Study Management
PP – 501.00

STANDARD OPERATING PROCEDURE FOR
Safeguarding Protected Health Information

Approval: Nancy Paris, MS, FACHE
President and CEO

24 May 2017
(Signature and Date)

Approval: Frederick M. Schnell, MD, FACP
Chief Medical Officer

30 May 2017
(Signature and Date)

Issue Date: 01 June 2017

Effective Date: 01 June 2017

Expiration Date: 01 June 2019

Document Review Date: 01 March 2017

Reviewer: Joni N. Shortt, BSN, RN, CCRC

Primary Author: Anita Clavier, BSN, MPH

Previous Reviewer: Alice S. Kerber, MN, APRN

I. INTRODUCTION AND PURPOSE

This standard operating procedure (SOP) describes the steps taken to ensure that subject protected health information (PHI) is kept confidential and access to such information is limited to authorized Georgia CORE staff and consultants for approved purposes only. Access to confidential information should only be permitted for direct subject management, administrative oversight, or with Institutional Board approval. Maintaining high standards of conduct with respect for the privacy of individuals and the confidentiality of information is essential for all Georgia CORE personnel.

2. SCOPE

This SOP applies to all Georgia CORE staff and consultants to maintain high standards of conduct with respect for the privacy of individuals and the confidentiality of information both during the hours they are performing their professional and work-related activities and outside their work-related activities.

3. APPLICABLE REGULATIONS AND GUIDELINES

45 CFR Parts 160, 162, and 164, Federal Code of Regulations, 17 March 2017
Health Insurance Portability and Accountability Act of 1996 (HIPPA) Privacy and Security Rules

4. REFERENCES TO OTHER APPLICABLE SOPs

GA-102	Sponsor Responsibility and Delegation of Responsibility
GA-103	Training and Education
SM-301	Communication
SM-303	Documentation and Records Retention
DM-401	Data Management

5. ATTACHMENTS

A. Guidelines for Safeguarding Protected Health Information
B. Fax and E-mail Transmission Procedure
C. Fax Log

6. RESPONSIBILITY

This SOP applies to those members of Georgia CORE involved in overseeing clinical trials. This includes the following:

- President and CEO
- Chief Medical Officer
- Georgia CORE staff and consultants

7. DEFINITIONS AND GLOSSARY

Case Report Form (CRF): A printed, optical, or electronic document designed to record all of the protocol-required information to be reported to the sponsor on each trial subject

Confidentiality: Prevention of disclosure, to other than authorized individuals, of a sponsor's proprietary information or of a subject's identity.

Direct Access: Permission to examine, analyze, verify, and reproduce any records and reports that are important to evaluation of a clinical trial. Any party (e.g., domestic and foreign regulatory authorities, sponsors, monitors, and auditors) with direct access should take all reasonable precautions within the constraints of the applicable regulatory requirement(s) to maintain the confidentiality of subjects' identities and sponsor's proprietary information.

Health information: any information, whether oral or recorded in any form or medium, that:
(1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Individually identifiable health information: information that is a subset of health information, including demographic information collected from an individual, and:
(1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
(i) That identifies the individual; or
(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Protected Health Information: Information that is created or received by a health care provider, health plan, employer, or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and identifies the individual; or when there is a reasonable basis to believe the information can be used to identify the individual. (Under HIPAA regulations at 45 CFR 164, PHI (*Protected Health Information*) also includes: Individually identifiable health information that is: (i) Transmitted by electronic media; (ii) Maintained in any medium described in the definition of *electronic media* at §162.103, or (iii) Transmitted or maintained in any other form or medium.)

8. PROCESS OVERVIEW

A. Oral and phone communication
B. Computer access and security
C. Electronic communication
D. Documents and written communication
E. Transporting confidential documents

9. PROCEDURES

A. Oral and phone communication

• All Georgia CORE staff and consultants	Oral communications between Georgia CORE staff and consultants and investigators and research staff and other health care providers, whether in person or by phone, are essential to effectively manage subjects while on study. Attachment A, Guidelines for Safeguarding Protected Health Information (PHI). Ensure that discussions regarding the treatment of individuals take place in areas that are not public and where others cannot overhear confidential information and identifiers. Ensure that staff and employees do not discuss subjects in public areas, such as elevators, waiting rooms, cafeterias, and hallways. Names and unique descriptions of individuals should not be discussed except in areas where privacy is maintained, such as a private office or treatment room.
• Contracts and Regulatory Administrator	Confirm through monitoring that site staff is complying with the Guidelines for Safeguarding Protected Health Information, Attachment A. Follow-up with site staff as required.

B. Computer access and security

• President and CEO or Program Manager	Limit and control direct access to the PHI that resides on Georgia CORE's computer system. Locate workstations in areas of limited public access. Maintain access lists and password assignments.
• President and CEO or Program Manager	Determine access level prior to allowing individual access to PHI. Base these determinations on minimum necessary access. Instruct users regarding password assignment and use and logging on and off procedures.

C. Electronic communication

• President and CEO or Designee • All Georgia CORE Staff and Consultants	Ensure that each member of Georgia CORE's staff and consultants is aware of and adheres to requirements for safeguarding PHI via: *e-mail* – Do not transmit PHI unless individuals request such transmission in writing, or such information is protected via encryption software. *Fax* – Care shall be taken when documents containing PHI are transmitted via fax. (Attachment B, Fax and E-mail Transmission Procedure.) Maintain a fax log (Attachment C) when faxing PHI documents.

	Ensure that encryption procedures or other security software is installed and monitored regularly.
• Program Manager	*Intranet, internet* – Remind sites that PHI is to be transmitted on secure servers only.
• Contracts and Regulatory Administrator	Confirm through monitoring that site staff are following the Fax and e-mail transmission procedure (Attachment B) and maintaining a fax log regularly (Attachment C). Follow up with site staff as needed.

D. Documents and written communication

• All Georgia CORE staff and consultants	Ensure that IRB approved informed consents contain the research subject's consent to release patient specific information, including medical information to the Site, Georgia-CORE, Sponsor, FDA, and other regulatory entities. Handle all PHI in written form in a manner that respects the privacy of the individual and the confidentiality of information. Do not carry, transport, use, or share written information in a careless manner. Share case report forms, documents, test results, notes, and any other written information about a subject only with other staff members who have a need to see such information as part of their duties. Ensure that written information is not held in public areas, not taken off premises and not handled in a manner that allows unauthorized access.
• Designee	Ensure that IRB approved informed consents contain the research subject's consent to release patient specific information, including medical information to the Site, Georgia-CORE, Sponsor, FDA, and other regulatory entities. Confirm through monitoring that site staff handles all written PHI in a manner that respects the confidentiality of the information.

E. Transporting confidential documents

• All Georgia CORE staff and consultants	Transport confidential documents by authorized staff only, using secure methods. Remind individuals transporting confidential information of their responsibility for the security of such information until it arrives at another secure location.
• Contracts and Regulatory Administrator	Confirm through monitoring that site staff transports confidential documents appropriately.

10. HISTORY OF CHANGES

Version Number	Section Number	Modification	Approval Date
501.00	All	Original Version	
501.00	All	No change was necessary	09 March 2012
501.00	All	No change was necessary	01 June 2014
501.00	3	Update date of Federal Code of Regulations	17 March 2017

Attachment A

GUIDELINES FOR SAFEGUARDING PROTECTED HEALTH INFORMATION

Subject information is never discussed in public areas.

Conversations with the subject/family regarding confidential information are not held in public areas, particularly waiting rooms.

Phone conversations are held in areas where confidential information cannot be overheard.

Except for the subject's name, confidential information is not called out into the waiting room or discussed in transit to the examination room.

Lists, including scheduled procedures and appointment types and notes, with information beyond room assignments are not readily visible by others.

Records are filed in storage cabinets and rooms are locked.

Dictation is completed in an area where confidential information cannot be overheard.

At the front desk or examination rooms, documents with subject information are kept face down or concealed to avoid observation by patients or visitors. Only authorized site personnel have access to confidential information.

Paper records and medical charts are stored or filed to avoid observation by others.

External hardware containing ePHI is properly stored.

Physical access to fax machines and printers is limited to authorized personnel.

Confidential information is not left on an unattended printer, photocopier or fax machine, unless these devices are in a secure area.

Release of confidential information is done with a HIPAA compliant release by staff specifically authorized to do so.

Answering machines are turned down so information being left cannot be overhead by other staff or visitors.

Confidential information is discarded by shredding and/or placing in an appropriate confidential container.

Confidential information should remain in the medical/ research record. Original records should never be removed from the site.

Confidential information should not be copied or removed in any form from the site without appropriate approval.

Computer monitors are positioned away from common areas.

Computer monitors positioned away from common areas or privacy screens are utilized.

The screens on unattended computers are returned to a logon screen. IDs and passwords are never shared.

Subjects are appropriately escorted to ensure they do not access staff areas, chart storage etc.

Restricted areas are clearly identified.

Consultation and exam room doors are closed during subject examination and/or counseling.

Confidential documents are transported by authorized staff only, using secure methods.

Individuals transporting confidential information are reminded of their responsibility for the security of such information until it arrives at another secure location.

Share case report forms, documents, test results, notes, and any other written information about a subject only with other staff members who have a need to see such information as part of their duties.

Ensure that written information is not held in public areas, not taken off premises and not handled in a manner that allows unauthorized access.

e-mail – Do not transmit PHI unless individuals request such transmission in writing, or such information is protected via encryption software.

Fax – Care shall be taken when documents containing PHI are transmitted via fax.

Attachment B

FACSIMILE AND E-MAIL TRANSMISSION PROCEDURES

General Policies

Only fax machines in non-public areas are to be used to send and receive faxes that contain PHI; OR

Only fax machines in areas that require security keys, badges, or similar mechanisms in order to gain access shall be used to send and receive PHI.

Double check the recipient's fax number before transmittal and confirm delivery via telephone or review of the appropriate confirmation of fax transmittal.

Designated staff shall check fax machines a minimum of every 4 hours for faxes that contain PHI. Documents found shall be immediately secured in the appropriate location or given to the designated recipient.

Fax machines should be pre-programmed to destination numbers whenever possible to eliminate errors in transmission from misdialing.

Fax and e-mail senders of individually identifiable health information should routinely check and re-check fax numbers and e-mail addresses of recipients before transmission.

Destination numbers and e-mail addresses should be checked and confirmed at least quarterly. Frequent recipients of individually identifiable health information should be encouraged to notify you if their fax number or e-mail address is to change.

Each user is to complete an entry in the Fax log for every item sent (this may be revised if the fax machine is able to provide fax transmittal summaries and confirmation sheets). The logs shall be reviewed periodically for unauthorized access or use by President and CEO or Designee.

Mitigation

The fax cover sheet and e-mail transmissions must have a confidentiality statement at the bottom:

> The documents accompanying this transmission contain confidential health information that is legally privileged. This information is intended only for the use of the individual or entity named above. The authorized recipient of this information is prohibited from disclosing this information to any other party unless required to do so by law or regulation and is required to destroy the information after its stated need has been fulfilled.
>
> If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution, or action taken in reliance on the contents of these documents is strictly prohibited. If you have received this information in error, please notify the sender immediately and arrange for the return or destruction of these documents.

If the sender becomes aware that a fax or e-mail was misdirected, contact the receiver and ask that the material be returned or destroyed.

Attachment C

FAX LOG

Item sent	Sender initials	Date	Time	To	Fax #	Receipt confirmed	
						Yes	No