UNIVERSITY OF SOUTH ALABAMA

IRB SOP 704
HIPAA Authorization and Security

Purpose

These are the procedures by which the Office of Research Compliance and USA Institutional Review Board (USA IRB) fulfill their obligations with respect to the federal Health Insurance Portability and Accountability Act (HIPAA). See HIPAA in Research Compliance Plan for descriptive HIPAA privacy and security policies related to University of South Alabama's human subject's research activities.

Scope

This Standard Operating Procedure (SOP) applies to all human subjects' research under USA HIPAA Covered Entity that involves the collection, use, and disclosure of protected health information.

Applicability

The HIPAA Privacy Rule only applies if investigators use, receive and/or disclose protected health Information (PHI) from a covered entity in the course of conducting research with human participants or human participant data.

Definitions

Authorization: An individual's signed permission to allow a covered entity to use or disclose the individual's protected health information (PHI) that is described in the Authorization for the purpose(s) and to the recipient(s) stated in the Authorization.

Covered Entity: A covered entity is a health plan, a health care clearinghouse, or a health care provider transmitting health information, and is, therefore, subject to the HIPAA regulations.

Disclose/Disclosure: The release or transfer of information to, or the provision of access to information by, a person or entity outside of the entity holding the information.

Informed consent: The process by which individuals are given information necessary to decide whether or not to participate in a research study and provided the opportunity to voluntarily agree to such participation without coercion or undue influence.

Limited Data Set: Protected health information from which direct identifiers have been removed that may be used and disclosed for research purposes pursuant to a data use agreement.

Privacy Rule: Standards for Privacy of Individually Identifiable Health Information, promulgated by the U.S. Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and codified at part 160 and part 164, subpart E, of Title 45 of the U.S. CFR (as amended from time to time).

Protected Health Information (PHI): Information transmitted or maintained in any form (i.e., by electronic means, on paper, or through oral communication) that: (1) 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 health care; and (2) identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Security Rule: Adopted to implement provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). It sets forth specific requirements for the adoption of administrative, physical, and technical safeguards for the protection of electronic protected health information.

Policy

HIPAA stands for the "Health Insurance Portability & Accountability Act of 1996" (Public Law 104-191). The Rule specifies the actions required to protect the security and privacy of personally identifiable health care information and establishes the conditions for its use and disclosure. In the course of conducting research, researchers may obtain, create, use, and/or disclose individually identifiable health information. Under the Privacy Rule, covered entities are permitted to use and disclose protected health information (PHI) for research provided an individual gives written authorization to use or disclose PHI unless such authorization is waived or excepted by an IRBs or Privacy Board. The use of decedent's information is protected by the Rule but authorization is not required.

USA's activities include both HIPAA covered and non-covered functions; the University is considered a "hybrid" HIPAA entity covering the USA Health System (i.e., USA Hospitals, USA Physician's Group, Physical Therapy, Occupational Therapy, Speech Pathology and Audiology, Psychology Clinic, Mitchell Cancer Institute, Center for Strategic Health

Innovations and Center for Healthy Communities). Investigators who are not employed or are involved with research falling under the jurisdiction of the University's hybrid entity are not covered by HIPAA; therefore, HIPAA regulations do not apply. However, confidentiality of data collected must be maintained.

The IRB/Privacy Board protects and safeguards PHI created, acquired, and maintained during the conduct of human participant research in accordance with the privacy regulations promulgated pursuant to the HIPAA Privacy Rule, applicable state laws, and the University HIPAA privacy policies.

Under HIPAA, a covered entity must establish a privacy board or delegate authority to the IRB to serve as a privacy board to review uses and disclosures of PHI in research. The University has designated the IRB to serve as the privacy board for research.

1.0 HIPAA Determinations

The USA IRB shall make the following determinations:

1.1 The written Authorization documents permission from the research participants for the University to collect, use, and disclose their PHI.

1.2 The USA 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.

1.3 An Authorization is not required for research that involves only the PHI of decedents, as documented by an investigator on form entitled *Research Involving Deceased Individuals*.

1.4 An Authorization is not required for research that involves health information that is non-identifiable to a participant

1.5 When a research project involves health information that is identifiable only by certain identifiers specified under HIPAA, the data is considered a limited data set. If the investigator plans to release the limited data set to another covered entity, a written agreement (Data Use Agreement) must be utilized.

1.6 When the investigator is reviewing PHI preparatory to research, such as to prepare a research protocol, the investigator must submit verification to the USA IRB of such activity on form entitled *Investigator's Access Preparatory to Research*. PHI may not be removed from the custodian of the PHI for such activity.

Procedures

The IRB Office conducts a preliminary review of all new research, continuing review, or modification submissions to determine that those studies involving the collection of PHI or electronic PHI include the appropriate HIPAA documentation.

1.0 The IRB Office or the convened IRB reviews the collection, use, and/or disclosure of PHI for each submission to determine if an Authorization, waiver, Data Use Agreement, or other HIPAA privacy form is needed.

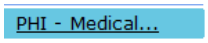
2.0 The IRB Office correspondences with the research team to request an alternate or additional HIPAA form if indicated upon preliminary review or at a convened meeting of the IRB.

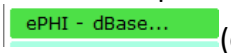
3.0 The IRB Office directs HIPAA research-related issues requiring additional guidance to the Office of Research Compliance and Assurance, who confers with the University HIPAA Privacy Officer.

4.0 The University HIPAA Compliance Office documents any indicated instructions or revisions and returns to the IRB Office. The Office of Research Compliance and Assurance and the IRB Office serves as a liaison between members of the IRB and the University Privacy Officer.

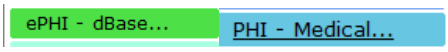
5.0 Projects determined by the IRB to be non-research, but which require review regarding Privacy issues, shall be forwarded to the University HIPAA Compliance Office for a determination. These projects do not generally require further involvement by the IRB.

1.0 Review of medical records and ePHI

Designation is made in IRBNet for projects involving retrospective chart review and tagged 

(PHI – Medical Records) and / or projects involving electronic personal health information, which includes the development and completion of the Research Database Registration Form which will be tagged 

(ePHI – dBase)

These two designations / tags 

are shared with the USA HIPAA Office. An automated email is generated and routed through IRBNet as a notification that reviewer access has been granted.

2.0 HIPAA Authorization and Informed Consent

The authorization document must include all elements defined in the HIPAA regulations as described in the USA HIPAA in Research Compliance Plan. The full compliance plan is available on the Office of Research Compliance and Assurance website at:
https://www.southalabama.edu/departments/research/compliance/humansubjects/regulations.html

Researchers must generally obtain authorization for the use of PHI from the human subjects whose PHI will be included in the study. The HIPAA authorization is incorporated into the informed consent within the confidentiality section. The USA IRB provides an authorization template that complies with HIPAA requirements. The researcher must customize the authorization template for the specific study he/she intends to perform. The USA IRB approved HIPAA Authorization template is located in the USA Local Context Language.

The following differences in procedures for signing an authorization are outlined below:

Adults: A competent individual 18 years of age and older, should always sign the authorization to use or disclose his/her PHI. (the general ability to understand the concept of releasing his/her medical information).

Minors: Any parent or legal guardian may sign an authorization for a minor child in his/her legal custody. HIPAA does not require that an assent document specifically for research participation include any version of a HIPAA authorization.

3.0 HIPAA Security/ Use of ePHI

The IRB application collects information on the maintenance of electronic identifiable health information (ePHI) for each individual study. If ePHI is maintained, a separate application "*Research Registration for Utilization and Storage of ePHI for Research Only*" must be submitted by the study site for IRB review and approval. This form provides minimum standards and instructions for utilization and storage of ePHI and located in IRBNet forms and templates. There are several key components that are evaluated during the review process to include the following, 1) workstation use for sending, receiving, storing, or accessing e-PHI information; 2) workstation security; 3) transmission security and implementing measures to protect the security of ePHI when transmitted electronically from one point to another; 4) data disposition; 5) information system(s) the data will be obtained; and 6) applications(s) used for the storage of data.

The University of South Alabama has the appropriate contractual protections for storing ePHI in Google's GSuite applications. The IRB Office is responsible for creating and

assigning a secure folder in Google GSuite. The IRB approval letter outlines the terms for compliance and access to the secured assigned folder. Additionally, periodic monitoring to ensure compliance with access and storage of ePHI will be performed by USA HIPAA Compliance Office, in conjunction with the Office of Research Compliance and Assurance. If a determination of non-compliance is made, the IRB may sanction suspension of project approval.

4.0 HIPAA-related Noncompliance or Breaches

The Office of Research Compliance and the IRB follows the procedures described in the USA HIPAA Privacy and Security Compliance Plan when information is received that suggests noncompliance, or inappropriate or unauthorized access, involving research and PHI.

Regulated Documentation

45 CFR 160,162, and 164

University Related Documents

HIPAA in Research Compliance Plan
HIPAA Waiver of Subject Authorization
USA HIPAA in Research Training

References

USA Office of Research Compliance: HIPAA website
Department of Health and Human Services, Office of Civil Rights

HISTORY

Effective Date: April, 2003
Revisions: February, 2018, June 2021

Responsible Party:

Office of Research Compliance and Assurance