

29.0 HIPAA and IRB Review

“HIPAA” refers to the Health Insurance Portability and Accountability Act of 1996. HIPAA regulations apply to health care providers, insurers and clearinghouses. HIPAA’s privacy regulations afford privacy protections for individually identifiable health care and demographic information (this includes nonmedical information such as addresses) that has been obtained in the course of health care treatment, payment or operations. This individually identifiable information is called “protected health information” (“PHI”). For a definition of “Protected Health Information” see the Definitions section of these SOPs. HIPAA’s privacy requirements are additional to other ethical and regulatory protections for human research subjects and do not supersede them.

The application of the HIPAA privacy regulations to research occurs at the interface of research with health care – i.e., when researchers access and use PHI held by health care providers, insurers or clearinghouses. The HIPAA access and use rules are based on the purpose for accessing and using the PHI. A clinician who also is an investigator may create PHI in the course of providing health care services to a patient and may also wish to use this patient’s PHI in a research study. The rules for the clinician’s access to and use of the PHI for treatment purposes are different from the rules for that same clinician’s access to and use of the same PHI for research. When both treatment and research are occurring simultaneously in a study, it is very important to comply with all appropriate regulations for each of these separate purposes/functions as required by law.

Research use of PHI requires an explicit written authorization except under the following circumstances:

- The individually identifiable health information is not PHI (as defined by HIPAA) because it was not generated in the course of the provision of health care services by a health care provider, health plan, or health care clearinghouse and does not flow from the researcher into a medical record or other record related to health care treatment, payment or health care operations; Examples of this would be (a) personal health information provided directly by the research subject to the researcher and put into a research record but not flowing from the researcher into any medical record of that individual, or (b) physical or physiological measurements of an individual made by a researcher in a nonclinical setting and entered by the researcher into a research database but not flowing from the researcher into a medical record; or
- The IRB has approved a waiver of authorization; or
- The PHI is no longer PHI governed by HIPAA because it has been “deidentified” by being stripped of all 18 identifiers specified by HIPAA (See Appendix N) before the data are provided to the researcher; or
- The PHI data are converted to a “limited data set” as defined by HIPAA before the data are provided to the researcher, and the use of the “limited data set” is governed by a data use agreement that includes the HIPAA-required provisions; or

- The research is limited to decedents;

Note that while decedents are not included in the Common Rule definition of “human subjects,” the disclosure of their PHI by a covered entity is subject to HIPAA requirements as further described in the UNC-Chapel Hill HIPAA and Research Policy; or

- The research is limited to a “review preparatory to research.”

Note that UNC-Chapel Hill policy is that use of the “review preparatory to research” option under HIPAA (a) is limited to preparation of a research protocol or assessment of feasibility of performing a specific research protocol; and (b) does not permit recording or copying any PHI; and (c) may not be used to prescreen patients as part of the recruitment process. Such a review may be utilized only to determine the existence of potential research subjects and not to identify them or to permit a more comprehensive review of the medical record – nor may such PHI leave the health care facility during the course of the review. See below for more discussion. Once there is intent to recruit pursuant to a formulated protocol, then the research activity is sufficiently well prepared to require IRB approval. See the UNC-Chapel Hill HIPAA and Research Policy.

The health care provider, insurer or clearinghouse is responsible for HIPAA compliance in providing access or disclosure of PHI in its custody. HIPAA requires that a health care provider, insurer or clearinghouse permit access to PHI for research purposes only in accord with HIPAA’s requirements for the transaction. The UNC-Chapel Hill IRB has been designated to function as the Privacy Board when required by HIPAA for the use of PHI in research. Therefore, the IRB will review and approve the following HIPAA documentation for UNC-Chapel Hill research studies:

- Review and approval of all authorization documents used by University researchers in the informed consent process for University research.
- Review and approval of all waivers of authorization, including limited waivers of authorization, for access, use and/or disclosure of PHI for University research purposes.

The IRB’s review and approval of these HIPAA documents is within the performance of the IRB’s broader responsibilities for the protection of human research participants, including privacy and confidentiality protections beyond those required by HIPAA. Several questions in the IRB application are relevant to HIPAA but are also applicable to all studies, not just those using PHI subject to HIPAA. The IRB does not serve as the Privacy Board when HIPAA applies beyond the scope of research studies. (See SOP 29.1)

As explained above, researchers generally must obtain written authorization for the use of PHI from the human subjects who’s PHI will be included in a study. This is a separate regulatory requirement from the requirement for informed consent. The authorization document must include all elements defined in HIPAA and described in the UNC-Chapel Hill HIPAA and Research policy. The authorization document would generally be executed as a separate document from the informed consent document; however, the IRB has the discretion to accept a HIPAA-compliant

authorization that has been incorporated into the informed consent document except with respect to authorization for the access, use or disclosure of psychotherapy notes for research. For the access, use, or disclosure of psychotherapy notes, the HIPAA authorization and the informed consent must be executed as separate documents. The UNC-Chapel Hill IRB provides access to a HIPAA-compliant authorization template for the researcher to customize for the research study and submit with the application for IRB review and approval.

29.1 Procedure for signing an authorization

Adults: A competent individual, 18 years of age or older, should always sign the authorization to use or disclose his/her PHI. A person is competent if he/she has the general ability to understand the concept of release of his/her medical information. If the patient is not conscious, coherent or not competent for other reasons, a legally authorized representative must sign the authorization.

Minors: Any parent or legal guardian may sign an authorization for a minor child in his/her legal custody. Note that HIPAA does not require a child's assent for access to PHI. The individual must be provided with a copy of the signed authorization.

29.2 HIPAA waiver of authorization:

In some circumstances, authorizations for research use of PHI may be waived by the IRB, provided that the IRB determines and documents its finding that the HIPAA authorization waiver criteria, listed below, are satisfied. These waiver criteria are in addition to the criteria for waiver of research consent requirements under 45 CFR 46.116, although some of the waiver criteria overlap. A request for a waiver of authorization must be completed by the researcher and submitted to the IRB for prior review and approval. The IRB shall maintain documentation of the request and its approval. This request may be combined with a waiver of informed consent for research.

HIPAA authorization waiver criteria:

The use or disclosure of PHI involves no more than a minimal risk to the privacy of individuals, based on the presence of at least the following elements:

- An adequate plan to protect the identifiers from improper use and disclosure; and
- 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 the identifiers or such retention is otherwise required by law; and
- Adequate written assurances that the PHI will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research project, or for other research for which the use or disclosure of PHI would be permitted by the federal HIPAA policy; and
- The research could not practicably be conducted without the waiver; and
- The research could not practicably be conducted without access to and use of the PHI.

Uses or disclosures of PHI made pursuant to a waiver are subject to the “minimum necessary” rules (see University Policy, the “Minimum Necessary” Standard for Accessing, Disclosing and Requesting Protected Health Information (PHI)).