Health Insurance Portability and Accountability Act (HIPAA) and Research

Background on HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), along with the follow-up Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act), implemented a number of changes to the nation's health care system, including two rules that directly affect researchers: the Privacy Rule and Security Rule:

> The **Privacy Rule** requires safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. A part of the Privacy Rule deals directly with research, and specifies the conditions under which patient data can be used for research.
>
> The **Security Rule** sets standards for protecting the confidentiality, integrity and availability of electronic protected health information.

Effects of HIPAA on Research

HIPAA's definition of research is identical to that of the Common Rule: "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge." Under HIPAA, "covered entities" must manage what is called "protected health information" (PHI) in accordance with the Privacy Rule.

The Privacy Rule permits a covered entity (such as a hospital) to use or disclose PHI for research under the following circumstances and conditions, among others:

1. If the subject of the PHI has granted specific written permission through an authorization.
2. If a waiver of authorization has been granted by the Privacy Board (the Northwestern IRB serves as the Privacy Board in most instances) based on the required criteria.

A critical point of the Privacy Rule is that it applies only to individually identifiable health information held or maintained by a covered entity or its business associate acting for the covered entity. Hence, not all individually identifiable information qualifies as PHI under the HIPAA Privacy Rule. For example, individually identifiable health information that is held by a researcher (*e.g.*, information obtained directly from a consented research participant or obtained from a covered entity after a consented participant has signed an authorization allowing the sharing of information) is not PHI protected by the Privacy Rule and may be used or disclosed without regard to the Privacy Rule. That said, the research community may need to check with the covered entity before collection of any sensitive information just to verify what information is protected under the Privacy Rule.

For further guidance on HIPAA at NMHC: contact Laurel Fleming, Corporate Compliance & Integrity/Chief Privacy Executive, Northwestern Memorial HealthCare at: lflemin1@nm.org or (312) 695-9452.

Additional resources:

For more information see: NIH guidance "Institutional Review Boards and the HIPAA Privacy Rule" https://privacyruleandresearch.nih.gov/irbandprivacyrule.asp).

For FAQs regarding HIPAA and "Research Use and Disclosures" see: https://www.hhs.gov/hipaa/for-professionals/faq/research-uses-and-disclosures.

FSM General Information Security Policy for standards of protecting electronic patient, research, and other sensitive information: (http://www.feinberg.northwestern.edu/it/docs/General-Security-Policy-092216-V2-1.pdf)

For assistance in understanding the impact of HIPAA on research activities at NU, please contact the NU IRB Office at (312) 503-9338 or irb@northwestern.edu.

07/15/2017