Health Information & the Law
HealthInfoLaw.org
Fast Facts June 2014

How Does the HIPAA Privacy Rule Apply to Research?

Researchers frequently create, collect, use, and/or share individually identifiable health information to conduct research. The HIPAA Privacy Rule defines research as "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge."[1] Researchers who are covered entities (health care providers, health plans, or clearinghouses) or business associates of such entities under HIPAA are subject to the HIPAA Privacy Rule.

In general, covered entities must obtain the authorization of the individual who is the subject of the protected health information (PHI) in order to use it for purposes other than treatment, payment, health care operations, and other specific uses permitted by the Privacy Rule (e.g., law enforcement, threat to health or safety). As such, covered entities generally must obtain authorization prior to using PHI for research purposes. However, covered entities may obtain a waiver of the authorization requirement if the information will be used for research purposes and if approved by an Institutional Review Board (IRB) or Privacy Board.

In order to grant a waiver (or modification) of the authorization requirement for research, an IRB or Privacy Board must be satisfied that the following criteria are met:

1. The use or disclosure of PHI involves no more than a minimal risk to individual privacy, as shown by: (A) an adequate plan to protect against improper use and disclosure; (B) an adequate plan to destroy identifiers as soon as the research purpose ends; and (C) adequate written assurances that the PHI will not be reused or disclosed to anyone else;
2. The research could not practicably be conducted without the waiver or modification; and
3. The research could not practicably be done without the PHI.

A covered entity may also disclose a limited data set for research purposes without obtaining an authorization or waiver of authorization. A limited data set is PHI from which certain identifiers have been removed, but not the full range of identifiers that make the information de-identified (and no longer PHI). If a limited data set is to be disclosed for research, a data use agreement (DUA) is required between the covered entity disclosing the information and the researcher receiving it. The DUA must outline the specific permitted uses of the PHI contained in the limited data set, including who can use the PHI, and stipulate that the information will not be re-disclosed or used other than as specified in the DUA.

Finally, note that researchers who are not covered entities or business associates under HIPAA must follow other federal and state laws that govern research activities, such as informed consent requirements and

[1] 45 CFR 164.501

guidelines for the use of human subjects, as well as any DUA governing the information in their possession, but they would not be subject to the HIPAA Privacy Rule.

For more information on limited data sets, see the Fast Facts here: http://www.healthinfolaw.org/article/fast-facts-what-limited-data-set. For more information about HIPAA, see www.healthinfolaw.org/federal-law/HIPAA.
Follow us on Twitter at ***@HealthInfoLaw.***