PP-701 STANDARD OPERATING PROCEDURE FOR SAFEGUARDING PERSONAL HEALTH INFORMATION

I. INTRODUCTION AND PURPOSE

This standard operating procedure (SOP) describes the steps taken to ensure that subject personal health information (PHI) is kept confidential and access to such information is limited to authorized research staff 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 personnel involved with the conduct of clinical research.

2. SCOPE

This SOP applies to all staff, employees, students, consultants, monitors and others at this research site 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

None

4. REFERENCES TO OTHER APPLICABLE SOP'S

GA-102	Responsibilities of the Research Team
GA-103	Training and Education
PM-301	Site-Sponsor/CRO Communications
PM-303	Regulatory Files and Subject Records
DM-501	Data Management

5. ATTACHMENTS

A. Guidelines for Safeguarding Personal Health Information

6. RESPONSIBILITY

This SOP applies to those members of the clinical research team involved in conducting or overseeing clinical trials at this research site. This includes the following:

- Principal investigator

- Sub-investigator
- Research coordinator
- Monitor
- Support staff

7. DEFINITIONS

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.

Personal 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 of confidential information

9. PROCEDURES

A. ORAL AND PHONE COMMUNICATION

RESPONSIBILITY	DESCRIPTION OF PROCEDURE
All research team members	Oral communications between 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 Personal Health Information.)

	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.
PI Research coordinator Support staff	When a PI/research coordinator talks with a subject in a semi-private area, such as a hospital or clinic room, emergency room, or other areas where absolute privacy cannot occur, conversations should take place behind curtains, or in a partitioned area. When it is impossible to ensure absolute privacy, staff and employees must make every effort to remove themselves from the area, when possible, and to keep anything over heard confidential. Ensure that PHI is not discussed on a cell phone except in an emergency. If subjects' PHI must be discussed via cell phone, it will be done in a private area (parked car, office, etc.).

B. COMPUTER ACCESS AND SECURITY

RESPONSIBILITY	DESCRIPTION OF PROCEDURE
PI Research Director/Manager	Limit and control direct access to the PHI that resides on the site's computer system(s). Locate workstations in areas of limited public access, except when necessary to provide care. Maintain access lists and password assignments.
Research coordinator	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

RESPONSIBILITY	DESCRIPTION OF PROCEDURE
PI Research coordinator	Ensure that each member of the research team 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. Make copies whenever e-mail that includes PHI is sent.

	Fax – Care shall be taken when documents containing PHI are transmitted via fax.
Research coordinator Support staff	Intranet, internet – Transmit PHI on secure servers only. Install and monitor encryption procedures or other security software and update regularly.

D. DOCUMENTS AND WRITTEN COMMUNICATION

RESPONSIBILITY	DESCRIPTION OF PROCEDURE
PI Research coordinator	Handle all PHI in written form in a manner that respects the privacy of the individual and the confidentiality of information. Ensure that staff 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.

E. TRANSPORTING OF CONFIDENTIAL DATA

RESPONSIBILITY	DESCRIPTION OF PROCEDURE
PI Research coordinator	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.

Attachment A

Guidelines for Safeguarding Personal Health Information

- Subject information is never discussed in public areas.
- Conversations with the subject/family regarding confidential information is 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 personal have access to confidential information.
- Paper records and medical charts are stored or filed to avoid observation by others.
- 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 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 placing in an appropriate 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.
- The screens on unattended computers are returned to a logon screen. IDs and passwords are never shared.

Subjects are appropriately es