SOP Number: GCP 05
SOP NAME: Maintaining Privacy and Confidentiality
Effective Date: 3-Mar-2016 (rev 14-Jun-2023)

1. POLICY

The purpose of the Standard Operating Procedure (SOP) is to describe the practices for managing Protected Health Information (PHI) collected for research purposes in accordance with regulations of the Health Insurance Portability and Accountability Act (HIPPA).

2. DEFINITIONS AND ABBREVIATIONS

CE	Covered Entity
CIRB	Central Institutional Review Board
CRF	Case Report Form
FDA	Food and Drug Administration
HIPPA	Health Insurance Portability and Accountability Act
IRB	Institutional Review Board
IP	Internet Protocol
NIH	National Institutes of Health
PHI	Protected Health Information
RCC	Regional Coordinating Center
SOP	Standard Operating Procedure
StrokeNet	NIH StrokeNet Network
URL	Uniform Resource Locator

Definitions:

Protected Health Information- Individually identifiable health information

HIPAA Security Rule- The rule that covers security standards for certain health information specifically focusing on safeguarding electronic PHI.

HIPAA Privacy Rule- The rule that defines the standards for how protected patient health information should be controlled.

Covered Entity- A health plan, a health care clearinghouse, or a health care provider that transmits any health information in electronic form in connection with a transaction covered by HIPAA.

3. SCOPE

This SOP applies to the management of any and all Protected Health Information (PHI) collected for research purposes in the NIH StrokeNet. The SOP applies to all investigators, staff, subcontractors or other entities associated with StrokeNet who manage, oversee, and conduct research within the network.

4. PROCEDURES

A. General Guidelines for Managing PHI

I. PHI includes any information about health status, health care provisions or payments for health care that can be linked to a specific individual. This includes any medical records or payment histories.

II. HIPAA regulations list 18 participant identifiers which are considered PHI

- Names
- Geographic Information
- Dates related to the individual (including birthdates) and exact age if 90 years or older
- Phone numbers
- Fax numbers
- Email addresses
- Social Security numbers
- Medical record numbers
- Health insurance beneficiary information
- Account numbers
- Certificate/License numbers
- Vehicle identifiers
- Device serial numbers or other identifiers
- Web Uniform Resource Locators (URL)
- Internet protocol (IP) address
- Biometric identifiers (fingerprint, retinal scan, etc.)
- Full face photographic images
- Unique identifying number, characteristic, or code

III. De-identification

Before submitting study-related data, PHI should be de-identified to remove all identifying information that could link data to a participant. This applies to imaging or specimen data in addition to electronic Case Report Form (CRF) data. Each participant can be assigned a code

or other record identifier provided that the code is not derived from or related to any of the identifying characteristics listed above and the identifying mechanism is only the minimum necessary for research purposes. Codes or record identifiers may be maintained in an electronic form depending on local institutional regulations. These codes should not be capable of being translated in any way to identify the participants, and the coding mechanism should not be disclosed to outside parties.

The only exception to any privacy rule is the requirement for a trial performance site to maintain a subject identification code list for all subjects enrolled in the trial in case follow-up is required. This list is to be kept in a secure and confidential manner while a trial is ongoing and for 15 years after (SOP GCP #12).

Regional Coordinating Centers (RCCs), satellite sites, and performance sites are responsible for identifying and maintaining compliance with their specific institutional practices regarding the management of PHI in additional to those outlined in this SOP.

Paper or electronic source data that may or may not contain PHI must be stored securely. Access to source data for review and inspection by covered entities must be assured over the trial-defined period of time. During review of source data by covered entities such as Food and Drug Administration (FDA) personnel, sponsor or network monitors, it is important to ensure adequate protection of the subject's privacy and confidentiality.

IV. Regulations for violations of PHI disclosure
Any unauthorized disclosure of PHI should be reported to the Central Institutional Review Board (CIRB) and any other locally required legal boards.

B. HIPAA Procedures

I. The HIPAA Privacy Rule and Security Rule:
These rules provide federally mandated protections over identifying health information, giving patients the right to their information. The Security Rule enforces standards on how PHI is created, received and used. These protections were put into place to ensure the confidentiality, integrity and availability of participant health information. Any research using identifiable personal medical records or involving information that could be potentially added to those regulations is subject to HIPAA privacy laws. The CIRB should be consulted if there is any doubt regarding whether or not research data is considered PHI.

II. HIPAA Security Rule regulations maintain that administrative, physical and technical safeguards are in place to protect the confidentiality and accessibility of PHI. This includes ensuring that protections are in place for PHI stored electronically, with processes for computer password protection, monitoring and back up of data. All log-in information should

be maintained for an institutionally regulated period, either on the server or thorough backups. Only authorized personnel should have access to electronically stored PHI. Additionally, all investigators or others who have access to PHI should undergo periodic training or re-training in information security as determined by institutional policy.

III. HIPAA Research Regulations:

A signed HIPAA authorization is required for all study participants consenting to research programs involving the collection of PHI. If HIPAA protections do not apply to a specific research study, a CIRB approved Waiver of Authorization may be attached to the project. According to HIPAA regulations, seven elements of research require additional explanation and consent for use of PHI. These elements include:

- the description of the information being collected
- name of the person(s) authorized to use this information
- name of the person(s) or organizations to whom PHI will be released
- expiration date of authorization to use PHI
- right to revoke authorization
- possible disclosures to any other non-protected organizations
- statement that the participant may inspect records after completion of study

Depending on the state where the research is conducted, a "stand-alone" HIPAA authorization may be required as an additional document separate from the informed consent. This stand-alone authorization language is not required to be reviewed by the CIRB. Some states may allow for a consent form combined with HIPAA authorization, and this language must be reviewed by the CIRB. Local IRBs should be consulted for further guidance on how to capture HIPAA authorizations according to local guidelines. The NIH StrokeNet CIRB will work with the institution's IRB to determine the requirements for HIPAA content at each performance site. Unless otherwise required, the standard CIRB consent format will be a combined consent and HIPAA authorization document. Performance sites or their RCC are responsible for identifying the specific institutional practice regarding HIPAA documentation.

C. State and Local Privacy Laws regarding the management of PHI collected for research purposes

The Privacy Rule establishes the minimum federal rule for protecting identifiable personal information. Federal laws override any state laws about the management of PHI that may be contradicting. However there may be state laws that mandate broader protections then what is covered by federal laws. Any state law provisions that are not contrary to the Privacy Rule must be followed in addition to federal regulations. In addition, any state law that is more stringent to the

Privacy Rule even if it is contrary should be followed. This may include required disclosures of death or injury for public health surveillance or investigation purposes. Local institutional legal departments and IRBs should be consulted to determine state laws that may be applicable to research involving PHI. If a local institution has additional privacy laws, the performance site is responsible for communicating that to the CIRB liaison during the protocol submission/review process.

5. APPLICABLE REGULATIONS AND GUIDELINES

ICH E6 (R1)-5.15

ICH E6 (R1)-6.12

Guidance for Industry Electronic Source Data in Clinical Investigations, Sep 2013

21 CFR 312.62 Investigator record keeping and record retention

21 CFR 11.10 Electronic Records; Electronic Signatures

Health Information Privacy, U.S. Department of Health & Human Services:
http://www.hhs.gov/ocr/privacy/

6. REFERENCES TO OTHER APPLICABLE SOPS

SOP GCP #1: Human Subjects Protection

SOP GCP #9: Site Performance Monitoring, Audits/Inspections

SOP GCP #12: Regulatory and Clinical Data; Maintenance and Data Storage

7. ATTACHMENTS AND REFERENCES

HIPAA Regulations: http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html

National Institutes of Health, Clinical Research and the HIPAA Privacy Rule:
http://privacyruleandresearch.nih.gov/clin_research.asp

National Institutes of Health, Privacy Rule Booklet:
http://privacyruleandresearch.nih.gov/pdf/HIPAA_Privacy_Rule_Booklet.pdf

Centers for Disease Control: HIPPA Privacy Rule:
http://www.cdc.gov/mmwr/preview/mmwrhtml/m2e411a1.htm

8. DOCUMENT HISTORY

Version	Description of Modification	Completion Date	Issue Date	Effective Date
0.1	Draft of GCP #5	22-Apr-2014		
0.2	Edits per NCC	1-May-2014		
1.0	Final	3-Mar-2016	3-Mar-2016	3-Mar-2016
2.0	Administrative review	28-Jun-2023	29-Jun-2023	29-Jun-2023