Maintaining and Providing Electronic Research Records

The purpose of this guidance is to assist researchers in the use and storage of electronic study documents (i.e., research records), and how to share study files securely with the Institutional Review Board (IRB) Compliance team in preparation for post-approval monitoring and directed (for-cause) reviews.

Contents

General Information

The IRB Office Compliance team conducts routine and directed reviews of research. Read about these processes in detail on our dedicated Post-Approval Monitoring, Directed Reviews (For-Cause Audits), and SOPs pages.

The Principal Investigator (PI) is required to make research records available for review and to comply with applicable institutional policies governing data security, storage, and access.

The PI is responsible for maintaining adequate research records in compliance with the IRB's Research Document Retention Requirements for Principal Investigators. Review the Investigator Manual (HRP-103) for additional PI responsibilities. The IRB Office provides the Research Record Components tool to assist investigators in maintaining research documentation in compliance with best research practices, IRB standards, and applicable regulatory and institutional requirements. Researchers should maintain their research records electronically.

See the Resources section at the end of the guidance for additional links to guidance and policies.

Advantages of Electronic Records

Security and Confidentiality: Electronic records, if encrypted and stored in secure, password-protected environments, will significantly reduce the risk of unauthorized access or loss of sensitive data. This is crucial in research settings, where confidentiality is a priority for protecting participant privacy and maintaining compliance.

Accessibility and Convenience: Electronic records can be accessed remotely by authorized individuals from a location with secure access. This is especially beneficial when research collaborators are geographically dispersed by plan or in response to emergent situations. Additionally, electronic records enable researchers to provide oversight agency representatives with easy access to perform required routine or for-cause reviews. Paper records may be harder to access or share quickly, especially in a time-sensitive environment.

Audit Trail and Data Integrity: Electronic systems can be set up to track changes, updates, and modifications with audit logs, providing a clear history of all actions taken with a particular document. This is critical for maintaining the integrity of the data and ensuring that it remains unaltered unless authorized. With paper records, it can be more difficult to track alterations or provide an audit trail. Of particular relevance is the ease with which electronic storage enables creating and maintaining backups of research records to protect against emergent situations.

Efficiency in Storage and Organization: Digital records eliminate the need for physical storage space and can be easily organized, tagged, and indexed for quick retrieval. They can also be searched by keywords, making it easier to locate specific files or pieces of information, as opposed to sifting through large paper files.

ALCOA+C: Electronic records may ease compliance with ALCOA+C standards. ALCOA+C is an acronym for good clinical research documentation that applies to FDA (21 CFR 58.130.e) and GCP E6 R3 (C.3.1.) regulations. ALCOA + C stands for:

A: Attributable

L: Legible

C: Contemporaneous

O: Orignal

A: Accurate

+C: Complete

Please refer to the Galter Health Sciences Library & Learning Center ALCOA resource for additional information regarding ALCOA documentation standards.

Maintaining Electronic Documentation

Paper-based source documents, including signed informed consent forms, can be scanned and saved to an appropriate cloud storage location. The Principal Investigator or designee should certify that all pages, not just the signature pages, are captured when scanned, with no obscured or cut-off text, within a note-to-file. Consider verifying and documenting the sponsor's agreement to accept electronic storage of research records. Electronic records must be stored securely, with access only to approved individuals. See the Resources section for applicable security policies. See the Electronic Study File Folder Examples section for guidance on Electronic Records Naming Conventions.

Converting paper records into electronic format requires an upfront investment in time, resources, and possibly technology, but the benefits are long-term. These include improved organization, better compliance with institutional and regulatory standards, enhanced security, and more efficient management of research records.

Other requirements may apply based on your study's regulatory oversight. Research regulated by the Food and Drug Administration (FDA) may have additional recordkeeping requirements. The FDA requires certified copies of source documents. See 21 CFR Part 11 and Electronic Source Data in Clinical Investigations (fda.gov) for further information. If your research involves protected health information (PHI), the Health Insurance Portability and Accountability Act (HIPAA) requires covered entities and business associates to implement administrative, physical, and technical safeguards to protect electronic protected health information (ePHI). These requirements are primarily found in the HIPAA Security Rule (45 CFR §§ 164.302–318). PIs must understand the requirements that apply to their research and ensure that their data and retention plans satisfy those requirements.

Providing Electronic Documentation

It is appropriate to provide the Compliance team remote access to the research records when requested. The IRB Office Compliance team generally utilizes SharePoint, Northwestern University's preferred secure platform, to obtain access to copies of study documents from researchers. eIRB+ does not serve as an electronic version of your research records.

When the Compliance team requests study documentation from the study team, the Compliance unit will provide access to a SharePoint folder for the study team to share requested documents. The Compliance team will provide instructions in the post-approval monitoring and directed (for-cause) audit notification letters, including deadlines for providing access and soliciting a list of those individuals on the research team to provide access to the review folder. In addition to the specific instructions, the following are general guidelines the researchers should follow:

- The study team should upload copies of the requested documents to the designated SharePoint folder (while retaining their local copies).
- For any requested documents maintained in a paper-based format, the study team is responsible for uploading scanned electronic copies to the designated SharePoint folder.
- Any requested participant files or data should be unredacted.
- Files and folders should be clearly named and organized, and include a folder map if necessary (see below section Electronic Study File Folder Examples).
- The PI and study team are responsible for uploading the requested documents to the SharePoint folder by the requested deadline date.

If research data is housed in a proprietary system(s) (e.g., Complion, REDCap, study-specific electronic data capture (EDC) database), the PI is responsible for granting the Compliance team access to the system(s), facilitating a brief introduction and training on how to navigate their data within the system(s), and assigning a knowledgeable designee from the research team to be available during the review to promptly respond to Compliance team queries and resolve system access issues.

Resources

The following links are provided to assist Investigators and may not represent all relevant institutional policies and regulations.

Researchers must follow their own school's or unit's requirements in alignment with School and Unit Policies: University Policies.

Northwestern University Information Technology

- Choosing Appropriate Data Storage
- Research Data Storage Service
- Research Data Management and Storage
- Organize, Describe, Preserve, and Share
- Document Sharing and Data Storage Finder

Northwestern University IRB Office

- Human Research Policies & Guidance Page
- Investigator Manual (HRP-103)
- Research Document Retention Requirements for Principal Investigators (HRP-1914)
- Study Support Resources and Templates
- Post-Approval Monitoring Checklists

Northwestern University Feinberg School of Medicine

- Data Security Plan Requirements for FSM Research
- Data Storage Policy: Feinberg Information Technology

FDA

- Electronic Source Data in Clinical Investigations (fda.gov)
- 21 CFR Part 11

HIPAA

- HIPAA, PHI, and PII
- 42 CFR 164.530
- Summary of the HIPAA Security Rule

Electronic Study File Folder Examples

Electronic Records Naming Conventions

Electronic record file and folder names should be readable and relevant to the document and folder's content. For example:

- Title: "DCIM_0238251" does not provide pertinent information.
- Title: "Participant001_Visit2_ECG" provides additional helpful context that this is the ECG document for Participant 001's Study Visit #2.

Storing records in a logical nested folder structure aids in ease of access and comprehension. For example:

Participant_0378

- Eligibility Checklist
- Signed Informed Consent Form(s)
- Visit/Status Tracker
- Completed Questionnaires
- Payment Record
- Notes-to-File

See the IRB Office's Study Support Resources for a Regulatory Binder Checklist or Research Record Components