PRIVACY REQUIREMENTS AND USE OF HEALTH DATA

Jessica Austin, University of Colorado Boulder

This check sheet contains general guidelines for working with health data, including an overview of privacy requirements under the Health Insurance Portability and Accountability Act (HIPAA) and best practices for ensuring research participant protection.

What are HIPAA and the HIPAA Privacy Rule?

The Health Insurance Portability and Accountability Act was passed by the U.S. Congress in 1996 to regulate and modernize information flow within the healthcare and health insurance industries, including how patient data is collected, stored, and protected. Specifically, the HIPAA Privacy Rule governs the use and disclosure of protected health information by covered entities. Under the Act, covered entities who disclose health data, as well as those who use the data—covered entity or not—are subject to Privacy Rule regulations.

What is a covered entity?

Covered entities (CEs) generally fall into one of three categories: health plans, healthcare clearinghouses, or medical providers. *Researchers should be aware that they may be considered part of a covered entity*. The legal organization of a university with an academic medical center, for instance, will determine whether the entire university or only the medical center is considered a CE. Many universities with medical centers are considered hybrid entities, meaning that only clinical divisions are considered CEs, while other academic units are exempt. *Remember that even if your institution or unit is not a CE, it is still subject to the HIPAA Privacy Rule if you receive data from a CE*. It is always a good idea for researchers to check with their respective compliance offices to ensure all Privacy Rule requirements are met.

What is protected health information?

Protected health information (PHI) is data held or transmitted by a covered entity that can be linked to a particular, identifiable individual. PHI data concerns health status, treatment, or payment, and personal identifiers including 18 data elements specified in the Privacy Rule (e.g., name, address, social security number). A full list can be found on page 10 of *Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule*.

Is the data I collect in my study considered PHI?

Provided that you are not a member of a covered entity, health data generated in your study is *not* considered PHI if:

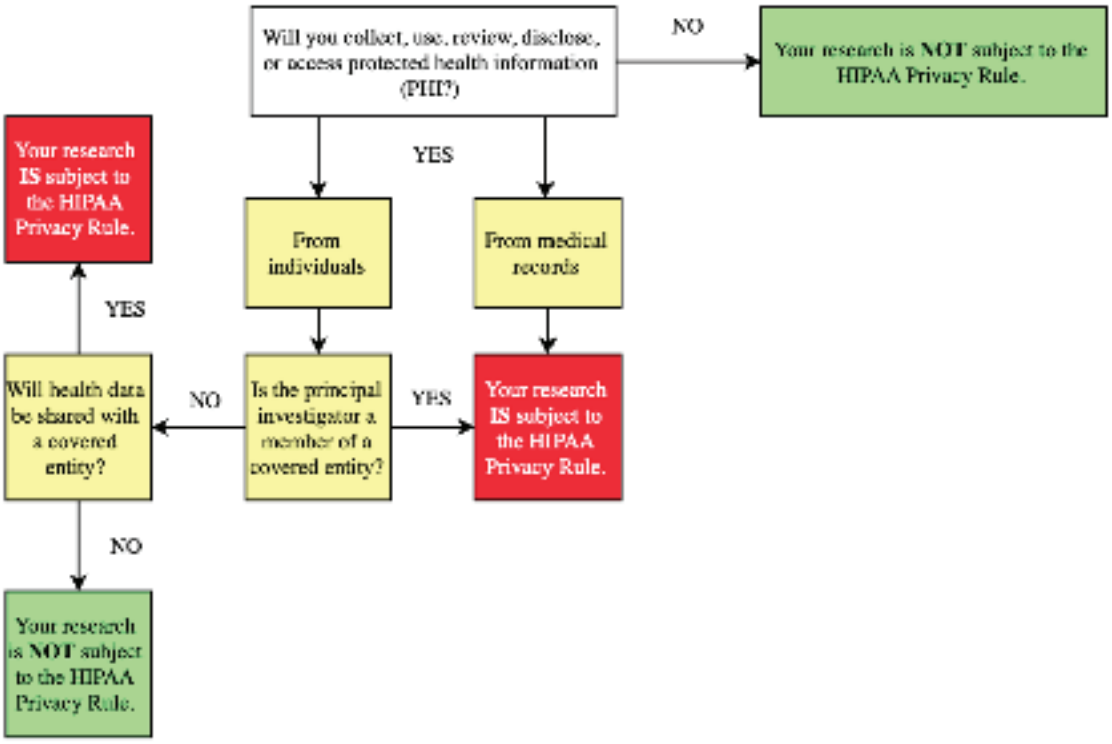
1. No health care services are administered; and
2. Participants are not billed for any treatments; and
3. Data generated by the study is not shared with participants' healthcare or insurance providers, and does not become part of the participant's medical record.

CONVERGE | Natural Hazards Center | CU Boulder
483 UCB | Boulder, CO 80309-0483 | (303) 735-5844
converge@colorado.edu | hazards.colorado.edu

Health information shared by participants in the course of your research is not considered PHI, as long as the data is not gathered in the course of clinical care or shared with a covered entity. Even if you were to gather physiological data, such as blood pressure, you are not subject to the HIPAA Privacy Rule if the data is not used or shared in the clinical context. *Remember: Connection to covered entities is what distinguishes regular health data from PHI.*

The following decision tool, adapted from the Office of the Vice Chancellor at the University of Missouri-Kansas City, will help you determine whether your research is subject to the HIPAA Privacy Rule.

Decision Tool: Is Your Research Subject to the HIPAA Privacy Rule?



If my research *is* subject to the HIPAA Privacy Rule, what are my next steps?

If you determine that your research must comply with the HIPAA Privacy Rule, or if you are unsure, you should contact your Institutional Review Board (IRB) or other human subjects oversight committee to determine the appropriate process to follow. Generally, you will fill out forms detailing your research process, subject protections, and data usage. As the IRB reviews your application, they may request further information or ask that you amend your protocol to ensure compliance. After the IRB has approved your application, they will provide you with information regarding how you must secure appropriate consent from research participants.

HIPAA regulations are enforced by the Office of Civil Rights (OCR) within the U.S. Department of Health and Human Services. If an investigation reveals that a covered entity is not in compliance, OCR may pursue corrective action with the organization to rectify the error. If violations continue, OCR may impose fines of up to $50,000.

If my research is *not* subject to the HIPAA Privacy Rule, what are my responsibilities for protecting my research participants' data?

Even if your research does not require compliance with the Privacy Rule, all human subjects research will require approval from your IRB or other similar human subjects oversight committee. As part of your IRB application, you will be required to detail how you will safeguard your participants' privacy and data. Guidance from your IRB will specify expectations for confidentiality and data protection depending on the sensitivity of the data collected. Some general best practices include:

- Storing paper forms and removable computer storage in locked cabinets.
- Locking computers with robust password protections when not in use.
- Using individual rather than group logins.
- Encrypting data when transferring between users.

REFERENCES AND ADDITIONAL RESOURCES:

National Institutes of Health. (2003). "Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule." Washington, DC: United States Department of Health and Human Services. https://privacyruleandresearch.nih.gov/pdf/HIPAA_Booklet_4-14-2003.pdf

Institute of Medicine Committee on Health Research and the Privacy of Health Information. (2009). *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research*. Washington, DC: National Academies Press. https://www.ncbi.nlm.nih.gov/books/NBK9584/

Office of Compliance, University of Wisconsin-Madison. (2019). "Researcher FAQs." Madison, WI: University of Wisconsin-Madison. https://compliance.wisc.edu/hipaa/researchers/hipaa-for-researchers-faq/

Office of the Dean for Research, Princeton University. (2019). "Best Practices for Data Analysis of Confidential Data." Princeton, NJ: Princeton University. https://ria.princeton.edu/human-research-protection/data/best-practices-for-data-a

Office of the Vice Chancellor, University of Missouri-Kansas City. (2019). "Is Your Research Covered by HIPAA's Privacy Rule?" Kansas City, MO: University of Missouri-Kansas City. http://ors.umkc.edu/research-compliance/hipaa/umkc-privacy-board

Suggested Citation: Austin, J. (2021). Privacy Requirements and Use of Health Data. CONVERGE Extreme Events Research Check Sheets Series. DesignSafe-CI. https://doi.org/10.17603/ds2-0bn5-dv59.

This series is based upon work supported by the National Science Foundation (NSF Award #1841338) and the Institute for Catastrophic Loss Reduction (ICLR). Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the NSF, ICLR, or CONVERGE.

CONVERGE | **Natural Hazards Center** | **CU Boulder**
483 UCB | Boulder, CO 80309-0483 | (303) 735-5844
converge@colorado.edu | hazards.colorado.edu