Navigating HIPAA Compliance in Human Subject Research: The Privacy Rule

The Health Insurance Portability and Accountability Act (HIPAA) aims to safeguard health information and includes provisions under which a covered entity may use or disclose protected health information (PHI) for research purposes. HIPAA includes both a Privacy Rule, which focuses on how PHI is *utilized*, and a Security Rule, which focuses on how PHI is *safeguarded*. The information provided below pertains to the Privacy Rule. For additional information on the Security Rule, see the information available here).

Generally, in order to conduct research *using* PHI, one of the following conditions must be met:

- Individual authorization is obtained from the subject;
- A waiver of HIPAA authorization is granted by the Research Subjects Review Board (RSRB);
- The information is de-identified;
- The information is part of a limited data set and a data use agreement is executed; or
- For reviews: a) preparatory to research or b) on decedent information, certification regarding the review and disclosure of information obtained during the review is provided to the Privacy Officer.

Individual Authorization

Authorization for use or disclosure of PHI is typically combined with the informed consent document (see RSRB Biomedical Consent Template), though in some cases authorization may be obtained separate from informed consent. HIPAA requires that individual authorization:

a) Be obtained *prior* to use or disclosure of PHI;
b) Include specific elements/statements (e.g., a description of the PHI that will be used or disclosed, a description of the purpose of the use or disclosure, individuals or organizations who may use, disclose or receive the information, the subject's right to revoke the authorization, etc.); and
c) Be signed and dated by the subject or their authorized representative.

Waiver of HIPAA Authorization

In some cases, the use or disclosure of PHI without individual authorization may be permissible (e.g., when conducting a chart review of existing medical record data) provided that an IRB determines and documents that the following criteria in the Privacy Rule are satisfied:

a) The use or disclosure of PHI involves no more than minimal risk to the privacy of the subject;
b) The research cannot practicably be conducted without the waiver; *and*
c) The research cannot practicably be conducted without access to and use of the PHI

Partial waivers or alterations of HIPAA authorization may also be requested for specific circumstances when the criteria listed above are met. A ***partial waiver of HIPAA authorization*** allows for limited use or disclosure of PHI for recruitment and screening purposes. For example, a partial waiver may be required if the study team needs to collect and verify eligibility criteria and share that information outside the covered entity *prior* to obtaining individual authorization to participate in the research. Note that a partial waiver applies only to one portion of the study; not the use or disclosure of PHI for the purposes of the study as a whole. Meaning, the

partial waiver is initially applied only to the screening process; once eligibility is verified, full authorization is obtained at the time of consent for the use/collection/disclosure of PHI from that point forward.

An ***alteration of HIPAA authorization*** allows for some, but not all, of the required HIPAA elements (e.g., required statements and/or written signature and date) to be waived. For example, an alteration may be granted for a study that will obtain subject consent orally (via a waiver of documentation of consent). In this manner, the subject might be provided the necessary HIPAA statements in an information letter or have them read aloud to them but, because the subject is only providing their agreement to participate in the research orally and not physically signing the consent form, the written signature and date requirement can't be met and therefore an alteration of HIPAA authorization must be requested.

When waivers, partial waivers, or alterations are included as part of an IRB submission, they will be reviewed and approved by the reviewing IRB. If waivers, partial waivers or alterations are included in projects not requiring IRB review and approval (e.g., case studies), the Privacy Officer will review and approve the request via URMC HIPAA Form 25.2.

De-Identification

Information is considered de-identified when it cannot be related or attributed to a specific person. More specifically, this means that:

a) None of the 18 HIPAA identifiers are used/collected; ***and***
b) None of the used/collected information could be used alone or in combination to identify who the data is attributed to.

Health information that has been de-identified at the outset of a project is not individually identifiable. As such, it is not considered to be PHI and therefore not subject to HIPAA compliance. URMC HIPAA Policy, however, requires covered entity investigators utilizing de-identified information certify that the data is appropriately de-identified prior to use via URMC HIPAA Form 25.5.1. Information that is de-identified at the outset of a project is also not typically considered to meet the definition of 'human subject' and therefore IRB review and approval may not be required (see OHSP Policy 301 RSRB Scope and Authority).

Note that careful consideration must be paid to evaluating whether a project's data is de-identified or coded as these codes are often used interchangeably, though they do not have the same meaning. Clarification on de-identified and coded terminology is available in OHSP Explains… Coded vs. De-Identified; Anonymized vs. Anonymous.

Limited Data Set and Data Use Agreement

A limited data set (LDS) is a data set of PHI that may include:

a) Town, city, state and zip code;
b) Dates related to an individual (e.g., birth date, clinic visit date, vaccination date, admission date, etc.); and
c) A unique code or identifier that is *not* a direct identifier.

In other words, a limited data set excludes all 18 HIPAA identifiers except those listed above. Limited data sets may be used without the subject's authorization for research conducted by investigators within the covered entity or external individuals/organizations that may or may not be part of another covered entity. Use of a LDS

requires execution of a data use agreement (DUA), which establishes the ways in which the information in the LDS will be utilized, disclosed and protected.

Investigators wishing to a create a LDS utilizing PHI generated by the URMC covered entity must complete URMC HIPAA Forms 25.6.1 (Creation of Limited Data Set). To implement a DUA, depending on whether the Investigator is sending or receiving a LDS, the Investigator should complete URMC HIPAA Form 25.6.2 or URMC HIPAA Form 25.6.3 or the corollary Office of Research and Project Administration DUA forms. If the terms set forth in the DUA require deviation from the standardized language provided in these forms, the Privacy Officer or the investigator's Research Administrator in the Office of Research and Project Administration must be contacted *prior* to signing the DUA.

Reviews Preparatory to Research

Reviews 'preparatory to research' involve accessing PHI, without authorization, prior to conducting the actual research (e.g., for purposes related to designing the research or assessing feasibility of the research). Investigators wishing to access PHI for these purposes, must complete URMC HIPAA Form 25.3, for each applicable study, prior to accessing any PHI. Completing the form certifies that:

a) The PHI is only being used or disclosed to prepare for research;
b) Collection of the PHI is necessary to prepare for the research; and
c) Collected PHI will not be disclosed outside the URMC covered entity.

Note that, from a recruitment standpoint, preparatory to research activities, only allows researchers to identify potential subjects. Further use or disclosure of PHI, beyond these activities (i.e., contacting or recruiting subjects) requires approval by the reviewing IRB.

Research on Decedent Information

While not technically human subject research, research involving *only* decedent information may be conducted without authorization provided URMC HIPAA Form 25.4 is completed. The form certifies that research PHI is sought solely for research on decedents (i.e., data on living family members or relatives will not be collected) and that the PHI is necessary for the purposes of the research. Investigators conducting such research must also be able to provide, at the request of the reviewing IRB, Privacy Office or their designee, documentation of the death of involved individuals.

Additional Considerations

HIPAA compliance is not only a matter of determining how to appropriately access PHI; it can affect how you manage your study team, how you recruit and communicate with subjects, and how you run your day-to-day operations. Consider the following:

- All covered entity workforce members (including unpaid volunteers, students and interns) are required to complete **HIPAA Privacy training**. While faculty and staff are typically directed to complete this training as part of New Hire Orientation; investigators, administrators and managers should ensure team members have completed the training prior to engaging with subjects. Alternately, if study team members do not complete New Hire Orientation, they should be directed to do so via the HIPAA Privacy Office's Training & Education website.
- Only investigators with '**routine access**' to prospective subjects should recruit subjects directly ('routine access' means the investigator already has a clinical reason to know/review a potential subject's record). 'Cold calling' subjects is not permitted (see OHSP's Guideline for Recruitment Methods & Materials for additional information).

- The Privacy Rule imposes a 'minimum necessary' standard for most uses and disclosures of PHI. This means that study team members must restrict their access to PHI to the minimum necessary in order to accomplish their aims.
- All data must be appropriately **safeguarded**. Access to study files and data should be limited to study team members only. Hard copy documentation should be stored securely. Electronic data should be stored on the University's network server as opposed to a computer hard drive. Electronic devices (e.g., digital voice recorders, iPads) used to collect data must be encrypted.
- Individual patients may request a record of certain PHI disclosures made by a covered entity. As such, per URMC HIPAA Policy, investigators must account for any disclosures of PHI outside the URMC covered entity via URMC HIPAA Form 9.1 (except when individual authorization has been obtained or the research involved a LDS under a DUA). **Accounting for disclosures** includes tracking the date of the disclosure, the individual/organization that received the information (including their address), a description of the PHI disclosed, and the purpose for the disclosure.
- Study teams must be cognizant of all forms of **PHI-related communications**. Conversations with subjects and among study team members should be kept private. The content of voicemails left for subjects should adhere to the 'minimum necessary' standard; communicating only necessary information in a manner that protects the subject's privacy should another individual overhear the voicemail. E-mail communications with subjects must be encrypted and restricted to those who have provided explicit consent to e-mail communications. Text messaging is *not* a secure method of communicating with subjects and is generally not permitted.
- Documentation pertaining to HIPAA Privacy Rule compliance (e.g., signed authorizations, DUAs, HIPAA certification forms, etc.) must be **retained for 6 years** following completion of the research.
- Beware of phishing! Email and internet use unrelated to a specific study or subject can still affect PHI security. Avoid opening unrecognizable or questionable links/attachments in emails and surfing to unknown websites.

APPENDIX 1: WHAT IS PHI?

PHI is defined as any individually identifiable information that is created or received by a health care provider that relates to: a) the past, present or future physical or mental health or condition of an individual; b) provision of health care to an individual; or c) the past, present or future payment for the provision of health care to an individual.

APPENDIX 2: WHAT IS A 'COVERED ENTITY'?

A covered entity is defined as a health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a standard transaction. The University of Rochester Medical Center (URMC) & Affiliates covered entity includes over 22 local healthcare facilities/entities (for a full list see the URMC & Affiliates Notice of Privacy Practices). Individuals working in any of the facilities/entities that are part of the URMC & Affiliates covered entity are considered part of the covered entity, regardless of whether they provide direct clinical care to patients (e.g., all individuals working at Eastman Dental, irrespective of their role, are part of the covered entity).

HIPAA requirements only apply to research conducted under a covered entity (e.g., URMC, Highland Hospital, Mt. Hope Family Center, etc.). When all study team members are part of the covered entity, HIPAA compliance is required. Conversely, if *no* members of the study team are affiliated with the covered entity then HIPAA

requirements do not apply to the research. If, however, the study team is comprised of ***both*** members of the covered entity and members who are not part of the covered entity (e.g., River Campus faculty or staff), the entire study team must comply with HIPAA when PHI is collected as part of the research.

APPENDIX 3: WHAT HAPPENS WHEN A BREACH OCCURS?

When a breach (or suspected breach) involving PHI occurs related to a research study, investigators must report the incident to the Privacy Office and to the RSRB. The Privacy Office and the RSRB/Reviewing IRB will work together to collect any additional information needed in order to make determinations about risk and possible notifications to the affected subjects. The Privacy Office conducts a risk assessment to determine whether PHI has been compromised and the risk associated with the breach. The RSRB/Reviewing IRB reviews the incident considering the result of the Privacy Office's review and determines if the breaches is a UPIRTSO (unanticipated problem involve risk to subjects or others). The Privacy Office and the RSRB will work together to notify affected subjects, if it is determined that subjects need to be notified.

The Privacy Office has only 60 days from the date the covered entity is aware of a potential breach to conclude the investigation, so it is critical that Investigators report potential breaches promptly.

ADDITIONAL RESOURCES:

- OHSP Policy 702 HIPAA Privacy Rule
- UR Guideline for Human Subject Research Data Security Requirements
- RSRB Biomedical Consent Template
- OHSP Explains… Assurances, Agreements & Reliance
- OHSP Explains… Coded vs. De-Identified; Anonymized vs. Anonymous
- URMC & Affiliates HIPAA Policy 0P25 Use or Disclosure of PHI for Research Activities
- URMC & Affiliates HIPAA Procedure 0P25 Use of Disclosure of PHI for Research Activities
- URMC & Affiliates HIPAA Research Activities Forms & Guidance
- HHS HIPAA for Professionals: Research
- NIH's Clinical Research and the HIPAA Privacy Rule
