HIPAA Privacy & Security Compliance for Research

Office of Research Compliance and Assurance
AD 240

Effective: April, 2003
Updated: October, 2022

HIPAA PRIVACY & SECURITY COMPLIANCE PLAN FOR RESEARCH

TABLE OF CONTENTS

I. INTRODUCTION TO HIPAA

A. Adoption of the HIPAA Privacy Compliance Plan

The University of South Alabama is committed to complying with all local, state and federal laws relating to the privacy of health information and to consistently operate with the highest standards of business and professional ethics. In that regard, we have implemented this HIPAA Privacy Compliance Plan for Research to safeguard the confidentiality and privacy of protected health information ("PHI") as required by the Federal Standards for Privacy and Individually Identifiable Health Information at 45 CFRParts 160 and 164, subparts A and E, as may be amended and applicable state privacy laws.

The compliance date for health care facilities and providers is April 14, 2003. The regulations are commonly referred to as the "Privacy Rule" and are administered by the HHS Office of Civil Rights. The University of South Alabama as a whole is a "Hybrid Entity" which consists of a single entity whose business includes covered and non-covered functions. The Covered Entities within the Hybrid Entity, along with the USA Health Services Foundation, are part of the USA Health System OrganizedHealth Care Arrangement (OHCA). This means that within the OHCA different areas need to share protected health information about their patients, and that individuals who obtain services here expect that different areas share health information and are jointly managed.

Updates to HIPAA, known as the Health Information Technology for Economical and Clinical Health Act (HITECH), went into effect in March 2013. The HITECH Act includes a number of measures designed to broaden the scope and increase rigor of HIPAA compliance. The Act specifically requires that patients be notified in the event of a breach of privacy or security, and establishes penalties for non-compliance.

By virtue of implementing and enforcing this Plan, we are committed to ensuring that PHI is collected, handled, transmitted and stored in a manner which preserves its confidentiality and privacy in accordance with the Privacy and Security Rules. This guidance document serves as a primer that will focus only on HIPAA health data privacy regulations as they pertain to research.

B. Purpose of the HIPAA Research Compliance Plan

The purpose of this Compliance Plan is to outline conditions for obtaining, using, and/or disclosing PHI for research. This includes the following:

- To assist us in identifying PHI and the manner in which it is to be used and disclosed;
- To assist us in avoiding improper use and disclosures of PHI;
- To establish compliance standards and procedures for members of our workforce;

- To effectively communicate the compliance standards, policies and procedures set forth in this Plan to all members who conduct clinical research;
- To take reasonable steps to achieve compliance with the standards, policies and procedures set for in this Plan by, for example, implementing, monitoring and auditing systems reasonably designed to detect the improper use and disclosure of PHI; and

- To respond appropriately to non-compliance after detection and to prevent recurrence, which may require modifications to this Plan.

The regulations impose three core requirements on health care providers and facilities (called "covered entities" in the regulatory text) that hold or maintain PHI. First, covered entitiesmust obtain the agreement of patients to use or disclose their PHI unless specified exceptions are applicable. Secondly, persons must be notified by covered entities of their rights under the privacy regulations. Lastly, use and disclosure of PHI by covered entities must generally be restricted to the minimum necessary to accomplish the intended purpose. The HIPAA Rule exercises four basic rights of persons with respect to their PHI to include: to agree to the use anddisclosure of PHI, to inspect and copy their records, to amend their records and to obtain certain limited audits of the disclosures of their records that have been made by covered entities.

C. Conditions when PHI may be utilized for Research Purposes

- Individual Subject's Authorization: After obtaining the individual subject's (or legally authorized representative's) authorization using the USA IRB HIPAA Authorization template located in IRBNet;

- Waiver of Authorization: After obtaining a Waiver of Authorization from any duly constituted IRB or Privacy Board (duplicative review is not required);

- Limited Data Set & Data Use Agreement: By using a Limited Data Set, subject to a Data Use Agreement;

- Deidentified Data: After the PHI has been deidentified; or

- Activities Preparatory to Research/Research on Decedent: After making certain representations to the appropriate organizational unit when utilizing PHI preparatory to research or PHI about a deceased individual. Note: compliance with these conditions is not in lieu of any IRB or other committee reviews required under a campus' human research protections program.

II. Research Use of PHI With Authorization

The HIPAA Privacy Rules characterize two basic types of written agreement that are utilized to secure the permission of persons for the use and disclosure of PHI. The first type is a general written consent by individuals for the use and disclosure of their PHI for treatment, payment and health care operations ("TPO") in the non-research setting. This written consent provides a one-time blanket permission for a covered entity to use PHI for various purposes related to clinical care. The second type of written agreement involves authorization for the use of PHI for specific purposes other than TPO. Specific written authorization is required for the use and disclosure of PHI in research studies. Under the regulations, this authorization may be incorporated into consent forms for clinical research or may be secured via a separate authorization form. The University of South Alabama IRB Office has adopted the option of including the authorization in the consent form for research studies.

> ** Core elements of information must be provided in writing to prospective subjects in securing authorization for the research use of their PHI. These items are provided in the HIPAA authorization template located in IRBNet.. This template must be inserted into the confidentiality section of the informed consent form.

A valid authorization for the release of PHI for research purposes requested by or asked of a potential subject in a research study must be retained for at least six years from the date permission is granted and must contain the following required elements:

1. a description of the information to be used or disclosed that identifies the information in a specific and meaningful manner;

2. the name of the covered entity or person(s) authorized to make the requested use or disclosure;

3. the name or other specific identification of the person(s) or entities which may include the covered entity itself to whom the covered entity may make the request for use or disclosure;

4. an expiration date and a signature and date;

5. the authorization must be written inplain language;

6. if the authorization is executed by a legal representative authorized to act for the individual, a description of his/her authority to act for the individual must be specified as well as the relationship to the individual;

7. a statement that the individual acknowledges that he/she has the right to revoke the authorization except to the extent that information has already been disclosed under the authorization;

8. a statement that the individual acknowledges that information used or disclosed to any entity other than a health plan or health care provider may no longer be protected by the federal privacy law;

9. a description of the purpose(s) of the requested use or disclosure;

10. a statement that the individual may inspect or copy the protectedhealth information to be used or disclosed; and

11. a statement that the individual may refuse to sign the authorization.

A. Research Use of PHI Without Authorization

HIPAA regulations allow the covered entity to use and disclose PHI for research purposes without subject authorization provided that any of the four criteria below are met. These include Waiver of Authorization, review of PHI preparatory to research, research involvinga decedent's information and use involving limited data sets. Applications for request to use PHIfor research purposes without subject authorization should be submitted to the IRB. Without appropriate documentation and approval, PHI can only be disclosed with authorization from the individual.

1. Waiver of Authorization **

A covered entity is permitted to disclose PHI for research purposes without a written authorization when approval is obtained from the IRB. A Waiver of Authorization form is located in IRBNet. In most cases, if a protocol will qualify for a waiver of aresearch informed consent from the IRB, it will be able to qualify for a Waiver of Authorization under HIPAA. The investigator must provide information about the research study that enables the IRB to determine that three requirements are satisfied:

a. there must be no more than minimal risk to the privacy of individual subjects based on the presence of the following elements:

- an adequate plan to protect the identifiers from improper use and disclosure;
- an adequate plan to destroy the identifiers at the earliest opportunity consistent with the conduct of the research, unless there is a health or research justification for retaining identifiersor such retention is otherwise required by law;
- an adequate written assurance that the PHI will not be reused or disclosed to any other person or entity, except as required by law,or for authorized oversight of the research study, or for other research for which the use or disclosure is permitted without authorization.

b. it must not be practicable to conduct the research without the waiver or alteration of the authorization requirement; and

c. it must not be practicable to conduct the research without access toand use of the PHI.

Once the IRB has approved the Waiver of Authorization, the investigator must provide the covered entity maintaining the PHI with documentation from the IRBof approval. The IRB approval letter will include the following elements:

(1) identification of the IRB and provide the date on which the Waiver of Authorization was approved, (2) a statement that the IRB has determined that the waiver satisfies the criteria explained above, (3) provide a brief description of the PHI for which use or access has been determined to be necessary by the IRB, and (4) the letter must describe whether the request for Waiver of the Authorization requirements was reviewed via full board or expedited review procedures.

A Waiver of Authorization may be sought for three specific research uses of PHI to identify potential research subjects through review of their PHI, to contact potential subjects in order to determine their interest in research participation and to receive or collect PHI during the conduct of research studies.

** The Waiver of Authorization form is located in IRBNet forms and templates.

2. Reviews Preparatory to Research **

Investigators may review PHI without authorization to prepare a research protocolor for similar purposes preparatory to research (i.e., limited to designing a study and/or determining the feasibility of completing a study). Neither recruitment nor patient contact is considered review preparatory to research. Under this provision of the regulations, the investigator must provide the following assurances to the covered entity:

1. The investigator shall not remove any PHR from thecovered entity;
2. The use/disclosure of PHI is sought solely for the purpose of preparing a research protocol; and
3. The PHI for which use or access is sought is necessary for research purposes.

In addition, reviews preparatory to research must not involve making copies of PHI or making notes that include PHI. However, medical records of interest to investigators in preparing a study may be flagged for future reference.

** Investigators may use PHI as preparatory to research if the investigator certifies the above provisions by completing the form attached as Appendix D.

3. Research on Decedent's Information **

An investigator is not normally required to submit research involving deceased individuals to the IRB for review, unless other living individuals, such as family memberscould be affected (i.e., genetic markers of certain diseases) and should contact the IRB if assistance is needed to make this determination. If IRB review is necessary, the investigator shall submit a protocol to the IRB. If not, the investigator may use PHI of deceased individuals without authorization from the decedent's estate.

Qualifications under this provision requires that the researcher provide the covered entity:

1. Assurance that the use or disclosure is being sought solely for research on thePHI of decedents;
2. Documentation, at the request of the covered entity, of the death of such individuals; and
3. Assurance that the PHI is necessary for research purposes.

** Investigators may use PHI in research on decedent's information if the investigator certifies the above provisions by completing the form entitled Research Involving Deceased Individuals.

4. Research Involving the Use of Limited Data Sets **

Regulations permit covered entities to use or disclosure PHI for research purposeswithout subject authorization if the use or disclosure only involves a "limited data set" and the covered entity enters into a data use agreement with the investigator. A "limited data set" is PHI that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual subjects:

a) names

b) postal address information, other than town or city, state and zip code

c) telephone numbers

d) fax numbers

e) email addresses

f) social security numbers

g) health plan beneficiary numbers

h) account numbers

i) certificate/license numbers

j) vehicle identifiers and serial numbers

k) device identifiers and serial numbers

l) web universal resources locators (URLs)

m) Internet protocol (IP) address numbers

n) biometric identifiers, including finger and voice prints

o) full face photographic images and any comparable images

p) A limited data set may, however include other indirect identifiers, especially datesof birth, treatment, discharge, or death.

** Investigators may use or disclose a limited data set without subject authorization for research purposes only if an assurance is obtained in the form of aLimited Data Use Agreement.

C. Use of De-Identified Data in Clinical Research **

The de-identified health information under HIPAA is much more specific than thegeneral de-identification standard applied under the federal laws relating to human research subjects. PHI can be released freely if it does not contain "individually identifiable information." PHI is not individually identified if the subject is not identified, directly or indirectly, and has no reasonable basis to believe that the information can be used to identify the subject. It may be used in research without subject authorization or an IRB waiver. The Privacy Rule refers to such health information as "de-identified data." Research which involves the use of "de-identified data" is exempt from the HIPAA requirements. To be exempt from HIPAA, none of the subject identifiers can be reviewed or recorded by the research team.
In order to de-identify PHI, the investigator will comply with one of the two following procedures:

A. *Use of a Statistician to include:*

- Obtain services of a person with appropriate experience and knowledge applying generally acceptable statistical and scientific principles and methods for determining that the information is not individually identifiable;
- Who makes a determination that there is a very small risk that the information could be used by itself or in combination with other available information by the anticipated recipient(s) to identify the subject with the information; and
- Who documents the methods and results in making such determination.

B. *Removal of all identifiers*

- Removal of all identifiers and have no actual knowledge that the information remaining could be used alone or in combination with other
  information to identify the patient who is the subject of the information.

** For research involving de-identified health information the investigator shall complete the HIPAA De-identification Certification form. The IRB shall determine if the PHI has been adequately de-identified in accordance with the privacy laws. If so, the IRB shall issue documentation to the researcher confirming review and approval of the research protocol as involving de-identified health information. The investigator may then use the IRB approval notice to access and create a de-identified database.

D. Transition Provisions

Personnel at the University of South Alabama may continue to use and disclose information concerning a research subject for a particular study, without obtaining the HIPAA authorization or the IRB action required by this policy, regardless of when the

information is created, collected or received, if, prior to April 14, 2003, the Principal Investigator obtained, and has written documentation of, any one of the following:

- An authorization or other express legal permission from the research subject to use or disclose the information for the research study;
- The research subject's informed consent to participate in the researchstudy;
- An IRB waiver of informed consent for the research study.

If the investigator has such documentation for a research subject, he/she may create, collect, or receive information after April 14, 2003. However, for subjects without such written documentation prior to April 14, 2003, the investigator must obtain a specific authorization or other appropriate documentation required by this policy. For subjects who enroll in studies on or after April 14, 2003, the regulations of the Privacy Rule described above must be followed.

E. Research subjects' rights under HIPAA

1. Right to an accounting -

   When a research subject signs an authorization to disclose PHI, the covered entityis not required to account for the authorized disclosure. Nor is an accounting required when the disclosed PHI is contained in a limited data set or is released tothe researcher as de-identified data. However, an accounting is required for research disclosures of identifiable information obtained under a waiver or alteredauthorization, reviews preparatory to research and research on decedents. In general, the Privacy Rule requires that individuals have a right to receive an accounting of disclosures of PHI made by covered entities over a six year period. It is anticipated that requests for an accounting of disclosure will come to the hospitals and the medical records department will respond in accordance with the policy on HIPAA: Accounting of Disclosures.

2. Right to revoke authorization -

   A research subject has the right to revoke his or her authorization unless the researcher has already acted in reliance on the original authorization. Under the authorization revocation provision, covered entities may continue to use or disclose PHI collected prior to the revocation as necessary to maintain the integrity of the research study. Examples of permitted disclosures include submissions of marketing applications to the FDA, reporting of adverse events, accounting of the subject's withdrawal from the study and investigation of scientific misconduct.

F. Research Recruitment

The Department of Health and Human Services states that covered entities may continue to discuss with patients the option of enrolling in a clinical trial. This can be done without subject authorization and without an IRB waiver of authorization. Similarly, direct care providers may communicate with their current or past patients about research opportunities without prior

authorization of these patients. This permission does not extend, however, to disclosure of information to a third party for purposes of recruitment. In the latter case, the covered entity either has to obtain an authorization from the individual or secure a Waiver of Authorization as permitted by the Privacy Rule. The use of a partial Waiver of Authorization fromthe IRB would allow researchers to get specific information from other practitioners.

G. Research Databases

If an investigator maintains a database containing PHI, then the investigator has an obligation to insure that the use and disclosure of PHI is in compliance with HIPAA policies.

A. Maintaining applicable security for the database, including physical security and accesscontrol;

B. Control and manage the access, use and disclosure of PHI, including verifyingappropriate IRB approvals and patient authorizations; and

C. Any PHI in the database used for treatment or payment purposes must be a duplicate andthe original must be included in the patient's medical record.

Remember, HIPAA applies to uses of PHI. In order to use a research database containingPHI, one must have authorization or a waiver from the IRB. Another pathway to using PHI in a research database is by utilizing a limited data set and completion of a Limited Data Use Agreement, enabling certain identifiers to be used during the research study. Example, the users of a tissue bank database would need to obtain individual authorization or a IRB waiver if he/she wanted to use and disclose the information in a research study.

H. HIPAA Security

The Security Rule defines the standards, which require covered entities to implement basic safeguards to protect the confidentiality, integrity, and availability of electronic protected health information (ePHI). Privacy depends upon security measures: no security, no privacy.

1. Administration

The covered components of University of South Alabama will maintain the security of ePHI, in the manner set forth in the University's HIPAA Security policies. The University adheres to all applicable general requirements, approaches, standards, implementation specifications, and maintenance requirements of the Security Rule in developing and maintaining policies and procedures for security standards for the protection of electronic protected health information.

2. Requirements and Responsibilities

The HIPAA Security Rule requires the University to put into place appropriate administrative, physical and technical safeguards to protect the integrity, confidentiality and availability of electronic protected health information (ePHI) that is created, received or managed by the University's covered components.

These requirements are fulfilled through completion of the IRB application process. The researcher will complete information requesting the utilization and storage of ePHI for research purposes.

3. Approved Tools for Storing ePHI

The following are licensed tools used by USA and USA Health and are expected to be used by employees, students and other agents of the University for storing ePHI of research subjects in accordance with HIPAA.

- Google Drive associated with USA account only
- Microsoft Office 365, SharePoint
- USA Health REDCap

Acceptable tools made available via third parties for clinical research may include:

- Sponsor or collaborator provided databases or portals for research data
- Database provided for Data Registry Participation

Direct questions regarding electronic platforms for storage of ePHI to the USA Health HIPAA Security Compliance Office, cpace@health.southalabama.edu

References:

Forms located in IRBNet, Forms and Templates -

Access Preparatory to Research

HIPAA Subject Authorization Template

Research Involving Deceased Individuals

Request for waiver or alteration of subject authorization for the use and disclosure of protected health information

USA's IRB HIPAA webpage

NIH Guide on Privacy Rule and Research