Institutional Review Board Procedure No. 15

EFFECTIVE DATE: ***July 26, 2024***

PROCEDURE TITLE:

HIPAA and Research

To be reviewed every three years by:
Institutional Review Board

REVIEW BY: ***July 25, 2027***

PROCEDURE

This Procedure implements the requirements of Institutional Review Board Policy No. 1 *Authority of the Institutional Review Board,* which requires the Trinity Health Mid-Atlantic (THMA) Institutional Review Board (IRB) establish policies and procedures to ensure that the THMA's IRB operations fully comply with applicable laws, regulations, professional standards, and the *Ethical and Religious Directives for Catholic Health Care Services*, including promoting the conduct of ethical and compliant research.

The THMA IRB has been designated as the Privacy Board for all use and disclosure of protected health information (PHI) for research purposes. The IRB will ensure that its use and disclosure of PHI for all research is in accordance with Health Insurance Portability and Accountability Act of 1996 (HIPAA) otherwise known as the Privacy Rule.

Application

This policy applies to any research study meeting the HIPAA definition of research: "a systematic investigation; including research development, testing, and evaluation; designed to develop or contribute to generalizable knowledge". This includes exempt research, as well as data and specimen banks designed for research purposes.

The use of the term "IRB" will be equivalent with "Privacy Board" for research use and disclosure of PHI for this Policy. All researchers must comply with this policy when PHI is used or disclosed for research purposes.

Regulatory background

The U.S. Department of Health and Human Services issued the Privacy Rule and the Security Rule to implement the requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

The Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule") establish a set of national standards for the protection of certain health information. The Privacy

Rule standards address the use and disclosure of individuals' health information, called "protected health information", as well as -standards for individuals' privacy rights to understand and control how their health information is used.

The Security Standards for the Protection of Electronic Protected Health Information ("Security Rule") establish a national set of security standards for protection of certain health information that is held or transferred in electronic form. The Security Rule operationalizes the protections in the Privacy Rule by addressing the technical and non-technical safeguards that organizations called "covered entities" must put in place to secure individuals' electronic protected health information (e-PHI). Refer to your Hospital's Security policies for more information.

The Office for Civil Rights (under Department of Health and Human Services) has the responsibility for implementing and enforcing the Privacy and Security Rules with respect to voluntary compliance activities and civil money penalties. A major goal of the Privacy and Security Rules is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care, conduct research, and to protect the public's health and well-being.

The Security Rule applies to any health care provider who transmits health information in electronic form under HIPAA (the "covered entities") and to their business associates.

I. Accessing Protected Health Information for research purposes

A. Covered entity's workforce or member

The THMA hospitals are each a covered entity. Workforce or member means "employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate" (45 CFR 160.103).

B. Business Associate Agreement

In general, a business associate is a person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of individually identifiable health information.

A person who is not part of the covered entity cannot access the medical record and extract PHI on the behalf of the Hospital without a fully executed Business Associate Agreement. Each Hospital's HIPAA Privacy Board, in consultation with the legal department, facilitates the need for and creation of Business Associate Agreements.

C. Protected Health Information:

The Privacy Rule protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.

The Privacy Rule calls this information "protected health information (PHI)". Protected health information is information, including demographic data that relates to the participant or to the relatives, employers, or household members of the participant, and:

- the individual's past, present or future physical or mental health or condition,
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual.

Protected health information identifies the individual or there is a reasonable basis to believe can be used to identify the individual. Protected health information includes many common identifiers:

1. Names;
2. Street address, city, county, precinct, state, and zip code; and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:
    i. The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
    ii. The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, date of service, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
4. Telephone numbers;
5. Facsimile numbers;
6. Electronic mail addresses;
7. Social security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers (including credit card numbers);
11. Certificate and license numbers;
12. Vehicle identifiers and serial numbers, including license plate numbers;
13. Device identifiers and serial numbers;
14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and other comparable images; and
18. Any other unique identifying number, characteristic, or code.

The Security Rule protects a subset of information covered by the Privacy Rule, which is all individually identifiable health information a covered entity creates, receives, maintains or transmits in electronic form. The Security Rule calls this information "electronic protected health information" (e-PHI). The Security Rule does not apply to PHI transmitted orally or in writing, but the Privacy Rule does.

The Security Rule defines "confidentiality" to mean that e-PHI is not available or disclosed to unauthorized persons. The Security Rule's confidentiality requirements support the Privacy Rule's prohibitions against improper uses and disclosures of PHI. The Security rule also promotes the two additional goals of maintaining the integrity and availability of e-PHI. Under the Security Rule, "integrity" means that e-PHI is not altered or destroyed in an unauthorized manner. "Availability" means that e-PHI is accessible and usable on demand by an authorized person.

D. Personal Representative:

Under the Privacy Rule, the scope of the personal representative's authority is to act for the research participant. This authority is derived from one's authority under applicable law to make health care decisions for the individual. Where the person has broad authority to act on the behalf of a living individual in making decisions related to health care, such as is usually the case with a parent with respect to a minor child or a legal guardian of a mentally incompetent adult, the covered entity must treat the personal representative as the individual for all purposes under the Privacy Rule, unless an exception applies. (See below with respect to abuse, neglect or endangerment situations, and the application of State law in the context of parents and minors).

Where the authority to act for the individual is limited or specific to particular health care decisions, **the personal representative is to be treated as the individual only with respect to protected health information that is relevant to the representation**. For example, a person with an individual's limited health care Power of Attorney regarding only a specific treatment, such as use of artificial life support, is that individual's personal representative only with respect to protected health information that relates to that health care decision. The covered entity (Hospital) should not treat that person as the individual for other purposes, such as to sign an authorization for the disclosure of protected health information for research purposes.

Finally, where the person has authority to act on the behalf of a **deceased individual** or his estate, which does not have to include the authority to make decisions related to health care, the covered entity must treat the personal representative as the individual with respect to protected health information relevant to such personal representation (e.g., an executor of an estate has the right to access all of the protected health information of the decedent relevant to these responsibilities).

Consult with the Hospital's legal department as State law should always be followed to determine the authority of the personal representative to receive or access the individual's protected health information.

Who must be recognized as the individual's Personal Representative under HIPAA (ONLY):

If the Individual Is:	The Personal Representative Is:
An Adult or An Emancipated Minor	• A person with legal authority to make health care decisions on behalf of the individual. • *Examples:* Health Care Power of Attorney, Court appointed legal guardian, General Power of Attorney or Durable Power of Attorney that includes the power to make health care decisions • Exceptions: See "abuse, neglect, and endangerment situations" discussion below in section F.
A Minor	• A parent, guardian, or other person acting in loco parentis with legal authority to make health care decisions on behalf of the minor child. • Exceptions: emancipated minor. Also see "parents and minors" and "abuse, neglect and endangerment situations" discussion below in sections E and F.
Deceased	• Person with legal authority to act on behalf of the decedent or the estate (not restricted to persons with authority to make health care decisions). • *Examples*: Executor or administrator of the estate. • Consensus of kin • Note that the Privacy Rule does not apply to the health information of an individual who has been deceased for more than 50 years; thus, a personal representative need not authorize disclosures of the decedent's health information nor does a personal representative have rights under the Privacy Rule with respect to such information.

E. Parents and minors

In most cases under the Rule, a parent, guardian, or other person acting in loco parentis (collectively, "parent") is the personal representative of the minor child and can exercise the minor's rights with respect to protected health information, because the parent usually has the authority to make health care decisions about his or her minor child. Privacy Rule defers to State law that expressly address the ability of the parent to obtain health information about the minor child.

However, the Privacy Rule specifies three circumstances in which the parent is not the "personal representative" with respect to certain health information about his or her minor

child. In these situations, the parent does not control the minor's health care decisions, and thus under the Rule, does not control the protected health information related to that care:

1. When State or other law does not require the consent of a parent or other person before a minor can obtain a particular health care service, and the minor consents to the health care service;

   Example: A State law provides an adolescent the right to obtain mental health treatment without the consent of his or her parent, and the adolescent consents to such treatment without the parent's consent.

2. When someone other than the parent is authorized by law to consent to the provision of a particular health service to a minor and provides such consent;

   Example: A court may grant authority to make health care decisions for the minor to an adult other than the parent, to the minor, or the court may make the decision(s) itself.

3. When a parent agrees to a confidential relationship between the minor and a health care provider.

   Example: A physician asks the parent of a 16-year-old if the physician can talk with the child confidentially about a medical condition and the parent agrees.

F. Abuse, neglect, and endangerment situations

When a physician or other covered entity reasonably believes that an individual, including an emancipated minor, has been or may be subjected to domestic violence, abuse, or neglect by the personal representative, or that treating a person as an individual's personal representative could endanger the individual, the covered entity may choose not to treat that person as the individual's personal representative, if in the exercise of professional judgment, doing so would not be in the best interests of the individual. For example, if a physician reasonably believes that providing the personal representative of an incompetent elderly individual with access to the individual's health information would endanger that individual, the Privacy Rule permits the physician to decline to provide such access.

G. Minimum necessary restriction:

The Privacy Rule imposes a minimum necessary requirement on all permitted uses and disclosures of PHI by a covered entity (Hospital). This means that a covered entity must apply policies and procedures, or criteria it has developed, to limit certain uses or disclosures of PHI, including those for research purposes, to "the information reasonably necessary to accomplish the purpose (of the sought or requested use or disclosure)." For uses and routine and recurring disclosures of and requests for PHI, the covered entity must

develop policies and procedures (which may be standard protocols) to reasonably limit such uses, disclosures, and requests to the minimum necessary to achieve the purpose of the use or disclosure. For non-routine disclosures and requests, a covered entity must review each disclosure or request individually against criteria it has developed.

II. Review process

A. Review of requests

The forms and template to make a request for the use and disclosure of PHI for research purposes are located in IRBManager. The IRB will receive and review all research requests for access to, use or disclosure of the PHI that the Hospital receives, creates, and/or maintains. When there are questions about whether a project constitutes research as defined under HIPAA, contact the IRB.

The type of review used will be dictated by the federal regulations that govern research (HIPAA, OHRP, FDA, etc.). The IRB may use an expedited review procedure if the research involves no more than minimal risk to the privacy of the individuals who are the subject of the protected health information for which use or disclosure is being sought.

When a request is made where authorization from the research participant(s) will not be obtained, the IRB will evaluate whether the purpose of the research project could be reasonably accomplished with alternatives such as using a de-identified dataset or, if appropriate, a limited data set.

An IRB member who has a conflict of interest with the research study or the HIPAA information requested may not participate in the review of the HIPAA request, including those at a convened meeting, as well as those requests reviewed via the expedited or exempt determination processes.

The IRB minutes must include sufficient detail to apprise the IRB members when a request for not obtaining HIPAA authorization (Limited Data Set, decedents, waiver) has been granted by the IRB via any of the review types, including exempt research.

III. Permitted use and disclose of PHI

Use and disclosure of protected health information (PHI) for any research purpose is only permitted if one or more of the following circumstances, below, applies.

Exception: a covered entity must obtain an individual's expressed HIPAA authorization for any use or disclosure of psychotherapy notes.

A. The participant's authorization is obtained

1. HIPAA authorization for the use and disclosure of PHI for a specified research purpose is obtained from the participant or their personal representative. The research HIPAA authorization must satisfy the required elements and statements listed below (as per 45 CFR 164.508) and are contained in each IRB's HIPAA Authorization template, which is part of the Informed Consent template. The template can be found on the respective IRB's website.

Required HIPAA authorization elements:

- A description of the PHI to be used or disclosed, identifying the information in a specific and meaningful manner
- The names or other specific identification of the person or persons (or class of persons) authorized to make the requested use or disclosure
- The names or other specific identification of the person or persons (or class of persons) to whom the covered entity may make the requested use or disclosure
- A description of each purpose of the requested use or disclosure
- Authorization expiration date or expiration event that relates to the participant or to the purpose of the use or disclosure ("end of the research study" or "none" are permissible for research, including for the creation and maintenance of a research database or repository)
- Signature of the participant and date. If the participant's personal representative signs the authorization, a description of the representative's authority to act for the individual must also be provided.

Authorization required statements:

- A statement of the participant's right to revoke authorization and how to do so, and, if applicable, the exceptions to the right to revoke authorization or reference to the corresponding section of the covered entity's notice of privacy practices.
- Whether treatment, payment, enrollment, or eligibility of benefits can be conditioned on authorization, including research-related treatment and consequences of refusing to sign the authorization, if applicable.
- A statement of the potential risk that PHI will be re-disclosed by the recipient and no longer protected by the Privacy Rule. This may be a general statement that the Privacy Rule may no longer protect health information disclosed to the recipient.

Additionally, the investigator:

- May combine the research HIPAA authorization with any other type of written permission regarding the same research study, including another research authorization or any consent to participate in the research except for authorization for the use and disclosure of psychotherapy notes;
- May condition the provision of research-related treatment on the provision of the authorization for the use or disclosure of PHI.
- Must include a statement as to the specific research study. However, future studies may be generalized and not study specific, but the authorization must adequately describe the future research purposed such that it would be reasonable for the individual to expect that his or her PHI could be used or disclosed for such future research.
- Must include a statement as to the end date for the use or disclosure. The authorization may include a statement such as "end of research study" or similar language to describe the expiration event for the authorization.
- May include a statement "none" or similar language to describe the expiration event if the authorization relates to the creation or maintenance of a research database or research repository or when the use is for future research (see your IRB's policy on data and specimen repository banks)
- Must use an authorization that is in plain, lay person language.
- Must provide a copy of the signed authorization to the participant.

2. Limits on using and disclosing PHI if HIPAA authorization is revoked

Although an Authorization for research uses and disclosures need not expire, a research participant has the right to revoke, in writing or verbally, his or her authorization at any time. The effective date of the participant's revocation is when the covered entity receives the revocation, except to the extent that the covered entity has taken action in reliance upon the authorization.

For example, a covered entity is not required to retrieve information that it disclosed under a valid authorization before receiving the revocation. This would permit the continued use and disclosure of PHI already obtained pursuant to the authorization to the extent necessary to protect the integrity of the research. For example, to account for a participant's withdrawal from the research study, to conduct investigations of scientific misconduct, or to report adverse events.

3. Alteration of HIPAA authorization

When HIPAA authorization for the use and disclosure of PHI for a specified research purpose is obtained from the participants, BUT the research HIPAA authorization does not include all or alters one or more of the required elements and statements (as per 45 CFR 164.508), this is referred to as an alteration of HIPAA authorization.

When some of the required elements of HIPAA authorization will not be included or will be altered, certain regulatory criteria must be met.

The IRB must document and confirm that an alteration of the research participant's authorization requirement is consistent with all of the following regulatory criteria prior to its use:

a. The use or disclosure of PHI involves no more than minimal risk to the privacy of the individuals based on, at least, 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 conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and
- Adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of protected health information would be permitted by this subpart;

b. The research could not practicably be conducted without the alteration;

c. The research could not practicably be conducted without access to the use of the PHI; and

d. The IRB has provided the researcher with correspondence that it has approved the alteration of authorization.

This documentation **must** include:

- The name of the IRB,
- The date the alteration of authorization was approved,
- A statement that the IRB/privacy board has determined that the alteration of authorization satisfies the regulatory criteria listed above,
- A description of the PHI needed,
- whether a conveyed or expedited procedure was used, and
- The signature of IRB Chair or designated IRB member

B. The participant's authorization is not obtained

When the participant's or personal representative's authorization will not be obtained, the use and disclosure for a specific research purposes must meet certain regulatory criteria

and the minimum PHI necessary for meeting the research purpose may only be used or disclosed.

Exceptions: Note that an individual's authorization to use or disclose psychotherapy notes must be obtained in order to be used for research purposes. Additionally, an individual's HIPAA authorization to use or disclosure of information about the diagnosis and testing for HIV, AIDS, and ARC (AIDS Related Complex); must be obtained, as well as informed consent.

Below are the options for research use and disclosure of PHI when authorization is not obtained:

1. Partial or full waiver of HIPAA authorization

The IRB must document and confirm that a partial or full waiver of the research participant's authorization requirement prior to it's use meets the following criteria (45 CFR 164.512):

a. The use or disclosure of PHI involves no more than minimal risk to the privacy of the individuals, based on a minimum of:

- 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 conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and
- Adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of PHI would be permitted;

b. The research could not practicably be conducted without the waiver;
c. The research could not practicably be conducted without access to and the use of the PHI; and
d. The use and disclosure is the minimum necessary for the research purpose, and
e. The IRB has provided the researcher with correspondence that it has approved the waiver of authorization.

This documentation must include:

- The name of the IRB,
- The date the waiver of authorization was approved,

- A statement that the IRB/privacy board has determined that the waiver of authorization satisfies the regulatory criteria listed above,
- A description of the PHI needed,
- Whether a conveyed or expedited procedure was used, and
- The signature of IRB Chair or designated IRB member

2. Deceased person's PHI

When a deceased person's medical record or PHI will be used or disclosed for research purposes without prior authorization, the IRB must review prior to the use and disclose and grant the request. The request must meet the following regulatory criteria (45 CFR 164.512):

a. Assurances must be obtained from the researcher that the use or disclosure of PHI is solely for research involving PHI of deceased persons,
b. The researcher must agree to provide documentation of the death of the individual(s), at the request of the IRB,
c. The research must provide assurances that the PHI for which use and disclosure is sought is necessary for the research purposes,
d. The use and disclosure of PHI must be the minimum necessary for the research purposes. When a decedent's PHI option is granted by the IRB/privacy board, this will be documented in writing to the investigator.

3. Limited Data Set with a Data Use Agreement

A Limited Data Set refers to when PHI will be made "anonymous" but not completely "deidentified" by allowing the use or disclosure of 4 of the 18 PHI direct identifiers (dates and/or locations) of the individual or of relatives, employers, or household members of the individual for research purposes without obtaining either an individual's authorization or a waiver or an alteration of authorization for its use and disclosure, with a Data Use Agreement (45 CFR 164.514). These may include:

- city
- state
- ZIP code
- elements of date
- and other numbers, characteristics, or codes not listed as direct identifiers.

The following identifiers must be removed from health information if the data are to qualify as a limited data set:

- names
- postal address information, other than town or city, state, and ZIP Code
- telephone numbers

- fax numbers
- electronic mail addresses
- social security numbers
- medical record numbers
- health plan beneficiary numbers
- account numbers
- certificate/license numbers
- vehicle identifiers and serial numbers, including license plate numbers
- device identifiers and serial numbers
- web universal resource locators (URLs)
- internet protocol (IP) address numbers
- biometric identifiers, including fingerprints and voiceprints
- full-face photographic images and any comparable images

With this option, the PHI is part of a Limited Data Set that the Hospital creates and the recipient, typically external to the Hospital has signed a Data Use Agreement with the Hospital prior to receiving the limited data set. Data Use Agreements are agreements that the covered entity enters into with the intended recipient of a limited data set that establishes the ways in which the information in the limited data set may be used and how it will be protected.

Data use agreements are processed and issued through the Hospital HIPAA Privacy Officer and/or Legal Department. The uses & disclosure of PHI must be the minimum necessary.

When a Limited Data Set with the required Data Use Agreement is granted by the IRB (who is the Privacy Board), this will be documented in writing to the investigator and be documented in the IRB minutes.

4. Data de-identified to the standards of HIPAA

Generally, for research purposes, de-identified data is provided to a researcher by someone who is part of a covered entity and who is not part of the research team. Someone else who is a Hospital or Trinity Health employee would extract the data and use a HIPAA compliant method to render the data de-identified, prior to giving only the de-identified data to the research team. The minimum necessary data will be used or disclosed to accomplish the research purpose. Note that there may not be a link, unless it meets the re-identification requirements below.

Protected Health Information is deemed to be "de-identified" under the HIPAA regulation (45 CFR164.514) if the health information does not identify an individual (or relatives, employers, or household members of the participant) and there is no reasonable basis to believe that the information can be used to identify these individuals.

a. PHI must be de-identified by one of the following two methods:

1st Option: The covered entity (Hospital) does not have actual knowledge that the information (PHI) could be used alone or in combination with other information to identify an individual who is a subject of the information. Additionally, the following identifiers of the participant, or of the relatives, employers, or household members of the participant, are removed:

1. Names;
2. Street address, city, county, precinct, state, and zip code; and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:
    i. The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
    ii. The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, dates of service, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
4. Telephone numbers;
5. Facsimile numbers;
6. Electronic mail addresses;
7. Social security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers (including credit card numbers);
11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers, including license plate numbers;
13. Device identifiers and serial numbers;
14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and other comparable images; and
18. Any other unique identifying number, characteristic, or code.

2nd Option: The second method of de-identifying participant PHI is to obtain the counsel of a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable (a statistical expert).

1. The statistical expert must apply generally accepted statistical and scientific principles and methods and determine that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify the research participant(s); and
2. Prior to the IRB approving the use or disclosure of de-identified information for research, the statistical expert must submit documentation of:
    i. his or her credentials to support their statistical expert expertise and
    ii. the methods and results of the analysis that justify the determination of a very small risk of re-identification. The written documentation must be reviewed by the IRB in order to make a determination.

b. Re-identification: Someone who is not on the research team may assign a code or other means of record identification to allow de-identified information to be re-identified. When doing so, the code or the mechanism for re-identification:

1. Must not be derived from or related to information about the individual;
2. Is not otherwise capable of being translated so as to identify the individual; and
3. The covered entity must not use or disclose the code or other means of record identification for any other purpose and does not disclose the mechanism for reidentification.
4. Must not be shared with members of the research team, including the PI, unless IRB approval is granted to do so.

c. Regardless of the method to de-identify data, the minimum necessary rule for the use or disclose of the PHI to accomplish the research purpose must be applied.

d. When a de-identified data method is granted by the IRB, this will be documented in writing to the investigator and be documented in the IRB minutes.

5. Preparatory to research

Preparatory to research can be used to achieve one of two options:

1st Option: to conduct preparatory activities prior to formulating a research idea to determine, for example, whether there is a sufficient number or type of records to conduct the research.

This option may be used by both non-workforce and workforce members, but no contact with the potential participants is permitted.

2nd Option: to identify (screen) or to contact potential participants. A Hospital workforce member or employee who has a research project can screen for or identify potential participants with the caveat of eventual obtainment of their HIPAA authorization.

This second option may not be used by non-workforce members, except that the covered entity may contract with a business associate to assist the Hospital in contacting individuals on its behalf to obtain potential participant's authorizations, as long as the other criteria, listed below, are also met.

Alternatively, the Hospital may disclose PHI to a researcher, who is either a non-workforce or workforce member, for recruitment purposes when the Hospital's IRB has partially waived the authorization requirement—see Partial or Full Waiver of HIPAA Authorization, above, for regulatory criteria that must be met for this option.

When using the 1st or 2nd options under preparatory to research, assurances must be obtained from the investigator that (45 CFR 164.512):

a. The use or disclosure of PHI is sought solely to review PHI as necessary to prepare a research protocol or similar purpose preparatory to research,

b. No PHI will be removed from the Hospital (the covered health entity) by the researcher during the course of the review, (e.g., physically taken out of a facility, or downloaded and retained on a researcher's personal device or external to the Hospital device).

Under the Cures Act, clarification is offered that remote access connectivity does not constitute removal of PHI, unless there is downloading, copying, printing, saving occurring; and the remote access connection complies with the HIPAA Security Rule's requirements for appropriate safeguards to protect the organization's electronic PHI [access control [45 CFR 164.312(a)], integrity [45 CFR 164.312(c)(1)], person or entity authentication [45 CFR 164.312(d)], and transmission security [45 CFR 164.312(e)(1)].

Note: The Hospital cannot reasonably rely on the researcher's representations that PHI will not be removed from the covered entity, when the research has no relationship with the Hospital, unless the researcher's ability to remove PHI is managed (e.g., view-only access to ePHI and prevent copying, printing, saving, downloading, or any other means to control or retain the PHI).

c. The PHI for which use and disclosure is sought is necessary for the intended research purposes, and

d. The minimum necessary data will be used or disclosed to accomplish the research purpose.

When a preparatory to research option is granted by the IRB, this will be documented in writing to the investigator.

IV. Revising an option for HIPAA use and disclose of PHI for research purposes

If a researcher finds that later on in the course of a research study that another piece of identifiable information is needed that has not been previously listed or the time frame needs to be expanded, the researcher must submit a new request to do so and obtain approval from the IRB, prior to its use in the same fashion as the initial authorization (or as appropriate). This applies to exempt and all other types of research.

V. Retention of records for 6 years

When a waiver of the HIPAA authorization (full or partial) or an alteration of the HIPAA authorization is granted, the Principal Investigator, as well as the covered health entity are required to retain the IRB's signed documentation granting approval of the request for six years from either the date that approval was granted or the date when it was last in effect, whichever is later.

VI. Re-disclosure by third parties

Sponsors and external contract research organizations are not considered covered entities as defined by the HIPAA regulation. Once protected health information is used and disclosed to non-covered entities the HIPAA rule may no longer apply and the information may not be protected.

VII. Disclosures requirement:

A covered entity must disclose protected health information in only two situations: (a) to individuals (or their personal representatives) specifically when they request access to, or an accounting of disclosures of, their protected health information; and (b) to federal authorities when it is undertaking a compliance investigation or review or enforcement action.

Accounting of disclosures

Accounting of disclosures is information that describes a covered entity's disclosures of individually identifiable health information without authorization (i.e., a waiver of authorization was granted), made after April 14, 2003. Covered entities are required to provide information describing disclosures involving less than 50 participants and these must be tracked on an individual basis with the exception of Limited Data Sets obtained under a Data Use Agreement.

The disclosure contains participants screened or enrolled and is tracked by the investigator. When the study involves 50 or more individuals, the investigator's disclosure report must include a summary of the study only. The accounting must include disclosures that have occurred during the

6 years (or a shorter time period at the request of the individual) prior to the date of the request for an accounting. The Hospital's HIPAA Privacy Officer oversees the accounting of disclosures.

Requesting an accounting of disclosures

Any patient can request an accounting of disclosures of their PHI by contacting the Hospital HIPAA Privacy Officer or the Health Records Department. The accounting provided to the individual will include a list of all research studies in which the individual's health information could have been potentially included without their authorization.

VIII. Policy violations

Warning: Those who violate HIPAA may be subject to significant criminal and civil penalties. Hospital employees, students and volunteers are obligated to report violations of this policy to the Hospital's HIPAA Privacy Officer, Integrity and Compliance Officer, IRB Chair, and the IRB Administrator. Such reports will be brought before the IRB that served as the Privacy Board, during a convened meeting. The IRB will make a determination, in consultation with applicable Hospital officials, to assess whether additional information and/or further investigation is required. Where violations are apparent, the Hospital HIPAA Privacy Officer and/or the IRB, in consultation with applicable Hospital officials, may take immediate corrective action as deemed appropriate, prior to review by the convened IRB. In addition, other applicable Hospital offices and/or external agencies (e.g., Office of Civil Rights) will be notified as required.

RESPONSIBLE DEPARTMENT

Further guidance concerning this Procedure may be obtained from the Trinity Health Mid-Atlantic Institutional Review Board.

RELATED PROCEDURES AND OTHER MATERIALS

http://privacyruleandresearch.nih.gov/pr_02.asp

https://privacyruleandresearch.nih.gov/irbandprivacyrule.asp

https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaasimplification-201303.pdf

https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

APPROVALS

Initial Approval: August 28, 2020

Subsequent Review/Revision(s): July 26, 2024