Mass General Brigham Human Research Affairs

GUIDANCE FOR INVESTIGATORS

Electronic Storage of Research Documents

This guidance presents an acceptable process for creation of electronic copies of source documentation (including consent documents). This guidance is applicable to Investigator-initiated research, including NIH funded and FDA regulated research. Industry and other Sponsors generally have specific requirements for electronic records to comply with 21 CFR Part 11, when applicable. Investigators should seek the written permission of the Sponsor and follow the Sponsor's requirements for electronic storage of source documents prior to creation of electronic source document storage. Documentation of Sponsor permission should be filed with study documents.

In order to convert existing paper source documentation to electronic source documentation the site must create a ***certified copy***. A ***certified copy*** is "a copy of original information that has been verified, as indicated by a dated signature, as an exact copy, having all of the same attributes and information as the original."

As with all research activities, the principal investigator (PI) is responsible for maintaining adequate records. The PI should therefore ensure that this guidance is followed when implementing electronic storage of source documents. It is recommended that Investigators create an SOP describing how source documents will be scanned, certified, and stored.

See also PHS-1055 Guidelines on Retention of Research Data, Materials, and Records

Recommended Procedures

(1) Creation of electronic files

Source documents/consent forms should be scanned individually and converted to an Adobe Acrobat PDF file. The PDF file name should be labeled with:

- The study's IRB assigned protocol number
- The study's assigned subject ID
- The date the source document was obtained or completed
- A word identifying the specific source document (e.g. "consent", "HAM-D")
  (For example: 2015P000000_A12345_20150531_consent)

(2) Certification of electronic files

The person who certifies the copy as an accurate and complete representation of the original, having all the same attributes and information as the original, should be the same person who actually created the electronic copy from the original. The person certifying is verifying that they have done all of the following:

- Reviewed all pages of the scanned document and confirmed that they are EXACT copies of the originals.
- Confirmed that each scanned page is legible and facing in the appropriate direction.
- Confirmed that wet ink signatures and dates are legible on the scanned document.

Although the PI does not have to personally certify every document, the PI still bears the responsibility for

ensuring that the certification process is being followed.

(3) Methods and storage of electronic files

Different software and applications can be used to create certified copies. For FDA regulated research documentation, systems and processes should be FDA compliant (including 21 CFR Part 11). For non-FDA regulated research documentation, systems must comply with Mass General Brigham policies.

In all cases, the person performing the certification should use their own personal account, identification, key or unique credentials. Using a shared account or someone else's account, such as a PI's account, does not comply with regulatory requirements or Mass General Brigham policies.

Electronic files of scanned and certified source documents should be stored on a Mass General Brigham secure file area (e.g. SFA, DFA) that is routinely backed up. Contact Information Systems to ensure the secure file area is backed uproutinely.

Frequently Asked Questions

1. ***Is IRB approval required when converting paper source documents to electronic storage?***

   No, IRB approval is not required to convert study source documents to electronic documents. An internal SOP for document scanning and certifying should be maintained on site. Additionally, records of documents scanned, and documentation of certification should be maintained onsite.

2. ***Once scanned, certified and placed on a Mass General Brigham server, can the paper documents be destroyed?***

   Yes, once the document is scanned and certified, the paper copy can be destroyed.

3. ***At what point can source documents be scanned and stored?***

   Anytime, as long as the site has a process/procedure for scanning, certifying, and storing electronic documents.

4. ***Can this be done for an ongoing (still enrolling) study?***

   Yes.

5. ***Can the person creating the electronic files be the person to certify the copies?***

   The person who certifies the copy as an accurate and complete representation of the original, having all of the same attributes and information should be the same person who actually created the electronic copy from the original. They must use their personal key, account or credentials when certifying the copy.

   As with all research activities, the principal investigator (PI) is responsible for maintaining adequate records. The PI should therefore ensure that this guidance is followed when implementing electronic storage of source documents.

6. ***How long should electronic source documents be maintained?***

   Consistent with record retention requirements for paper source documents, electronic files of source documents should be kept for a minimum of 7 years following study closeout and in accordance with institutional policy. Sponsored studies may have additional requirements, which would need to be met in addition to institutional policy.

7. How should Sponsor's permission for electronic storage of source documents be documented?

Sponsors should agree to electronic storage of source documents in writing. This can be in the form of an email or letter. This email or letter should specify the person granting permission and their job title. Documentation of sponsor agreement should be kept on file.

8. Is REDCap 21 CFR Part 11 compliant? What language can we submit to the sponsor if we want to use REDCap?

You can use the following language to request the use of REDCap from a Sponsor:

REDCap (**R**esearch **E**lectronic **D**ata **Cap**ture) is a web-based application hosted by Mass General Brigham Research Computing, Enterprise Research Infrastructure & Services (ERIS). As validated by Mass General Brigham, ERIS, and supported by Mass General Brigham Policies, REDCap has the controls necessary tostore scanned source documentation for 21 CFR Part 11 compliant studies.

Vanderbilt University, with collaboration from a consortium of academic and non-profit institutional partners, develops this software application for electronic collection and management of research and clinical study data. The REDCap Consortium is composed of thousands of active institutional partners in over one hundred countries who utilize and support REDCap in various ways. The REDCap Consortium's Part 11 Compliant Project's goal is to develop and maintain documentation and system features to ensure regulatory compliance. The FDA does not provide an overarching determination of compliance for any application. Only after a successful FDA audit of a study using REDCap, will it imply that REDCap can be used in compliance with 21 CFR Part 11. This has yet to happen across the REDCap Consortium or here at Mass General Brigham.

REDCap Resources:
REDCap Project: https://projectredcap.org/
REDCap at Mass General Brigham:
https://rc.partners.org/redcap
21 CFR Part 11: https://rc.partners.org/redcap/part11

9. What other tools/technologies can we use to certify copies?

In addition to REDCap, technologies that create a signature or certification on a PDF are acceptable as long as they comply with 21 CFR Part 11. Compliance includes, but is not limited to: systems validation, audit trail of the document to ensure no changes or only tracked changes have been made after certification, and access controls. Please contact riso@partners.org with any questions about technologies.

10. Can electronic source documents be maintained on Mass General Brigham network drives?

Electronic source documentation must be maintained in a secure file area (e.g. SFA, DFA).

11. Do all pages of the informed consent form need to be scanned, or just the signature page(s)?

All pages of the informed consent document should be scanned, verified and certified.