

## **Study Management PP – 501.01**

### **STANDARD OPERATING PROCEDURE Safeguarding Protected Health Information**

**Approval: Lynn M. Durham, Ed.D.**

**President and CEO**

**04 Feb 2021**

**(Signature and Date)**

**Approval: Frederick M. Schnell, MD, FACP**

**Chief Medical Officer**

**04 Feb 2021**

**(Signature and Date)**

<b>Issue Date:</b>	01 June 2017
<b>Effective Date:</b>	01 September 2020
<b>Expiration Date:</b>	01 September 2022
<b>Document Review Date:</b>	30 June 2020
<b>Reviewer:</b>	Jane Clark, PhD, RN, AOCN, OCN (2020)
<b>Previous Reviewers:</b>	Joni Shortt, BSN, RN, CCRC (2017) Alice Kerber, MN, APRN (2014)
<b>Primary Author:</b>	Anita Clavier, BSN, MPH (2013)

#### **1. INTRODUCTION AND PURPOSE**

Communication between Georgia CORE staff and consultants and Research Network Investigators and staff, other health care providers, and regulatory authorities is essential to effectively manage subjects while on study. Georgia CORE is responsible for ensuring that Research Network site Investigators and staff keep study subject personal health information (PHI) confidential and that access to the subject PHI is limited to authorized Georgia CORE staff and consultants and FDA and Sponsor representatives for approved purposes. Access to confidential information should only be permitted for direct subject management, oversight, or with Institutional Review Board approval. Maintaining high

standards of conduct with respect for the privacy and confidentiality of PHI is essential in the conduct of clinical trials.

The purpose of this SOP is to describe the processes to be used by all Georgia CORE staff and consultants to ensure the privacy and confidentiality of personal health information for all subjects enrolled in clinical trials are maintained.

## **2. SCOPE**

This SOP applies to all Georgia CORE staff and consultants both who monitor clinical trials and interact with Georgia CORE Research Network site personnel and regulatory authorities during the hours they are performing their professional and work-related activities and outside their work-related activities.

## **3. APPLICABLE REGULATIONS AND GUIDELINES**

The Code of Federal Regulations and the International Conference on Harmonization, Good Clinical Practice: Consolidated Guideline and selected program and guidance documents apply to this SOP (Appendix A).

## **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. Facsimile and E-mail Transmission Procedures
- C. Facsimile Log

## **6. RESPONSIBILITY**

This SOP applies to those employees of Georgia CORE and members of the Georgia CORE Research Network sites involved in the oversight of the conduct of clinical trials.

- President and CEO
- Chief Medical Officer
- Georgia CORE staff and consultants
- Research Network site Investigator, Subinvestigators, and staff

## **7. DEFINITIONS**

The following definitions apply to this SOP (Appendix B):  
Case Report Form (CRF)

Confidentiality  
Direct Access  
Health Information  
Individually Identifiable Health Information  
Protected Health Information

## 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**

Georgia CORE President and CEO	Ensure that all Georgia CORE staff and consultants are made aware of the guidelines for safeguarding protected health information (PHI).
Georgia CORE staff and consultants	<p>Ensure that Research Network Investigators, Subinvestigators, and staff are made aware of guidelines for safeguarding protected health information (PHI).</p> <p>Ensure that discussions regarding the identity and unique descriptions and treatment of study subjects do not take place in areas that are public, e.g., elevators, waiting rooms, cafeteria, and hallways and where others can overhear confidential information and identities.</p> <p>Oral communications related to study subjects should occur only in areas where privacy and confidentiality can be maintained, e.g., a private office or treatment room.</p> <p>Confirm through monitoring that Research Network site Investigators and staff are complying with the Guidelines for Safeguarding Protected Health Information. (Attachment A). Follow-up related to non-compliance is required.</p>

### B. **Computer Access and Security**

President and CEO	<p>Limit and control direct access in the PHI that results on the Georgia CORE computer systems.</p> <p>Locate workstations in areas of limited public access.</p> <p>Maintain access lists and password assignments.</p>
-------------------	---

Determine access level prior to allowing individual's access to PHI. Base these determinations on minimum necessary access.

Instruct users regarding password assignment and use and logging on and off procedures for the Georgia CORE computer system.

## **C. Electronic Communication**

President and CEO      Ensure that each member of Georgia CORE staff and consultants is aware of and complies to the requirements for safeguarding PHI by:

- E-mail: Do not transmit PHI unless individuals request such transmission in writing, or such information is protected by encryption software.
- Facsimile: Care shall be taken when documents containing PHI are transmitted by facsimile. (Attachment B: Facsimile and E-mail Transmission Procedures.)

Maintain a Facsimile Log (Attachment C) when faxing PHI documents.

Ensure that encryption procedures or other security software is installed and monitored regularly.

- Intranet/ Internet: Remind Research Network sites that PHI is to be transmitted on secure internet servers only.

Confirm through monitoring that the Research Network site Investigators and staff are following the facsimile and e-mail transmission (Attachment B) and maintain a facsimile log (Attachment C). Follow-up with site staff as needed.

## **D. Documents and Written Communications**

Georgia CORE staff and consultants      Ensure that IRB approved informed consents contain the consent of the research subject to release patient-specific information, including medical information to the Research Network site, Georgia CORE, Sponsor, FDA, and other regulatory entities.

All      Handle all PHI in written form in a manner that respects the privacy of the individual and the confidentiality of information.

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. Transporting Confidential Documents**

Georgia CORE staff and consultants Transport confidential documents by authorized staff only, using secure methods.

Remind Research Network site Investigators, Subinvestigators, and staff transporting confidential information of their responsibility for the security of such information until it arrives at another secure location.

Confirm through monitoring that authorized Research Network site staff are transporting confidential documents appropriately.

### **10. History of Changes**

<b>Version Number</b>	<b>Section Number</b>	<b>Modification</b>	<b>Approval Date</b>
501.00	All	Original Version	
501.00	All	No change necessary	09 March 2012
501.00	All	No change necessary	01 June 2014
501.00	All	Update date of Federal Code of Regulations	17 March 2017
501.01	All	Edited for clarity and logical consistency, update of links and Federal Code of Regulations	30 June 2020

**ATTACHMENT A:**  
**Guidelines for Safeguarding Protected Health Information**

1. Subject information is never discussed in public areas.
2. Conversations with the subject/family regarding confidential information are not held in public areas, particularly waiting rooms.
3. Phone conversations are held in areas where confidential information cannot be overheard.
4. Except for the subject's name, confidential information is not called out into the waiting room or discussed in transit to the examination room.
5. Lists, including scheduled procedures and appointment types and notes, with information beyond room assignments are not readily visible by others.
6. Records are filed in storage cabinets and rooms are locked.
7. Dictation is completed in an area where confidential information cannot be overheard.
8. 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.
9. Paper records and medical charts are stored or filed to avoid observation by others.
10. External hardware containing ePHI is properly stored.
11. Physical access to fax machines and printers is limited to authorized personnel.
12. Confidential information is not left on an unattended printer, photocopier or fax machine, unless these devices are in a secure area.
13. Release of confidential information is done with a HIPAA compliant release by staff specifically authorized to do so.
14. Answering machines are turned down so information being left cannot be overheard by other staff or visitors.
15. Confidential information is discarded by shredding and/or placing in an appropriate confidential container.

16. Confidential information should remain in the medical/ research record. Original records should never be removed from the site.
17. Confidential information should not be copied or removed in any form from the site without appropriate approval.
18. Computer monitors are positioned away from common areas.
19. Computer monitors positioned away from common areas or privacy screens are utilized.
20. The screens on unattended computers are returned to a logon screen. IDs and passwords are never shared.
21. Subjects are appropriately escorted to ensure they do not access staff areas, chart storage etc.
  
22. Restricted areas are clearly identified.
23. Consultation and exam room doors are closed during subject examination and/or counseling.
24. Confidential documents are transported by authorized staff only, using secure methods.
25. Individuals transporting confidential information are reminded of their responsibility for the security of such information until it arrives at another secure location.
26. 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.
27. Ensure that written information is not held in public areas, not taken off premises and not handled in a manner that allows unauthorized access.
28. *E-mail* – Do not transmit PHI unless individuals request such transmission in writing, or such information is protected via encryption software.
29. *Facsimile* – Care shall be taken when documents containing PHI are transmitted via facsimile.

## **ATTACHMENT B:**

### **Facsimile and E-mail Transmission Procedures**

#### **General Policies**

1. Only fax machines in non-public areas are to be used to send and receive faxes that contain PHI; OR
2. 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.
3. Double check the recipient's fax number before transmittal and confirm delivery via telephone or review of the appropriate confirmation of fax transmittal.
4. 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.
5. Fax machines should be pre-programmed to destination numbers whenever possible to eliminate errors in transmission from misdialing.
6. 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.
7. 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.
8. 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 the Georgia CORE President and CEO or Designee.

#### **Mitigation**

9. The facsimile cover sheet and e-mail transmissions must have a confidentiality statement at the bottom of the transmittal cover.
10. 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.
11. 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.
12. If the sender becomes aware that a facsimile or e-mail was misdirected, contact the receiver and ask that the material be returned or destroyed.



[illegible]