OFFICE FOR EDUCATION & QUALITY IN CLINICAL RESEARCH	CATEGORY	Clinical Research: Project Activities
	SUBJECT	Research Data Security and Storage
	SOP #	4.2
	EFFECTIVE DATE	August 6, 2008
	REVISION DATE	January 3, 2018

OBJECTIVE

Describe how to protect the confidentiality, integrity, and availability of research data. These procedures apply to all clinical research activities approved by the Office for Human Subjects Research conducted within the Hennepin County Medical Center campus.

APPLICABLE REGULATIONS AND GUIDELINES

45 CFR 46	Protection of Human Subjects
21 CFR 11	Electronic Records
21 CFR 312	Investigational New Drug Application
21 CFR 812	Investigational Device Exemptions

https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

REFERENCES TO RELATED SOPs

All SOPs are applicable to this SOP

ATTACHMENTS

HIPAA Identifier List

1) Printed data
   a) Keep records in a secure location such as a locked office or file drawer.
   b) Assure that only appropriate study personnel have access to records.
   c) Limit public access to areas containing research records.
   d) Original records should not be removed from the source location or from an approved research site.
   e) Do not leave records unattended.
   f) Do not bring records home.

2) Electronic data
   a) Keep computer resources including disks, CDs, flash drives and external hard drives in a secure location such as a locked office or storage area. Do not leave resources unattended.
   b) Do not bring electronic data home or store on a personally owned computer.
   c) Store study data on a designated institutional secure server.
   d) Position computer monitors to minimize viewing by others.

3) Face to face data collection
   a) Conduct interviews in a private location when possible so that subject information will not be overheard.
   b) Use video, audio, or supplementary media in a private location when possible so that subject information will not be overheard.
   c) Store all paper or electronic records from face to face data collection as outlined above.

4) De-identify subject treatment or diagnostic records before sending to sponsor.
   a) Remove or obscure all individual identifiers based on the HIPAA identifier list.
   b) Remove identifiers within a document body as well as the subject's name and medical record number.
   c) Ensure that identifiers cannot be discerned after obscuring.
   d) Ensure that all identifiers cannot be seen when source record copied or scanned (wax pencil suggested for redaction).

5) Long term record storage
   a) Store records so that a request to view records by a sponsor, regulatory agency, or internal auditor may be met promptly.
   b) Storage facilities should be secure with access limited to appropriate personnel.
   c) If records are stored in an off-site facility, ensure that the records are handled securely and that only authorized personnel has access to them.
   d) Notify the sponsor of any change in personnel responsible for stored records.
   e) Notify sponsor of any change in record storage location.

6) Record retention
   a) Retain all records used in the study as outlined in Federal or ICH regulations as appropriate.
   b) Check with Grant Administration to verify that the sponsor does not want records to be kept for a longer period.
   c) Check with the sponsor before destroying records.

7) Record destruction
   a) Shred paper documents with a mechanical (preferably crosscut) shredder or use a commercial shredding company to ensure that documents are destroyed so that information cannot be reconstructed.
   b) Physically destroy disks, CDs, or other transportable memory devices.
   c) Permanently delete files and data from internal and external hard drives using commercial scrubbing software or physically destroy hard drives.
   d) Permanently destroy video or audio tapes

HIPAA Identifier List

1. Names
2. Geographic subdivisions smaller than a state, includes county, city, street address, precinct, zip code, and equivalent geocodes (first three digits of a zip code excluded if the geographic unit formed by combining all zip codes with the same first three digits contains >20,000 persons)
3. All elements of dates (except year); all ages >89 and all elements of dates (including year) indicative of such age (may aggregate into a category of age >90)
4. Telephone numbers
5. Fax numbers
6. E-mail addresses
7. Social Security Numbers
8. Medical record numbers
9. Health–plan beneficiary numbers
10. Account numbers
11. Certificate and license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Medical device identifiers and serial numbers
14. Internet universal resource locators (URLs)
15. Internet protocol (IP) addresses
16. Biometric identifiers including finger and voice prints
17. Full-face photographic images or comparable images
18. Other unique identifying number or characteristic