UNIVERSITY OF SOUTH ALABAMA

CT-103 PROTECTING CONFIDENTIAL INFORMATION

EFFECTIVE DATE: May 2023

Purpose

This Standard Operating Procedure supports the USA HIPAA Privacy and Security Compliance For Research and other USA privacy policies, as well as the fully executed Clinical Trial Agreement. This SOP provides a mechanism by which a sponsor's proprietary information, data, and a subject's personal information are protected from disclosure to anyone other than authorized individuals.

Scope

This procedure pertains to any confidential information that is a part of a research study operated through the USA Clinical Trial Office. Confidential information includes but is not limited to protocols, investigator brochures, case report forms, research data, and identifiable personal health information. It is meant to supplement, not replace, other University of South Alabama's policies and procedures involving Protected Health Information (PHI) and/or protecting confidential information.

Definitions

Business Associate Agreement (BAA): Establishes a legally-binding relationship between HIPAA-covered entities and business associates to ensure complete protection of PHI.

Confidential Disclosure Agreement (CDA): A legal contract through which the parties involved in executing the agreement are obligated not to disclose any proprietary information covered under the CDA. A CDA outlines the scope of the confidential information the parties wish to share with each other for specified purposes. A CDA is also known as a nondisclosure agreement (NDA), confidentiality agreement or secrecy agreement.

Confidential Information: Any and all protected health information and proprietary information.

Clinical Trial Agreement (CTA): A clinical trial agreement (CTA) or clinical study agreement (CSA) is a legally binding agreement that governs the conduct of a particular study and sets forth the obligations of each party to the agreement.

Covered Entity: Any health care plan, provider, or service that transmits health care information in an electronic form and is thereby governed by laws and regulations in the handling of such data.

Proprietary Information: Material and information relating to or associated with a company's products, business, or activities, including but not limited to financial information, data or statements, trade secrets, product research and development, existing and future product designs and performance specifications. Examples include protocols, investigator's brochure, instruction for use, etc.

Protected Health Information (PHI): Individually identifiable health information, held or maintained by a covered entity or its business associates acting for the covered entity, that is transmitted or maintained in any form or medium. This includes identifiable demographic and other information relating to the past, present, or future physical or mental health or condition of an individual, or the provision or payment of health care to an individual that is created or received by a health care provider, health plan, employer, or health care clearinghouse. For purposes of the Privacy Rule, genetic information is considered to be health information.

Policy

The investigator and study staff are responsible for ensuring the protection of confidential information for all study participants and study documents. All study-related information should be shared on a need to know basis. Studies performed between institutions or through an outside sponsor must have a Confidential Disclosure Agreement (CDA) in place prior to sharing any proprietary information. A Clinical Trial Agreement (CTA) or Business Associates Agreement (BAA) must be in place before any PHI is released from the University of South Alabama.

Procedures

The following procedures outline activities research personnel must follow to stay in compliance with this policy.

1. Keep confidential information in a secure area that is locked when not in use. Computers should be locked when not in use. Computers and software systems should be secured with unique, confidential passwords. Passwords should not be shared.

2. All monitors, auditors, Clinical Research Associate, etc. who are not USA personnel should sign the Confidentiality Agreement for Monitors/Auditors if they will be reviewing or otherwise have access to electronic Protected Health Information. This confidentiality agreement does not need to be signed by a USA Signature Authority.

3. Limit discussions concerning confidential information to areas directly related to the conduct of research and necessary to complete the activity at hand. Such discussions should not be done in a public area such as elevators, waiting rooms, cafeterias, hallways, etc.

4. Confidential information should only be shared or accessed by research staff or ancillary staff that "need to know" such information to do their jobs.

5. Principal Investigator (PI) under a Covered Entity may use or disclose Protected Health Information (PHI) for research purposes when a research subject agrees to the use or disclosure of his or her information. This agreement is documented by signing an authorization that satisfies the HIPAA security and privacy requirements of 45 CFR 164.508.

6. To use PHI without authorization by the research subject one of the following criteria must be met:

   6.1. The PI must obtain an alteration or waiver of Authorization by the Institutional Review Board (IRB). IRB may determine a Waiver of Authorization is appropriate when direct permission from the research participant is either not necessary or not possible, and, as documented by an investigator on a Waiver of Authorization document, the use or disclosure of PHI involves no more than a minimal risk to the research participant's privacy. Clinical research will generally not qualify for a waiver if the research participant will be asked to sign an informed consent form.

   6.2. PHI may be reviewed preparatory to research when use of the PHI is solely to prepare a research protocol or similar activities preparatory to research such as determining the feasibility of a study. No PHI can be recorded or removed from the Covered Entity.

   6.3. An Authorization is not required for research that involves only the PHI of decedents. Records/specimens of deceased individuals that contain PHI will be examined and will adhere to all the following: The research requires the review of PHI solely for research on deceased individuals; The access sought to PHI is necessary for research purposes; If requested, documentation of the death of the individual(s) whose protected health information that will be accessed will be provided.

7. All PHI must be redacted when being electronically transmitted to a sponsor or a sponsor designee.

8. Any equipment/device used for clinical trials that store electronic PHI must be approved by the USA HIPAA compliance office prior to use.

   8.1. All equipment that electronically stores PHI must include an approved safeguard, such as encryption software.

   8.2. A Manufacturer Disclosure Statement for Medical Device Security form must be completed for such equipment.

9. PHI may be sent without redaction to appropriate people using an encryption program. Communication of PHI by text is strictly prohibited by hospital policy.

10. The HIPAA Privacy Rule gives subjects the right to receive an account of any or all disclosures of their PHI made by the Covered Entity.

    10.1. Covered Entities and Business Associates that are listed in the research ICF are exempt from the above requirement.

11. Data that is collected for the sole purpose of the sponsored research is property of the sponsor unless otherwise stated in the Clinical Trial Agreement. This data is subject to confidentiality measures outlined in this SOP.

12. All confidential information must stay on a University of South Alabama property. Transporting or storing of confidential information at an unapproved site or on an unapproved device is a breach of confidentiality.

13. Any breach of confidentiality involving PHI should be reported to HIPAA Compliance Office, the PI, the Office of Research Compliance and Assurance (ORCA), the IRB, and the sponsor (if appropriate). The below referenced policies for breach reporting must be followed.

14. Any breach of confidentiality involving sponsor proprietary information should be reported to the PI, Office of Research Compliance and Assurance, Director of Clinical Trials Office, and sponsor (if appropriate).

Additional Resources

RELATED DOCUMENTS

- **CONFIDENTIALITY AGREEMENT FOR RESEARCH MONITORS/AUDITORS**
- **WAIVER OF SUBJECT AUTHORIZATION**
- **LIMITED DATA USE AGREEMENT**

RELATED POLICIES:

- HIPAA Privacy and Security Compliance for Research
- Office of Research Compliance HIPAA Privacy Policies and Procedures
- USA Privacy Compliance Plan for Research
- USA Policy on Research Data Security
- USA Health HIPAA Breach Notification Policy (found in PolicyStat)

History

N/A

Next Review Date

January 2026

Responsible Party

Director, Clinical Trials Office