DISCLAIMER: This document has not been updated to reflect regulatory changes effective as of January 19, 2018.

HIPAA (Health Information Portability and Accountability Act) and Research at Cornell

1. Introduction

The *Standards for Privacy of Individually Identifiable Health Information* ("Privacy Rule")[1] promulgates a set of national standards for the protection of certain health information. The U.S. Department of Health and Human Services ("HHS") issued the Privacy Rule to implement the requirement of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). The Privacy Rule standards address the use and disclosure of individuals' health information—called "protected health information" — by organizations subject to the Privacy Rule — called "covered entities," — as well as for individuals to understand and control how their health information is used.

2. Protected Health information (PHI)

PHI is "individually identifiable health information" that is transmitted in any format (electronic, paper or oral) by a Covered Entity or its Business Associate. "Individually identifiable health information" is defined as health information, including demographic information that identifies the individual, and pertains to an individual's past, present, or future physical or mental health, diagnosis and/or treatment or payment for health care. PHI includes the following 18 identifiers which could be used to identify the individual or the individual's relatives, employers or household members:

- Name
- Telephone number
- Email address
- Date of birth
- Health plan ID number
- Account number
- Device identifiers and serial number
- URL
- Biometric identifiers, including fingerprints
- Address, including city and zip code
- Fax number
- Social Security Number
- Medical record number
- Dates of treatment
- Certificate/license number
- Vehicle identifiers and serial number
- IP address
- Full face photo and other comparable image

Data containing PHI becomes de-identified by removing all 18 data elements or by removing some of the data elements using documented statistical methods that result in a certification of de-identification. "De-identified" data is not considered PHI and is not subject to the requirements under the Privacy Rule.

3. Key points regarding HIPAA:

- Applies to health care providers, health plans, and health care clearinghouses. These are covered entities (CEs). If an entity does not meet the definition of a CE or business associate, it does not have to comply with the HIPAA Rules[2]. A "Business Associate" is allowed access to PHI under a contract with the CE; and is thereby subject to the same regulatory controls as a CE.
- Places responsibility on the CE to implement policies and procedures or establish criteria for the disclosure of the information. Individually identifiable health information that is collected and used ***solely for research*** is not PHI, and is therefore not covered under HIPAA.
- Places responsibility on the IRB to assure the CE that health information will be protected under the research protocol. However, approval by IRB for a particular research project does not by itself indicate that the project is HIPAA compliant(see #6 below)
- Does not replace Common Rule or FDA human subject protection regulations.
- Does not override any State Law that provides greater protection for the privacy of health information.

---

[1] The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, was enacted on Aug 21, 1996.
[2] See definitions of "business associate" and "covered entity" at 45 CFR 160.103.

HIPAA (Health Information Portability and Accountability Act) and Research at Cornell

4. Cornell Ithaca's HIPAA status

At Cornell University, the following units have been formally designated as Health Care Components and therefore part of the CE: Weil Medical College of Cornell University (WMC), WMC Health Plan, Gannett Health Services, Cornell (Ithaca) Health Plan, and the attorneys and paralegals of the University's Counsel's office. Cornell is not a CE for the purposes of research.[3]

Cornell will not agree to be a "Business Associate" (BA) of a Covered Entity for the purposes of research.

5. Access to HIPAA controlled data for Cornell research

Cornell Ithaca researchers do not have access to the protected data collected, held or transmitted by any of Cornell's CEs. Any access to such data or information will be limited to the agents of the CE and in accordance with the requirements of the Privacy Act.

Cornell Units other than those listed above must not receive or maintain PHI and provide services related to the PHI from other sources outside Cornell; because in doing so, Cornell will be deemed a BA and have to comply with HIPAA , even in the absence of a contract/Business Associate Agreement.

Cornell researchers who wish to use HIPAA-protected data can do so under the following circumstances:

i. **Limited Data Set and Data Use Agreement** provided by the CE. A Limited Data Set is PHI that excludes 16 designated categories of direct identifiers, but may still include some direct identifiers. A Limited Data Set may include date of birth, dates of treatment, and city, State or Zip Code (excluding postal address).

ii. **Activities preparatory to research** (for example, to aid in study recruitment). In this case the PHI must be used on-site. The Researcher must make oral or written representations to the CE regarding the use of the PHI and agree that the data will not be removed from the CE. To access PHI on-site, researchers must obtain IRB approval and work directly with the CE.

6. Procedures for obtaining a Limited Data Set protected under the Privacy Rule:

i. Researcher identifies need for protected data.

ii. Researcher works with Cornell's OSP (Office of Sponsored Programs) and CRADC* to initiate an application to the CE for protected data. The application must outline the project activities, the intended use of the data and a data security plan.

iii. CE provides Data Use Agreement that :
   a. Contains provisions on the permitted uses and disclosures of the data
   b. Identifies individuals permitted to use or receive the data
   c. Requires that the recipient will use appropriate safeguards to prevent the unauthorized use or disclosure of the data and will make no attempt to identify or contact the individuals

iv. Researcher submits an application to the Cornell IRB describing the use of the data, and attaches the Data Use Agreement provided by the CE with the protocol. Researcher provides IRB approval letter to OSP.

v. OSP provides executed Data Use Agreement and IRB letter of approval to the CE.

vi. CE delivers a Limited Data Set to Cornell in agreed upon manner.*

vii. The researcher follows the terms and conditions of the Data Use Agreement throughout the conduct of the research.

viii. Researcher reports any deviations or violations of the Data Use Agreement to CRADC, IRB and the OSP for determination of next steps.

*NOTE: Given the regulatory exposure and risks related to the misuse or unintentional exposure of HIPAA data, we strongly recommend that such data is delivered to and managed by Cornell CRADC. [4] The researcher should work with CRADC, OSP and the IRB throughout the process.

---

[3] http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative Simplification/HIPAAGenInfo/Downloads/CoveredEntitycharts.pdf

[4] http://ciser.cornell.edu/cradc/what_is_cradc.shtml