The Health Insurance Privacy and Portability Act of 1996 (HIPAA): The Privacy Rule

History

The HIPAA Privacy Rule is an outgrowth of The Health Insurance Privacy and Portability Act of 1996. The Final Rule, originally published in December, 2000, was implemented with an Effective Date of April 14, 2001 and a Compliance Date of April 14, 2003. The final Privacy Rule (45 CFR Parts 160 and 164) was published in August, 2002 and the first guidance from the DHHS Office of Civil Rights (OCR) became available in December, 2002. This fact sheet summarizes information on the implications of HIPAA to researchers as they are currently known; changes and refinements in interpretation are expected over time.

■ WHO WILL BE REGULATED BY HIPAA?

Most typically, HIPAA will regulate the activities of health plans, health care providers and health care data clearing houses. These persons, institutions and organizations are 'covered entities.' Covered entities may assume the form of an independent single entity, a hybrid entity, an affiliated covered entity (ACE), or an organized health care arrangement (OHCA). HIPAA does allow access to health care information for treatment, payment and health care operations.

■ WHY IS HIPAA IMPORTANT TO ME IF I AM NOT A HEALTH PLAN, HEALTH CARE PROVIDER OR HEALTH CARE DATA CLEARING HOUSE?

Even if you or your organization are not a covered entity, if you receive health care data, for example, hospital discharge data, your access to and ability to use these data may be markedly restricted under HIPAA without changes in current practice.

■ WHAT IS 'PROTECTED HEALTH INFORMATION (PHI)?'

A person's identifiable health information, including information about a person's past, present or future physical or mental health, the provision of health care, or payment for health care, that a covered entity creates (e.g., clinical trial data) or receives is termed PHI. Covered entities are required to protect the privacy of a person's PHI; this means that PHI cannot be disclosed without a person's permission except under specific circumstances. HIPAA identifies 18 elements:

PIRE
Pacific Institute for Research and Evaluation

CSN Economics and Insurance Resource Center

Pacific Institute for Research and Evaluation
11720 Beltsville Drive, Suite 900
Calverton, Maryland 20705
Phone: 301-755-2700 Fax: 301-755-2799

1. Names
2. Geographic subdivisions smaller than a state, except for the initial 3 digits of the zip code, if the unit so formed contains more than 20,000 persons.
3. All dates directly related to an individual except for the year.
4. Telephone numbers.
5. Fax numbers.
6. E-mail addresses
7. Social Security Numbers.
8. Medical Record Numbers.
9. Heath plan beneficiary numbers.
10. Account numbers.
11. Certificate/license numbers.
12. Vehicle identifiers and serial numbers, including license plate numbers.
13. Device identifiers and serial numbers.
14. Web Universal Resource Locators (URLs).
15. Internet Protocol (IP) address numbers.
16. Biometric identifiers, including finger and voice prints.
17. Full face photographic images and any comparable images.
18. Any other unique identifying number, characteristic or code.

WHAT OTHER TYPES OF HEALTH INFORMATION DATA SETS ARE DEFINED UNDER HIPAA?

- 'Limited Data Sets' retain dates, geographic identifiers except for street address and other unique identifying numbers, characteristics or codes that are not specifically excluded. Only some Privacy Rule requirements apply to limited data sets.
- 'De-Identified Data Sets' do not contain the 18 identifiers described above. The Privacy Rule does not apply to de-identified data sets.

WHAT PROVISIONS ARE ASSOCIATED WITH THE USE OF PHI AND OTHER HIPAA-DEFINED DATA SETS FOR RESEARCH PURPOSES?

- Protected Health Information
  - 'Authorization' required – individuals must be asked to consent to each use of their PHI for research purposes. The request for authorization must include who will disclose and use PHI, the purposes and duration of disclosure, notice that the authorization can be revoked and that PHI may be disclosed to individuals not subject to the Privacy Rule.
  - Waivers can be obtained from an IRB or Privacy Board under specific circumstances, triggering the 'minimum necessary' standard which limits disclosure and requiring the tracking of use and disclosure.

Pacific Institute for Research and Evaluation
11720 Beltsville Drive, Suite 900
Calverton, Maryland 20705
Phone: 301-755-2700 Fax: 301-755-2799

- Limited Data Sets
  - Neither authorization nor waiver required to use the data.
  - The 'minimum necessary' standard does not apply.
  - The user must agree to a data use agreement specifying permitted uses and disclosures and prohibiting re-identifying and/or contacting individuals.
- De-Identified Data Sets
  - HIPAA provisions do not apply, but under the Privacy Rule definition of de-identification, these data sets are often quite limited in their usefulness for research.

UNDER WHAT OTHER CIRCUMSTANCES IS AUTHORIZATION NOT REQUIRED TO ACCESS AND USE PHI FOR RESEARCH PURPOSES?

- The research is on decedents.
- The activity is preparatory, e.g., reviewing PHI to determine if it might be suitable for use in a research study.

HOW MIGHT A RESEARCH PROJECT QUALIFY FOR A HIPAA WAIVER?

- An IRB or Privacy Board determines that the use or disclosure of PHI involves no more than minimal risk to the privacy of individuals, based on, at least, the presence of the following elements:
  - An adequate plan to protect the identifiers from improper use and disclosure;
  - An adequate plan to destroy the identifiers at the earliest opportunity consistent with 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
- The research could not practicably be conducted without the waiver or alteration; and
- The research could not practicably be conducted without access to and use of the PHI

ARE THERE LEGAL PENALTIES ASSOCIATED WITH HIPAA VIOLATIONS?

Yes. The civil fine is $100 per violation to a maximum of $25K per year per violation. The criminal penalties include large fines and imprisonment up to 1 year for knowing violations and up to 10 years for violations with intent of personal gain or malicious harm.

Pacific Institute for Research and Evaluation
11720 Beltsville Drive, Suite 900
Calverton, Maryland 20705
Phone: 301-755-2700 Fax: 301-755-2799

DOES THE PRIVACY RULE SUPERCEDE THE COMMON RULE (45CFR PART 46) AND/OR STATE OR LOCAL REGULATIONS?

No. The Privacy Rule addresses health care information, now called PHI. The Common Rule addresses human subjects protection; Institutional Review Boards (IRBs) interpret and set policies in this area. Though covered entities may choose to add Privacy Rule duties to the scope of IRB activities, other covered entities may establish separate Privacy Boards. Finally, the HIPAA Privacy Rule sets a minimum level of health information protection. State and local laws may set more stringent standards for protection of PHI.

HOW WILL PSEUDO-CODING HELP ME IN THE CONTEXT OF HIPAA?

- Pseudo-coded data are not protected by HIPAA, though the privacy rule does apply to the link file that would allow identification of PHI
- Common Rule provisions typically apply to pseudo-coded data sets. Consultation with an IRB is advisable.

WHAT SHOULD I DO?

- If you believe that you or your organization may be a covered entity or one of the variants, seek legal advice from a health care attorney to clarify your status. Changes in health information handling practices will be necessary.
- If you believe that the data sources for your research or program activities are covered entities or one of the variants, contact them soon and begin to explore any changes in their practices that will impact your work.
- Consider ways in which you can continue your activities using pseudocoded, limited or de-identified data sets and propose these alternatives to your data-supplying partners. Remember, the definitions of limited and de-identified are more restrictive under HIPAA than those under the Common Rule which governs human subjects' protections.

The Children's Safety Network is offering this fact sheet to provide an overview on HIPAA's implications. Individuals and organizations are strongly encouraged to consult with a qualified health care attorney if they believe that they are a covered entity.

PIRE
Pacific Institute for Research and Evaluation

CSN Economics and Insurance Resource Center

Pacific Institute for Research and Evaluation
11720 Beltsville Drive, Suite 900
Calverton, Maryland 20705
Phone: 301-755-2700 Fax: 301-755-2799