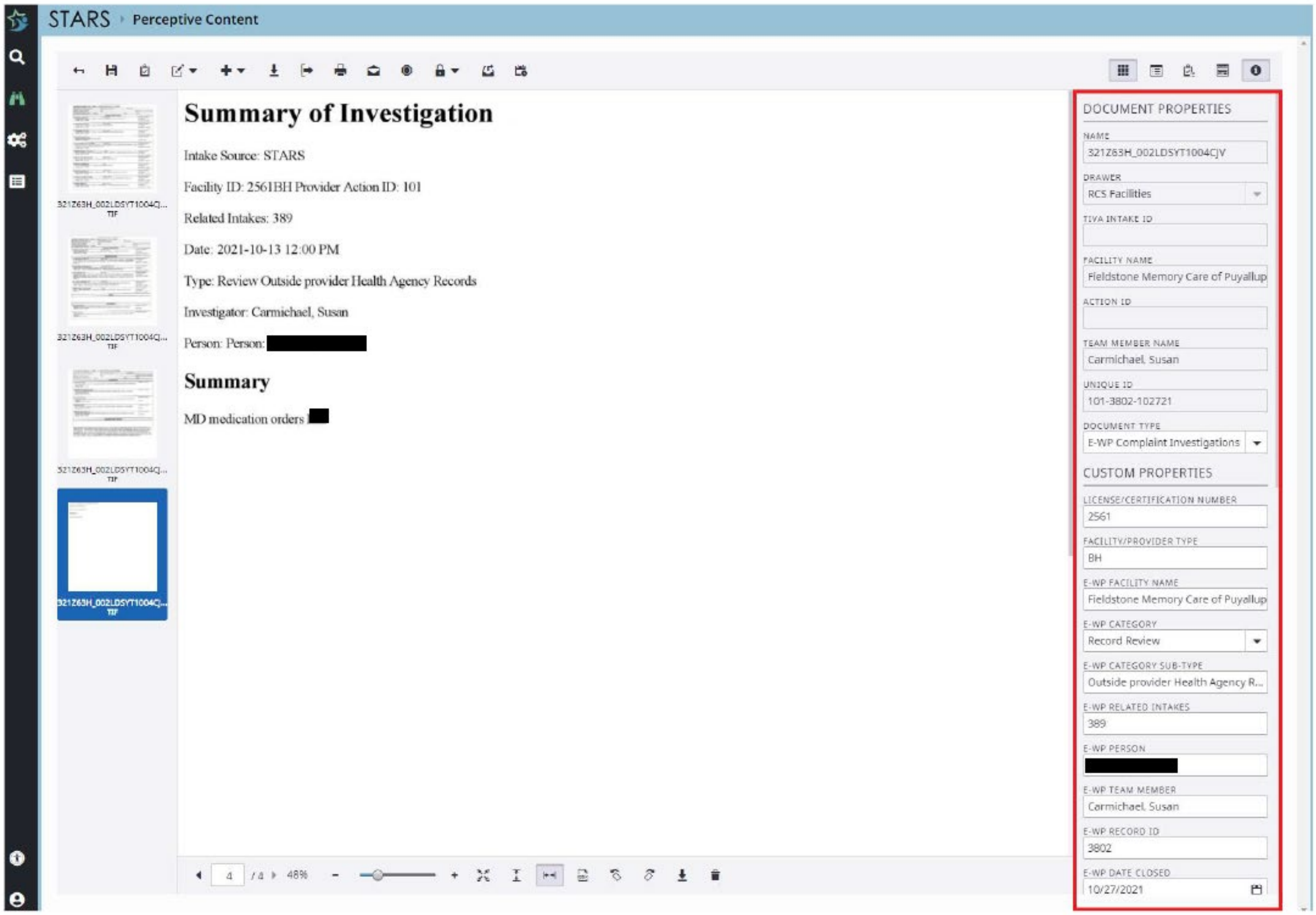
a. When scanning documents that will be preserved in Perceptive Content, records **must** be scanned and verified in a systematic and consistent fashion that ensures a complete and accurate copy of the source record. The document should have all associated pages in the correct order. The pages should not be contorted views of a document or blurry images.
b. Additional resources for scanning documents are available at Electronic Doc and Scanner Tools. This would include scanner user manual, scanner instructions, troubleshooting problems, and scanner training.

2. Verification

Prior to destruction of the record, the record must be **confirmed as complete and accurate** in Perceptive Content by an RCS staff person that has access to the original record. Perceptive Content is accessible to all RCS staff through STARS. Please see the STARS manual for additional instructions on how to search Perceptive Content in STARS.

> Note: Records are transferred from the Electronic Working Papers (EWP) application to Perceptive Content once the user clicks “save and close” within the EWP application and the user receives confirmation that the records were successfully transferred. Additional details on the EWP application may be found here.

Within 30 working days of import into Perceptive Content, staff with access to the original record must review the document to verify the records imported into Perceptive Content are complete and accurate by:
a. Locating the document within Perceptive Content;
b. Verifying the completeness of the record; and
c. Confirming the accuracy of the document properties and custom properties with the scan quality as noted in the red box below.


STARS
Perceptive Content
321Z63H_002LDSYT1004CJ... TIF
321Z63H_002LDSYT1004CJ... TIF
321Z63H_002LDSYT1004CJ... TIF
321Z63H_002LDSYT1004CJ... TIF
4 / 4 48%

Summary of Investigation

Intake Source: STARS

Facility ID: 2561BH Provider Action ID: 101

Related Intakes: 389

Date: 2021-10-13 12:00 PM

Type: Review Outside provider Health Agency Records

Investigator: Carmichael, Susan

Person: Person: [redacted]

Summary

MD medication orders [redacted]

DOCUMENT PROPERTIES

NAME: 321Z63H_002LDSYT1004CJV

DRAWER: RCS Facilities

TIVA INTAKE ID:

FACILITY NAME: Fieldstone Memory Care of Puyallup

ACTION ID:

TEAM MEMBER NAME: Carmichael, Susan

UNIQUE ID: 101-3802-102721

DOCUMENT TYPE: E-WP Complaint Investigations

CUSTOM PROPERTIES

LICENSE/CERTIFICATION NUMBER: 2561

FACILITY/PROVIDER TYPE: BH

E-WP FACILITY NAME: Fieldstone Memory Care of Puyallup

E-WP CATEGORY: Record Review

E-WP CATEGORY SUB-TYPE: Outside provider Health Agency R...

E-WP RELATED INTAKES: 389

E-WP PERSON: [redacted]

E-WP TEAM MEMBER: Carmichael, Susan

E-WP RECORD ID: 3802

E-WP DATE CLOSED: 10/27/2021

3. Destruction

After the staff verifies the records imported into Perceptive Content are complete and accurate according to the process of verification above, staff must destroy the original documents by:

a. Disposing of hardcopy records using DSHS-approved confidential shred bins; and
b. Deleting electronic records from computers and shared drives.

If after transferring documents into Perceptive Content corrections need to be made to the record for it to be considered complete and accurate, please contact the following:

a. For EWP records: RCSewp@dshs.wa.gov
b. For all other records: RCSCentralFiles@dshs.wa.gov

D. Records to Central Files

Background

The Central Files team has the responsibility of providing access, management, retention, storage, protection, and disposition of RCS facility records throughout their life cycle and to ensure timely and accurate information is available. Each field office must ensure records relating to Statements of Deficiency (SOD), Attestations, Plans of Correction (POC), Confidential Identifier Lists, and Back in Compliance (BIC) letters are sent to Central Files in a timely and organized manner. Programs utilizing Federal data bases to manage SOD and POC work send designated survey documents and Confidential Identifier Lists to Central Files.

All working papers are the responsibility of the units creating them. Working papers may be entered into the Electronic Working Paper (EWP) or program specific applications such LTCSP (Long-Term Care Survey Process). Any electronic working papers that are not entered into applications must be stored securely on shared files according to RCS standard document naming and saving procedures. Paper working papers must be stored in an organized manner at local offices. All paper and electronic files follow DSHS record retention schedules. Electronic and paper working papers should not be forwarded to Central Files for maintenance/storage.

Field Manager Responsibility

Review the process with staff.

- Train staff and ensure they can demonstrate they understand this procedure.
- Conduct periodic reviews of this procedure to ensure staff are following the SOP correctly.
- Request training or clarification from leadership as needed.

1. Electronic Packets

Each Long-term care (LTC) setting program will use a designated shared files location to collect documents into a “packet” to be sent to Central Files following steps outlined below. Once the Packet is complete, the packet is transferred or copied to the RCS Records for Central Files Q Drive Folder. Central Files staff then upload the packet documents into Perceptive Content (PC).

This procedure applies to all LTC settings: Adult Family Home (AFH), Assisted Living Facility (ALF), Certified Community Residential Supports and Services (CCRSS), Enhanced Services Facilities (ESF), Intermediate Care Facilities for Individuals with Intellectual Disabilities (ICF/IID), Nursing Home (NH).

Packet Content Examples:

a. Deficiency Free Inspection Letter
b. Consultation Letter

c. SOD and/or Related Documents
   1) SOD Letter Signed by the Field Manager
   2) Accepted POC and Attestation signed by provider
   3) Confidential Identifier List
   4) BIC letter

d. Survey Related Documents
   1) NH - 671, 1539, ID List
   2) ICF/IID - 3070G, 3070H, 1539, ID List, 2567B

Procedure

a. CREATE an electronic folder as a collection space for documents related to the regulatory visit. Follow the packet process document naming convention.

b. SAVE regulatory visit documents in the electronic file folder associated with the regulatory visit. All packet documents will be saved:
   1) In pdf format.
   2) Using the standard document naming convention.

c. RECEIVE and SAVE provider signed POCs and attestation in the electronic file folder. The Nursing Home Program Receives plans of correction through ASPEN ePOC and follows the ePOC process.

> Note: For provider documents related to the SOD, attestation or POC sent to RCS in paper format:
>
> a. Scan paper documents, save as PDF using document naming convention.
> b. Hold paper documents in a file folder in the local office until confirmation that the electronic version of the document is viewable in PC.
> c. Follow 'Record Scanning, Verification and Destruction' procedures once paper document is confirmed as viewable in PC.

d. NOTIFY RCS staff that the attestation and/or POC has been received and is available to review.
   1) Save final approved attestation/POC in the electronic packet file folder.
      a) There is no need to save multiple versions of a partial or non-approved attestation or POC in the folder.
      b) Nursing Home follows the ePOC process.
   2) Document correspondence and communication with the provider related to SOD delivery, reminders, and provider comments in the correspondence tab in STARS (preferred method) or the electronic SOD/POC tracking tool.

e. VERIFY all documents related to the regulatory visit are in the electronic file folder. Check to be sure:
   1) Department letters are signed.
   2) All packet documents are present and named correctly.
   3) All documents are in pdf format.

f. TRANSFER Packet files within 48 hours of packet completion to:
   i. Q: Drive: RCS Records for Central Files Folder
   ii. Shared Files: Once transferred (copied) to RCS Records for Central Files Q: Drive Folder – Move the packet folder to the "Transferred to RCS Records for Central Files" Folder.

> Note: There is no need to hold packet transfer for Informal Dispute Resolution outcome.

2. Follow-Up Visits

a. If the Follow-Up visit is not done within 90 days, transfer the packet with documents to RCS Records for Central Files Q: Drive folder.
   i. The CCRSS program creates a separate folder for each follow up and transfers the packet as soon as it is complete.
b. Follow-up visits after 90 days:
   i. If citations – create a new folder for SOD/POC documents.
   ii. If no citations - deposit the Back in Compliance (BIC) letter into the RCS Records for Central Files Q: Drive Folder.

Part II: Network Drives (Q: Drive)

Overview

Network drives are owned and maintained by DSHS Technology Innovation Administration. Files located on the network drives can be securely shared with staff within Residential Care Services (RCS), other divisions within Aging and Long-Term Support Administration (ALTSA) (e.g., Home and Community Services, Adult Protection Services) and other DSHS administrations (e.g., Developmental Disabilities Administration [DDA]).

There are multiple network drives to accommodate the business needs of RCS (e.g., Q: drive, R: drive). To access the network drives, users must connect to the network while in the office or VPN (Virtual Private Network) when out of the office and have permission to access the folder(s).

A. General Guidelines

Purpose

These guidelines establish the policies and procedures for folders in use by RCS found on the Q: drive. The purpose for establishing a governance promotes efficient and effective use, increases compliance with security through appropriate ownership and access, and mitigates risk for public disclosure requests or litigation holds.

Additional training resources on records management can be found in the Resources section.

Procedure

1. Q: drive users will:
   a. Consult with Central Files for questions about destruction of files or records retention requirements.
   b. Consult with Information Technology (IT) for technical issues or questions.
2. Folder Owners will:
   a. Train new staff who access the Q: drive to ensure they can demonstrate they understand this procedure.
   b. Conduct periodic reviews of this procedure to ensure staff are following it correctly.
   c. Request training or clarification from leadership as needed.

Section Overview Glossary of Terms Acronym List Table of Contents

B. Organization

Purpose

A hierarchical file system is used in the Q: drive that organizes contents into a tree structure. Having a standardized hierarchical structure of Q: drive folders allows for organizing folders in a consistent and logical manner, increases work productivity and efficiency in information search and retrieval, frees up space on the computer network system, and reduces duplication of files.

Procedure

1. Folder Hierarchy Structure

The Q: drive is the root directory that holds folders (also known as subdirectories). Each folder may contain one or more subfolders. For the purposes of this chapter, folders and subfolders are defined on a tiered system.

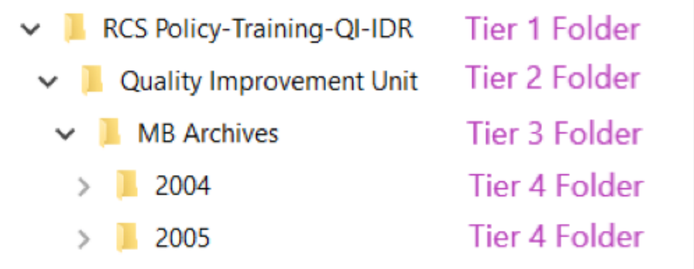
Q: drive – Root directory

→ Tier 1 Folder – First folder after the root directory. This is the top level of the file system hierarchy and is organized by office or content. Viewable by all ALTSA & DDA Q: drive users.

→ Tier 2 Folder – Subfolder located within a Tier 1 folder. Folder names should contain information on general content to help direct users. Viewable by all ALTSA & DDA Q: drive users.

→ Tier 3 Folder – Subfolder located within a Tier 2 folder. May contain subfolders or files, depending on user needs. Viewable by only those who have approved access.

Example:



2. Folder Naming Convention

Naming conventions allows information held within the electronic records database to be organized using a coherent context and logical framework. A naming convention will increase the usability of documents stored within folders by enabling easy retrieval and identification.

1. RCS Staff will:
    a. Follow folder naming convention properties for all folders found within the drive (see Resources for *file* naming conventions for working papers):
        1) All Tier 1 folders begin with "RCS" followed by a description of content.
        2) Avoid special characters (#%&{}\<>).
        3) Avoid underscore in place of a space (spaces are allowed).
        4) Use relevant, descriptive words to describe folder content.
        5) Commonly used RCS acronyms are acceptable.
        6) Do not write folder or file names in all caps.
        7) Keep folder names under 25 characters (best practice).
        8) If records are retrieved according to their date, that element should appear first.

> Examples: Recurring scheduled unit meeting or regularly pulled reports (e.g., 2024 Budget Meetings, 01-2024 RUG Reports)

        9) If records are retrieved according to their description, that element should appear first.

> Examples: Standard Operating Procedures; POD Training and Materials

> Note: Folder naming conventions document can also be found in the Q: Drive READ ME folder (Q:\RCS – README).

3. Folder Ownership

All Tier 2 folders must have an identified folder owner and co-owner. Folder owner(s) are considered the main point of contact for the folder, its contents, and serve as the gatekeeper to control access to contents. Co-owner(s) serve as a back-up contact if the owner is not available. Co-owner(s) have the same access permission level as an owner to modify contents or approve access for users.

Folder ownership is identified by position and may be passed to a new owner when staff change positions. A list of folder owners can be found in the RCS README folder (Q:\RCS – README). Folders may be collaboratively owned across administrations or divisions to meet business needs. When folders are collaboratively owned, each division or administration must identify one owner and one co-owner.

Procedure

a. The Folder Owner will:
   1) Act as the main point of contact to approve user access upon request.
   2) Determine permission level of each new user (read only or modify).
   3) Monitor the folder content for Record Retention requirements and verification and destruction.
   4) Oversee periodic clean-up of folders and electronically stored information (ESI). This should be done annually, or as information becomes outdated.
   5) Remove user access when applicable.
   6) Keep folder owner list found in the RCS README folder (Q:\RCS - README) up to date when staff changeover occurs.
   7) Ensure Tier 3 and subsequent subfolders follow naming convention guidelines.
   8) Send IT request when Tier 1 or Tier 2 folders require destruction.

> Note: Verify with all other applicable folder owners that the folder is no longer needed and ready for destruction. Include confirmation that all folder owners approve destruction when submitting the IT request when applicable.

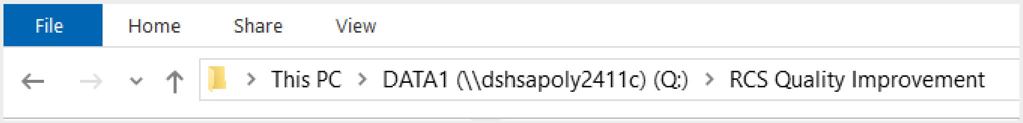
b. The Folder Co-owner will:
   i. Act as a backup contact for staff requesting access when the owner is not available.
   ii. Perform other owner duties as needed or during extended periods when owner is not available.

Section Overview Glossary of Terms Acronym List Table of Contents

4. Creating New Folders

New folders may be created anytime there is a business need.

a. Requests for new Tier 1 or Tier 2 folders must be submitted by a supervisor level or above. Send an IT Helpdesk request and include (see optional template in Resources section):
   1) Folder name of Tier 1 folder using Folder Naming Convention properties, if applicable.
   2) Folder name of Tier 2 folder using Folder Naming Convention properties. Include applicable Tier 1 folder name or path if one exists.

> Example of a path: The paths can be found on the top address bar - Q:\RCS Quality Improvement.
>
> 
>
>
> This PC > DATA1 (\\dshsapoly2411c) (Q:) > RCS Quality Improvement

   3) Owner and co-owner name(s) and position title.
   4) Purpose.
   5) List of personnel needing access to Tier 2 folders including permission level of each user (read, modify).

b. Tier 3 folders and any subfolders can be created anytime business need arise by users with modify rights using Folder Naming Convention properties. Newly created Tier 3 folders and subfolders will inherit the same permissions from the Tier 2 folder level.

> Note: Users with read only access cannot create new Tier 3 folders and must contact the folder owner to request modify rights.

5. Destruction of Folders

Folders may be destroyed when contents have gone through the Records Retention process with Central Files and all contents have been destroyed / removed.

a. Tier 1 or Tier 2 folders must be destroyed by the IT department. Folder owners will submit an IT Helpdesk request when a folder is no longer needed. Include:
   1) Q: drive name and path.
   2) Confirmation you are the owner of the folder and all other applicable owners approve destruction;

b. Tier 3 folders and their subfolders can be destroyed by any user with modify rights after contents have gone through the Records Retention process with Central Files. Users who are not the folder owner will consult with the folder owner before destruction.

C. Folder Access

Purpose

Access control is an important element of security on the Q: drive and formalizes who is allowed to access folders based on the business need of each user. Users are granted access based on their needed permission level. For the purposes of this chapter, permission levels include modify or read only access. Modify access allows for editing and creating new documents. Read only allows users to view and save a copy to their files.

All ALTSA and DDA Q: drive users have read only access to Tier 1 and Tier 2 folders. Users must have approved access with the appropriate permission level to view content within a Tier 2 folder.

1. Requesting and Granting Access and Permissions

Procedure

a. RCS staff will:
   1) Request new user access by emailing the folder owner (or co-owner when owner is unavailable). Requests must include:
      a) Name and position title.
      b) Tier 2 folder name and path.
      c) Reason for access.

> Note: A list of folder owners is available in the Q: drive README folder (**Q:\RCS - README**).

   2) Request increased permission level by emailing the folder owner when applicable. Request must include:
      a) Name and position.
      b) Tier 2 folder name and path.
      c) Reason for requested permission level.

b. Folder owner/co-owner will:
   1) Send an IT Helpdesk request to request user access or permission level request. Requests must include:
      a) Name of new user.
      b) Tier 2 folder name and path.
      c) Permission level of user (read only or modify).

2. Removing Access

a. Folder owner/co-owner will:

1) Request user access removal when applicable by submitting an IT Helpdesk request. Requests must include:

a) Name of user.

b) Folder name and path.

D. Records Retention

Purpose

A record is any document or recorded information (regardless of physical form or characteristics) that is created, sent, organized, or received during business. All RCS records are public records and are owned by DSHS. Accurate records management allows DSHS to retain historical records and respond to litigation, discovery, public records requests, and audits.

Records stored on the Q: drive are considered electronically stored information (ESI) and subject to established retention schedules. Records retention is governed by State General Records Retention Schedules and DSHS Retention Schedules. The state schedules apply to all state agencies and address retention requirements for overarching topics (e.g., administrative functions, legal records, etc.). Sections 1.1 and 2.4 of the DSHS Retention Schedule address retention requirements for RCS.

Procedure

a. Q: drive users will:
   1) Maintain records according to the statue, administrative policies, and record retention schedules in the State General Records Retention Schedules and DSHS Retention Schedules by retaining records according to the applicable schedule and dispose of records which have met retention.
   2) In the case of any accidental destruction of records outside of the required retention schedule:
      a) Notify the folder owner and Central Files of the accidental destruction.
      b) Send an IT Helpdesk request and inquire if documents are recoverable.
   3) Notify the folder owner before destroying content that is used or accessed by others and is not considered a transitory record.

> Example: Transitory records are records with minimal retention value. These include duplicate copies, drafts, empty copies of forms, and records finalized elsewhere. See Resources for additional guidance.

   4) Follow procedures in Chapter 9: Public Disclosure and Discovery (PDD) when files contained within Q: drive are subject to a public records request.
   5) Complete the DSHS Records Management training in the Learning Center annually.

b. Folder Owners will:
   1) Monitor contents of folders to ensure content follows State General Records Retention Schedules and DSHS Retention Schedules.
   2) Create a proposed destruction log using On-Site Records Destruction (DSHS 01-089) when electronic documents are identified for destruction. See Resources section for an example.
   3) Send the unsigned proposed On-Site Records Destruction log to Central Files (RCSCentralFiles@dshs.wa.gov) for review. Central files will review and respond within ten working days.
      a) Include in the subject line of the email "Proposed Destruction Log" and the folder name.

b) Include applicable Tier folder name(s) where the folder exists in the email body. Best practice is to provide the path name.

4) Amend the returned On-Site Destruction log to include only those records approved for destruction by Central Files.

5) Destroy only the approved records and sign the final On-Site Destruction log after destruction.

6) Preserve identified files and folders as identified by Central Files. Best practice is to update file(s) and folder(s) name with information provided by Central files (e.g., destroy date, public disclosure, litigation hold). Public disclosure and litigation holds will not have a destroy date.

> Example: COVID-19 PHE **[Destroy after 03.01.2032]**

> Note: It is not required to log transitory records whose minimum retention is "Retain until no longer needed for agency business."

7) Send the final signed On-Site Destruction log to Central Files at RCSCentralFiles@dshs.wa.gov.

8) Consult with the Records Coordinator with any questions.

c. Users with Modify Rights:

1) Share in the responsibility of meeting records retention guidelines.

2) Notify the folder owner when records are ready for destruction.

d. Central Files will:

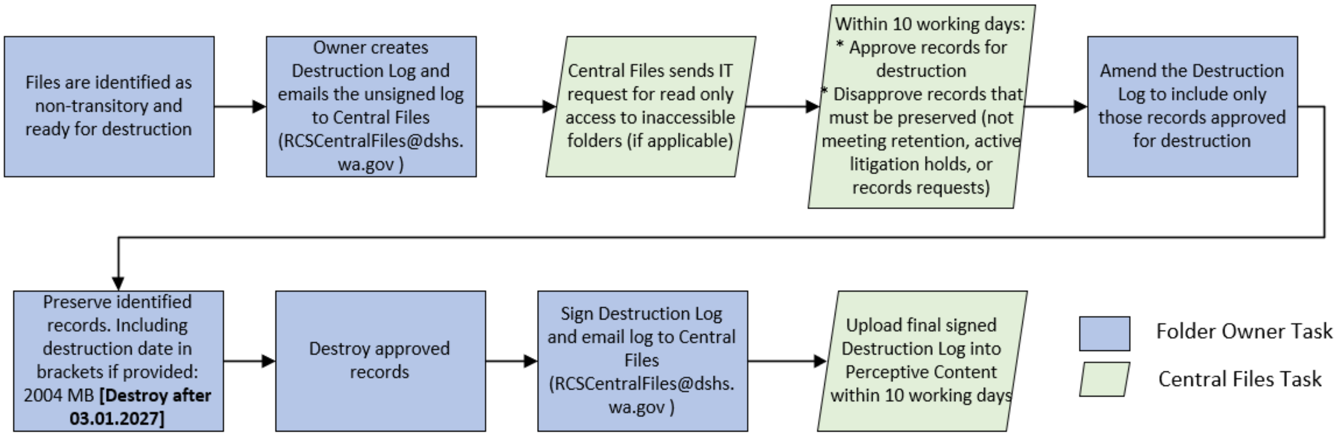
1) Send an IT Helpdesk requesting read only access to inaccessible folders if applicable.

2) Review the proposed On-Site Destruction log to verify contents have no current litigation holds and records meet retention schedules.

3) Respond within 10 working days approving those records that can be destroyed and highlight records that must be preserved with disposition date (if known).

4) Upload the final signed On-Site Destruction log into Perceptive Content within 10 working days of receipt.

Process Map of Records Clean Up

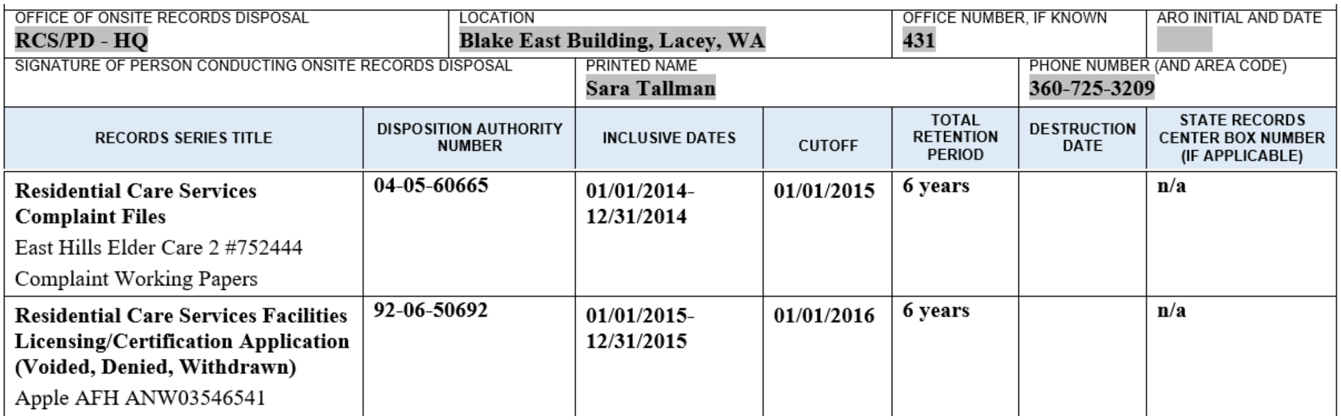

Files are identified as non-transitory and ready for destruction
Owner creates Destruction Log and emails the unsigned log to Central Files (RCSCentralFiles@dshs.wa.gov)
Central Files sends IT request for read only access to inaccessible folders (if applicable)
Within 10 working days:
* Approve records for destruction
* Disapprove records that must be preserved (not meeting retention, active litigation holds, or records requests)
Amend the Destruction Log to include only those records approved for destruction
Preserve identified records. Including destruction date in brackets if provided: 2004 MB **[Destroy after 03.01.2027]**
Destroy approved records
Sign Destruction Log and email log to Central Files (RCSCentralFiles@dshs.wa.gov)
Upload final signed Destruction Log into Perceptive Content within 10 working days
Folder Owner Task
Central Files Task

Section Overview Glossary of Terms Acronym List Table of Contents

Part III: Appendices

A. Resources

1. File naming convention for documents collected in the field.
2. Examples of records with minimal retention value can be found on the Washington State Archives website.
3. Training Resources:
   a. Records Management for DSHS Employees.
   b. Secretary of State Training and Events.
4. Completed On-Site Records Destruction log example:



OFFICE OF ONSITE RECORDS DISPOSAL **RCS/PD - HQ**	LOCATION **Blake East Building, Lacey, WA**	OFFICE NUMBER, IF KNOWN **431**	ARO INITIAL AND DATE
SIGNATURE OF PERSON CONDUCTING ONSITE RECORDS DISPOSAL	PRINTED NAME **Sara Tallman**	PHONE NUMBER (AND AREA CODE) **360-725-3209**	

RECORDS SERIES TITLE	DISPOSITION AUTHORITY NUMBER	INCLUSIVE DATES	CUTOFF	TOTAL RETENTION PERIOD	DESTRUCTION DATE	STATE RECORDS CENTER BOX NUMBER (IF APPLICABLE)
Residential Care Services Complaint Files East Hills Elder Care 2 #752444 Complaint Working Papers	**04-05-60665**	**01/01/2014-12/31/2014**	**01/01/2015**	**6 years**		**n/a**
Residential Care Services Facilities Licensing/Certification Application (Voided, Denied, Withdrawn) Apple AFH ANW03546541	**92-06-50692**	**01/01/2015-12/31/2015**	**01/01/2016**	**6 years**		**n/a**

B. Tools

Optional template to request a new Tier 1 or Tier 2 folder.

Request for New Q: drive Folder Creation		
Tier 1 Folder Name		
Tier 2 Folder Name (include the path when requesting a new Tier 2 folder under an existing Tier 1 folder)		
Owner Name and Position Title		
Co-Owner Name and Position Title		
User access **Name**	**Title**	**Permission Level** **(read only, modify)**
List of users needing access to Tier 2 folder		

C. Glossary of Terms

Access Control – A data security process that enables organizations to manage who is authorized to access data and resources.

Co-Owner – Fulfills the role of the folder owner when owner is unavailable. Primarily used to grant user access but may take on additional responsibilities during prolonged absences.

Deficient practice – The action(s), error(s), or lack of action on the part of the provider/licensee relative to a requirement and to the extent possible, the resulting outcome.

Deficient practice statement (DPS) – A statement at the beginning of the evidence that sets out why the entity was not in compliance with a regulatory requirement. Also commonly referred to as the "based on" statement.

Department – This term refers to the Washington state Department of Social and Health Services (DSHS).

Destroy/Destruction – Permanent deletion of an electronic record.

Disposition – To change the custody, location, or nature of DSHS records including transfer, microfilming, duplication, destruction, or deletion.

Drive – a device where users can save or retrieve files including hard drive, CD drive, USB flash drive.

Electronically Stored Information – DSHS records stored in an electronic format. Requires hardware and software to be accessed and read (e.g., spreadsheets, databases, images, video recordings). Also known as electronic records.

Folder – A type of aggregation or container within a file system used to store related records and folders.

Identifier – The name, title, or letters/numbers referring to entity staff or those living in the residential setting. Do not use the symbol # in front of the identifier number.

Modify - Allows users to read, write, and delete files and subfolders.

Owner – User who has control over the file or folder to grant access to the contents. Owners may be the creator of the folder or adopted previously created folders due to staff turn-over.

Path – The specific location or route a file or directory can be accessed within a file system. Paths represent the hierarchy of directories or folders leading to a particular file.

Permissions – operations associated with a shared resource such as a file or directory that are authorized by the system administrator for individual user accounts or administrative groups.

Provider – a) any individual or entity that provides services to DSHS, OR b) a person, group, or facility that provides services. RCS providers include Adult Family Homes, Assisted Living Facilities, Certified Supported Living providers, Enhanced Services Facilities, ICF/IID facilities and Nursing Homes.

Read Only - Allows users to view and download contents of the folder and subfolder.

Record – any document or recorded information regardless of physical form or characteristics created, sent, organized, or received by the agency in the course of public business.

Record Management – the practice of formally managing records in a file system (electronic or paper) including classifying, capturing, storing, and disposal.

Records Retention – The required minimum amount of time a records series must be retained to meet legal, fiscal, administrative, or historical value as listed on an approved records retention schedule or general records retention schedule.

Records Retention Schedule – a legal document approved by the state or local records committee that specifies minimum retention periods for a records series and gives agencies ongoing disposition authority for the records series after the records' approved retention period has been satisfied.

Shared Drive – A specialization of an operating system file system, comprising of a shared device (e.g. server space) used by multiple users and accessed over either a local area network or a wider area network connection.

Shared File – an electronic record (e.g., spreadsheets, word documents, images) with permissions granting additional users to access the record.

Shared Folder – a container within a file system with permissions granting additional users to access the contents held within.

Statement of deficiencies (SOD) – The official written report document from RCS staff that identifies violations of statute(s) and/or regulation(s), failed facility practice(s) and relevant findings found during a complaint/incident investigation conducted at an any setting regulated by RCS.

Transitory Records – records that can be destroyed when no longer needed for agency business. A transitory record does not require memorializing on a destruction log. Examples include copies of blank forms or publications, duplicate copies, working notes that have been written up into a formal record.

D. Acronym List

AA	Administrative Assistant
AFH	Adult Family Homes
ALF	Assisted Living Facilities
ALTSA	Aging and Long-Term Support Administration
ASPEN	Automated Survey Processing Environment System
BIC	Back In Compliance
BMP, GIF, JPEG, PNG, TIF, TIFF	File formats (and their extensions)
CCRSS	Certified Community Residential Services and Supports
DSHS	Department of Social and Health Services
eDoc	Electronic Document
ePOC	Electronic Plan of Correction
ESF	Enhanced Services Facilities
EWP	Electronic Working Papers
ICF/IID	Intermediate Care Facilities for Individuals with Intellectual Disabilities
IT	Information Technology
LTC	Long-Term Care
NH	Nursing Homes
PDD	Public Disclosure and Discovery
PDF	Portable Document Format
POC	Plan of Correction
RCS	Residential Care Services
RCW	Revised Code of Washington
RMT	Records Management Tool
SOD	Statement of Deficiency
SOP	Standard Operating Procedures
STARS	Secure Tracking and Reporting System
VPN	Virtual Private Network
WAC	Washington Administrative Code

Section Overview Glossary of Terms Acronym List Table of Contents

E. Change Log

Eff. Date	Chapter/ Section #	Description of Change	Reason for Change	Communication and Training Plan
05/23/2024	Part 2 Network Drive	Establish of Subchapter	Provide guidance to staff. Definitions & acronyms added for clarity	MB R24-049
04/30/2024	Part 1 & 2	Added content: Part 1: Electronic packet procedures Part 2: Definitions & Acronyms	Electronic packets are a new procedure. Definitions & Acronyms added for clarity	MB R24-039 Dedicated training for new packet procedure 2/22/2024
04/30/2024	Part 1	Added Sections on Scanners & Shared File management Moved from Chapter 1.	Sections moved to align with chapter focus.	MB R24-039 Weekly Update 3/1 review of SOP changes
04/30/2024	Full Chapter	Changed Chapter Name to “Record Management”	Name changed to reflect scope of chapter contents.	MB R24-039 Weekly Update 3/1 review of SOP changes
04/21/2023	Full Chapter	Complete chapter due to the conversion of hardcopy records to electronic form	New IT systems to manage records.	MB R23-039

Section Overview Glossary of Terms Acronym List Table of Contents