UNIVERSITY of SOUTH FLORIDA

Records Retention Guidance

Policies and guidelines regarding the retention and destruction of research records and consents are essential to keeping sensitive data and information private and secure. USF QA/QI and IRB have developed this guidance document to support researchers in maintaining and adhering to effective record retention. To support comprehension of this information the guidance will define essential terms and then list out crucial questions and answers regarding effective record retention.

Common Terms and Definitions:

Retention Periods: Institutions and regulatory bodies make specific determinations on how long research records, including the original signed consent forms, should be retained. This period is determined based on the type of research, potential future use of the data, and legal requirements. USF IRB requires that Investigators maintain their human subjects' paper and digital research records, including the original signed and dated consent documents, for at least five (5) years after completion of the research. If the research is HIPAA regulated, Investigators are required to store the original signed and dated HIPAA authorizations and consent documents that include HIPAA authorizations for at least six (6) years from the date of their creation or from the date on which they were last in effect, whichever is later. If your research is non-FDA, GCP or HIPAA regulated, the IRB may be able to approve the digitization of research records including signed consents. Contact the IRB at RSCH-IRB@usf.edu to discuss your research storage options.

Data Security and Confidentiality: Policies often include guidelines on maintaining the security and confidentiality of research records during the retention period. This may involve measures such as secure storage, restricted access, and data encryption. USF IRB affirm that Investigators are responsible for outlining in the protocol the information to be collected as part of the research and the measures that will be taken to protect the confidentiality of the data while the research is being conducted as well as when it is complete. If Investigators and study team plan to store protected health information (PHI) or sensitive PII (see definition below) in Box, they are asked to contact USF IT at secops-help@usf.edu to set up the study Box folder **before** storing data on the cloud. Investigators and study team will need to include the name of the Principal Investigator (folder owner), study title, data to be stored, and a list of IRB-approved study team members in your email to USF IT.

Sensitive Personally Identifiable Information (PII): Information that if lost, compromised, or disclosed could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Sensitive PII includes but is not limited the following types of data: SSNs, medical information (e.g. diagnoses, information about illicit substance use), insurance information, student information, and information about sexual behaviors and criminal history.

Notification and Approval: Some policies require researchers to notify relevant authorities or seek approval before destroying research records. This is often the case when the research is subject to ongoing monitoring or regulatory oversight. USF IRB affirms that Investigators are responsible for familiarizing themselves and the study team on the notification and approval requirements of the overseeing body of the study. This information is specific for each study and should be included with the study protocol and/or within the study BullsIRB approval letter.

Destruction Procedures: There are usually specific procedures for the proper destruction of research records at the end of the retention period. This may involve shredding physical documents or securely deleting electronic files. This information is specific for each study and should be included within the study protocol and/or within the study BullsIRB approval letter.

Common Questions and Answers:

Below are some common questions and answers that support researchers in comprehending effective research record retention.

What Are Electronic Records and Electronic Signatures?

Many researchers are now implementing electronic records (e.g. source documents) and regulatory records. Electronic records are generally defined as a collection of information, text, images, data, and all other media that is created, edited, stored, managed, and distributed digitally using computers. Usually, these records hold the same information as a hard printed record, the only difference is that the records exist digitally. Likewise, an electronic signature is considered with the same authority as a conventional legally binding handwritten signature, but instead of being on paper, it's a digital symbol within a computer system.

What Defines "Electronic" Record-keeping?

Many institutions and researchers are confused by what they see as broad, high-level rules expressed in FDA's 21 Code of Federal Regulations (CFR), Part 11. There are two core principles of Part 11 that determine if it applies:

1. When researchers **choose to use records in electronic format** in place of paper format, Part 11 would apply.
2. If a device is used to print electronic records and staff rely on paper records to perform research regulated actions, **it would not be considered using an electronic record in lieu of paper records.** You see in this case, study teams are simply using an electronic record to create a paper record, and thus Part 11 would not apply.

If the facility uses hard copy records for distribution amongst the study team, but ultimately digital records are used to perform research regulated actions, chances are the FDA will deem this as electronic record. Whichever method is used, it's important to document all details and the steps involved in either a specification document or a Standard Operating Procedure (SOP) for regulators and/or inspectors to review.

Should I Keep a Detailed Audit Trail?

Clinical research institutions, CRO's and inspectors may also decide to enforce rules encompassing time-stamped digital audit trails. Researchers should be diligent when recording times, sequences of events, and all entries into the applicable record-keeping system. Incorrect records (no matter how insignificant the issue might seem) can lead to bigger problems as well as open the door to more comprehensive investigations. Also be aware that audit trials are mandatory in cases where users of the electronic records system are expected to create, change, or delete regulated records.

What are Older Legacy Systems?

If you're using an electronic records system that's been in place before August 20, 1997, chances are you aren't required to follow FDA's 21 Code of Federal Regulations (CFR), Part 11 requirements. The agency has stated it intends to "exercise discretion" if electronic records system were operational and compliant before this date, or if documented evidence is available to justify the electronic records system as appropriate for its intended use. However, if you are using a legacy electronic records system and this system has been updated after August 20, 1997, Part 11 controls will need to be applied to both electronic records and electronic signatures.

How Do I Store Consents and Research Records?

Investigators must store original hard copy data and documents (including original signed consent documents) and electronic data in a secure location as described in the IRB-approved protocol. Investigators will need to provide access to copies of electronic records when examiners arrive for inspections. This includes informed consents (ICF/ICD).

Be aware that ICF/ICDs and research data should not be a part of the participants' medical records as ICF/ICD's have a different confidentiality process. In most cases the subject doesn't have to request a copy of their ICF/ICD, but they will have to submit forms for copies of their medical records. Once a participant has been provided with a copy of their signed study consent, a signed copy of the ICF/ICD is always retained as part of the research records. This documentation serves as evidence that the participant was adequately informed and willingly agreed to participate in the research.

In some cases, the ICF/ICD may be stored alongside the participant's medical records, especially if the research involves access to or use of medical information, but in most cases this document should NOT be a part of the participant medical record. It is recommended that USF study teams store digitized signed ICF/ICD and all other digital research records/source documents within the study Florence electronic system, or a Box folder created by USF IT. It is also suggested that researchers keep records in sharable, easy read file formats like PDF, XML, and SGML.

Summary

Researchers are responsible for familiarizing themselves with and adhering to proper and adequate hard and electronic research records retention policies and guidelines. They are also required to document and report the disposal or destruction of research records as part of their ethical and regulatory obligations. While the language used in Part 11 can be difficult to comprehend, its guidelines are relatively limited in scope. If researchers need compliance remediation in reference to Part 11 or any other FDA regulation, it is suggested that they review the FDA guidance documents below or reach out to the USF QA/QI Team (QA-QI@usf.edu) to help develop quality practices and support study team training efforts.

For more information on record retention and other compliance documents, visit the QA/QI website: Researcher Tools | QA/QI | Integrity & Compliance | Research & Innovation | USF or email QA/QI: QA-QI@usf.edu. You may also review the USF IRB Investigator Manual or email the IRB: RSCH-IRB@usf.edu

You may also review these FDA guidance documents: The Complete Guide to Compliance Remediation, 5 Items to Stock in Your FDA Inspection War Room, Clinical Research and Electronic Informed Consent