NIH RECORDS MANAGEMENT
GUIDANCE FOR UNAUTHORIZED DISPOSAL OF FEDERAL RECORDS

The following guidance is targeted towards National Institutes of Health (NIH) Institute, Center, or Office (ICO) Records Liaisons (RLs) who have management and oversight of paper and electronic Federal records.

What are the requirements for Unauthorized Disposal of Records?

The NIH is required to notify the National Archives and Records Administration (NARA) of any "actual, impending, or threatened unlawful or accidental removal, defacing, alteration, corruption, deletion, erasure, or other destruction of records in the custody of the agency" according to (36 CFR Part 1230). The statutory authorities for requirement are is 44 U.S.C. 3105 and 3106.

Unlawful or Accidental Destruction (Unauthorized Disposal) includes:

- Disposal of an unscheduled or permanent record.

- Disposal prior to the end of the NARA-approved retention period of a temporary record.

- Disposal of a record subject to a FOIA request, litigation hold, or any other hold requirement to retain the records.

36 CFR 1230.3 DEFINITIONS

Alteration: unauthorized annotation, addition, or deletion to a record.

Deface: to obliterate, mar, or spoil the appearance or surface of a record that impairs the usefulness or value of the record.

Removal: selling, donating, loaning, transferring, stealing, or otherwise allowing a record to leave the custody of a Federal agency without the permission of the Archivist of the United States.

NIH STAFF RESPONSIBILITIES

As noted in Manual Chapter 1743 Managing Federal Records, all records created and maintained by NIH ICOs must be managed according to the applicable laws and regulations.

NIH staff must immediately report submit reported incidents of record removal, alteration, loss, or destruction to their appropriate ICO Management and Supervisory Officials. NIH Supervisors who are notified about unauthorized disposal must report these incidents to the appropriate ICO Records Liaisons. ICO Records Liaisons must reports any incidents of unauthorized disposal to the NIH Records Officer. These incidents must be reported as soon as NIH staff are

aware of the situation.

It is the responsibility of each ICO to monitor the records they create and maintain to prevent unauthorized disposals, which is illegal under Federal law and carries penalties of a fine and up to three years of imprisonment.

ICO's should establish clear internal processes that designate recordkeeping roles and responsibilities such as Record Custodian(s) and Record Owner(s) to ensure Federal records are identified, managed, and captured. ICO staff should be encouraged to establish open communication with the ICO Records Liaison.

Questions to consider include:

How can NIH staff prevent the accidental deletion of Federal Records within my ICO?

DO:
- Be mindful of the ICO's file plan(s). All NIH records schedules and file plans are located within the Records Schedule System (RSS). The file plan(s) list disposal authorities for all records created by the ICO.

- Promptly dispose of temporary records once eligible for destruction unless there is a continued business need. If disposal of eligible temporary records is not prompt, NIH is obligated to include those records in response to a litigation discovery or FOIA request.

- Establish preventative measures to protect permanent records from disposal.

- Manage electronic records in a recordkeeping system, electronic information system, or accessible location such as SharePoint, OneDrive, or a Shared Network Drive.

DON'T:
- Destroy any Federal records without consulting with the ICO Records Liaison or ICO Records Custodian. NIH records must not be destroyed except under the provisions of NARA-approved NIH records schedules or the General Records Schedules (GRS) issued by NARA.

- Save official Federal records on your local hard drive C: or Home H: drive.

What are recommended steps of recovery if there is awareness of accidental disposal of Federal records?

Data recovery is critical when there is knowledge of accidental disposal or deletion of Federal records. There are several practical steps in recovering records.

General Recovery Tips to Consider:

- Reach out to NIH staff/Program offices who might have received or created a copy of the loss document(s).

- Search through old email to see if another copy has been saved.

- Open the recycle bin or deleted/sent items folder to see if a soft delete has occurred.

For the deletion of electronic records, interaction with the NIH Center for Information Technology (CIT) is a good place to start.

SharePoint/OneDrive:

When recovering files located in either SharePoint sites or OneDrive, the ICO staff should submit a ticket with CIT to retrieve the documents accidentally deleted.

SharePoint/OneDrive files are kept in a recycle bin for 90 days before permanent deletion. If a file is accidentally deleted from SharePoint or OneDrive, it can be recovered by CIT within that 90-day period.

Email:

When recovering emails the ICO staff should submit a ticket with CIT to retrieve the emails accidentally deleted.

NIH work-related email sent or received by Non-Capstone Officials that is marked for deletion is kept in a hidden folder for 14 days before it is permanently deleted. If an email was accidently deleted, it can be recovered by CIT within that 14-day period.

NIH work-related email sent or received by Capstone Officials are permanent records. If an email is marked for deletion it is kept in a hidden folder.

All NIH staff (Capstone and Non-Capstone Officials) will have the ability to mark email(s) and folders that are not work-related. All non-work-related emails or folders are not subject to retention policies but remain accessible to users in their inbox. If non-work-related emails are accidentally deleted, they can be recovered within 14 days.

Shared Network Drive:

If accidental deletion has occurred in a NIH shared network drive you can:

Navigate to the folder that used to contain the file or folder, right-click it, and then select Restore previous versions. If the folder was at the top level of a drive, for example C:\, right-click the drive, and then select **Restore previous versions**.

You'll see a list of available previous versions of the file or folder. The list will include files saved on a backup (if you are using Windows Backup to back up

your files) as well as restore points if both types are available.

Note: To restore a previous version of a file or folder that's included in a library, right-click the file or folder in the location where it's saved, rather than in the library. For example, to restore a previous version of a picture that's included in the Pictures library but is stored in the My Pictures folder, right-click the My Pictures folder, and then select Restore previous versions.
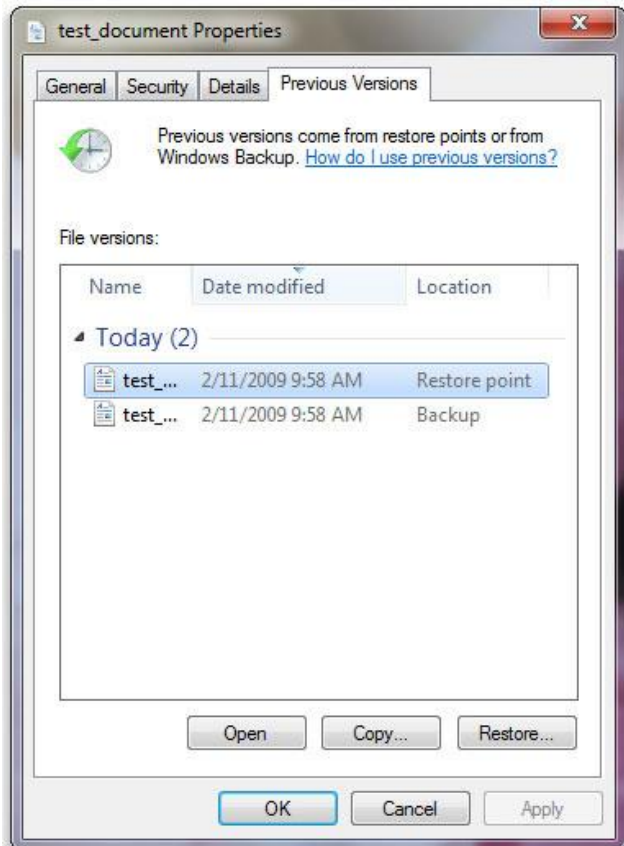

Figure 1 Picture of Restoring a Previous Version of a File

Some previous versions of files:
1. Double-click a previous version of the folder that contains the file or folder you want to restore. (For example, if a file was deleted today, choose a version of the folder from yesterday, which should contain the file.)
2. Drag the file or folder that you want to restore to another location, such as your desktop or another folder.

   The version of the file or folder is saved to the location that you selected.

Note: If the folder that has been accidently deleted is more than several layers deep, assistance from a CIT administrator might be needed. Restoration attempts might not be successful due to the multiple levels within that folder. When this happens, the ICO staff should submit a ticket with CIT to retrieve the documents accidentally deleted.

Periodically, records can be accidentally deleted when manually copying and/or moving files. It is a safe practice to consult with IT support when migrating files. IT support may be able to automate migration through scripting. If this is not possible, use caution when manually copying and moving files. You can manually perform these tasks by using the right click of the computer mouse to copy or move a file. The right click will provide a prompt which alerts you of your next action.

How do I respond when recovery efforts are not successful?

If records are accidentally deleted and recovery efforts are not successful. NIH staff must notify their immediate supervisor of any accidental removal, defacing, alteration, or destruction of records in their custody. Supervisors must notify their ICO Records Liaison. The Records Liaison must report the incident to the NIH Records Officer. A full description of the circumstances surrounding the incident must be taken:

Per 36 CFR part 1230.14, the report should include:

- Complete description of the records, along with volume and dates if known;

- The office that maintains the records;

- An explanation of the exact circumstances surrounding the removal, defacing, alteration, or destruction of records;

- Details, when appropriate, of the actions taken to salvage, retrieve or reconstruct the records; and,

- A statement of safeguards established to prevent further loss.

REFERENCES:

- HHS Policy for Records Management

- NIH Records Management Guidebook

- NIH Manual Chapter 1743 Managing Federal Records

- NARA Guidance: Disposition of Federal Records: A Records Management Handbook

- Unlawful of Accidental Removal, Defacing, Alteration, or Destruction of Records, 36 CFR, Chapter XII, Subchapter B, §§ 1230.1 – 1230.18 (2011).

- NARA Unauthorized Disposition of Federal Records Case Files

- NARA Bulletin 2013-03: Guidance for agency employees on the management of Federal records, including email accounts, and the

protection of Federal records from unauthorized removal.