Wake Forest Baptist Medical Center	**Retention and Destruction of Human Subjects Research Data/Records** RARI-S-03-05	**Dept:**	**CTSI**
		SOP Number:	
		Effective Date:	10/18/17
		Current (Revised) Date:	
		Contact:	**Office of Regulatory Affairs and Research Integrity - CTSI**
Approval Signature:		**Date of Signature:**	10/18/17
Name and Title: Christopher O'Byrne VP, Research Admin + Operations			

1) **General Procedure Statement:**
It is the standard operating procedure (SOP) of Wake Forest Baptist Medical Center to comply with all regulatory requirements regarding retention, storage and destruction of human research data and study records. In addition, it is the intent of Wake Forest Baptist Medical Center to honor the negotiated and accepted terms of grants or contracts with sponsors that extend retention or increase data security beyond the minimum requirements presented in this SOP. The requirements herein are to serve as a guide to the minimum standards. It is important to note, however, that each research study must meet any additional requirements originating from specific agreements or sponsor restrictions on data and records related to the study.

   a) Scope: All WFBMC employees, faculty and staff are responsible for complying with this SOP

   b) Responsible Department/Party/Parties:
      i. Procedure Owner: Clinical Translational Science Institute (CTSI)
      ii. Procedure: Office of Regulatory Affairs and Research Integrity
      iii. Supervision: Office of Regulatory Affairs and Research Integrity
      iv. Implementation: Office of Regulatory Affairs and Research Integrity

2) **Definitions:** For purposes of this SOP, the following terms and definitions apply:

   a) **WFBMC:** Wake Forest Baptist Medical Center and all affiliated organizations including Wake Forest University Health Sciences (WFUHS), North Carolina Baptist Hospital (NCBH), all on-site subsidiaries as well as those off-site governed by WFBMC policies and procedures.
   b) **Research Records:** Information recorded for the purpose of a research study, regardless of form or the media on which it may be recorded. Research records include the Case Report Form, Regulatory Binder, Consent Form and Source Data.
   c) **Case Report Form (CRF)** – Document (printed or electronic) designed to record all of the protocol required information to be reported to the sponsor on each trial subject. (ICH GCP 1.11)
   d) **Informed Consent Forms (ICF)** – Documents that provide a description of the study and are signed by both the study participant and a member of the study team.
   e) **Regulatory Binder (or Files)** – Place where all study-specific information and regulatory documentation, including IRB approved protocols, amendments, informed consent, case report

forms, FDA 1571 and 1572 (if applicable) and recruitment materials, is maintained. The regulatory binder provides a thorough history of the research study from protocol development to study completion.

- **Source Data** – Information contained within source documents that represent the original documentation of findings and observations of subjects participating in clinical research studies (ICH GCP 1.51).
- **Source Documents** – Original documents, data and records such as medical records, laboratory results, x-rays, pharmacy records and subject diaries. (ICH GCP 1.52)
- **Completion of the Research** - the point at which the study application is closed with the IRB, not the completion of participant activity.

3) Procedure Guidelines:

General Requirements: The Principal Investigator is responsible and accountable for collecting, filing, storing, and properly disposing of all study-related documents for each research study as required by federal and state law and institutional policy. The PI may delegate the task of maintaining accurate and complete records to another qualified study team member, but s/he may not delegate accountability. Access to research records should be controlled to prevent unauthorized use, disclosure, removal or destruction of the records. Research records must be stored in a manner that ensures confidentiality, security and accessibility.

- Research records existing on paper or in portable electronic media must be stored in a locked room and/or a locked cabinet when not in use. Access to the records must be restricted to authorized staff only.
- For electronic records, proper storage, access controls, and transfer provisions must be utilized, including encryption and password protection in accordance with Medical Center Policies.
- Research data and records should be quickly accessible to authorized staff members when needed for regulatory review or other reasons consistent with WFBMC policies.

After the study is completed, records must continue to be stored in accordance with all WFBMC policies to assure the confidentiality of the research subjects and other proprietary information. Offsite storage of hard-copy information must occur at a secure facility that is contracted to WFBMC to meet regulatory standards for protected health information. When preparing the research records for storage, the study team must be able to easily identify the contents of each storage box in the event that individual research files need to be pulled for an auditor or for data query. Investigators should include the cost of long-term storage of study related-records in their budget. The contents of stored containers must be recorded by the department from which it originated since that department is ultimately responsible for the disposition of the stored information.

How Long Should Research Records be Kept?

The PI is responsible for following the study records retention guidelines as required by federal regulations, the study sponsor, and the institution. The requirements for the retention of research records may vary depending on the government agency/study sponsor. The tables below indicate the minimum retention requirements for consent forms and study data by agency. Note that the completion of the research is defined as the point at which the study application is closed with the IRB, not the completion of participant activity.

Retention of Consent Forms

Policy Maker	Retention Period

Office for Human Research Protections	Three years after the completion of the research [45CFR46.115(b)]
HIPAA	Authorizations or informed consent documents when the Authorization has been included (compounded) in the informed consent must be retained until six years after the later of the date of their creation or last effective date [45CFR164.530(j)]
Study Sponsor (e.g. industry sponsored contracts)	The study sponsor may specify in the research contract or protocol specific requirements on the storage, retention and disposition of research records in addition to the standard regulatory retention requirements.

Retention of Study Data

Policy Maker	Retention Period
Wake Forest School of Medicine	Five years from the date of the last publication or the date of the final report issued upon completion of the project, whichever is later.
Office for Human Research Protections	Three years after the completion of the research [45CFR46.115(b)]
Food and Drug Administration	Two years following the date a marketing application is approved for the drug for the indication for which it is being investigated or, if no application is to be filed or if the application is not approved for such indication, until 2 years after the investigation is discontinued and the FDA is notified [21CFR312.62(c)]
Study Sponsor (e.g. industry sponsored contracts)	The study sponsor may specify in the research contract or protocol specific requirements on the storage, retention and disposition of research records in addition to the standard regulatory retention requirements.

Once the required retention period has been met, the study team can either destroy the data and records according to the procedures required under WFBMC policy or ensure that data and records are de-identified or coded. De-identified means that ALL of the 18 HIPAA identifiers are removed from the data and link to identifiers is destroyed, thereby preventing the possibility of re-identification. Coded data means that only a linkage file, stored separately from the data, would associate the identities of individuals with the data.

Physical destruction of WFBMC Records (including on and offsite) shall be in accordance with Wake Forest Baptist Medical Center's Information Security Policy. IT Security can assist with "cleaning/sanitizing" electronic equipment that contains confidential information before it is redeployed. Special processes may be necessary to minimize the likelihood that data could be restored and accessed, so it is important to consult with IT Security to determine the type of data destruction procedure your equipment needs. If electronic equipment containing confidential information is broken or otherwise no longer useable it should be destroyed according to Medical Center requirements. An Equipment/Asset Disposal Form is available in the Financial Services - Asset Management Policy and Procedure Manual

to request the destruction of electronic devices that have reached the end of their useful life. The Financial Services - Asset Management Policy and Procedure Manual can be found on the Medical Center's Policy and Guidelines iShare site.

Destruction of paper records should be carried out using the confidential shred process in place at the Medical Center. Compact disks can also be placed individually in the confidential shred containers for destruction. If paper records are stored off-site at a facility contracted to WFBMC for the protection of confidential information, the facility may have destruction services that provide disposal of records eligible for destruction. The Privacy Office can provide guidance if there are any questions about the best way to destroy paper records.

4) Review/Revision/Implementation

a) Review Cycle: This SOP shall be reviewed by the Office of Regulatory Affairs and Research Integrity at least every three years from the effective date.

b) Office of Record: After authorization, the Legal Department shall house this SOP in a policy database and shall be the office of record for this SOP.

5) Related Policies

Policy on Quality Conduct of Clinical Research
Record Retention and Destruction Policy
Information Security
Access Control Policy
Anti-Virus Policy
Encryption Policy
Computer Equipment and Media Disposal and Reuse Policy
Access Control Policy
Password Security Policy
Privacy and Security Awareness Policy
Financial Services Asset Management Policy and Procedure Manual

6) Governing Law or Regulations

Title 45 Code of Federal Regulations Part 46
Title 21 Code of Federal Regulations Part 312
Title 45 Code of Federal Regulations Part 164

7) Attachments

None

8) Revision Dates

July 25, 2017