The HIPAA Privacy Rule: Implications for CMS Proposed "Coverage With Evidence" Data Collection

May 2005

Nancy L. Perkins
Arnold & Porter LLP
nancy_perkins@aporter.com
202.942.5065

The HIPAA Privacy Rule:

Scope and Application

Covered Information

- HIPAA Privacy Rule governs:
  - (1) individually identifiable health information,
  - (2) in any form (written, electronic, oral)
  - (3) if created or received by any "covered entity."
- The Privacy Rule defines this as "protected health information" ("PHI").

Covered Entities

- Under HIPAA, covered entities include:
  (1) Health plans (HMOs, PPOs, health insurers),
  (2) Health care clearinghouses (companies that convert health data into standard formats), and
  (3) Health care providers that conduct certain insurance-related transactions electronically ("covered transactions").
- CMS is a health plan and thus is a HIPAA covered entity.

Covered Health Care Providers

- "Health care provider":

  includes any "person furnishing health care services or supplies."

- HIPAA definition of "health care":

  "*Health care*" means care, services, or supplies related to the health of an individual, including "sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription."

- Health care providers are "covered" by HIPAA only if they engage in electronic "covered transactions."

- Pharmaceutical companies generally are not "covered entities."

General Rules on Use and Disclosure

General Authorization Requirement

- Basic prohibition: Covered entities may not use or disclose PHI except:
  - (1) when the individual provides a valid written authorization; or
  - (2) pursuant to one of the exceptions specified in the Privacy Rule.
- Written authorizations must meet strict requirements.

Exceptions to Authorization Requirement

- Treatment, payment or health care operations
- Public health purposes (*e.g.*, FDA reporting)
- Law enforcement and judicial purposes
- Emergencies
- Mandatory reporting obligations (*e.g.*, child abuse)
- Medical research (which includes both clinical trials and retrospective analysis of previously collected data), but only in very limited circumstances

Exception: Treatment, Payment or Health Care Operations

- Treatment and payment exceptions apply to treatment or payment related to a specific individual – not a class or group of individuals.
- "Health care operations" include a wide variety of activities undertaken by health care providers and health plans (e.g., outcomes evaluation and development of clinical guidelines, protocol development, case management and care coordination), but *not including research*.
- Any use or disclosure of PHI must be *necessary* to conduct treatment, payment, or health care operations in order to qualify for exception.

Exception: Public Health Matters

- Under the "public health" exception, covered entities may disclose PHI to a public health authority or to a person or entity subject to FDA jurisdiction for purposes related to the quality, safety, or effectiveness of an FDA-regulated product or activity.
- Permissible purposes (non-exclusive list):
  - Collecting or reporting adverse events, product defects, or biological product deviations
  - Tracking FDA-regulated products
  - Enabling product recalls, repairs, replacement or lookback
  - Conducting post-marketing surveillance
- CMS is not a public health authority for this purpose

Limited Exception: Certain Types of Medical Research

- "Reviews preparatory to research" (*e.g.*, identifying potential trial subjects), but PHI must remain with covered entity
- Research on decedents' PHI
- Research using a "limited data set" (PHI from which almost all direct identifiers have been removed), pursuant to a written "data use agreement" between covered entity and researcher
- With an IRB or Privacy Board waiver

Options and Implications for CMS

Principal Options

- Obtain an IRB/Privacy Board waiver
- Obtain and use only de-identified data
- Obtain and use only a limited data set
- Obtain individual authorizations (*e.g.*, through informed consent)

Requirements for an IRB/Privacy Board Waiver

An IRB or Privacy Board may waive the requirement for an authorization only if it receives documentation confirming that:

- The PHI will be protected from improper use and disclosure; all identifiers will be destroyed at the earliest opportunity; and the PHI will not be reused or disclosed except (i) as required by law, (ii) for authorized oversight of the research study, or (iii) for other research for which the use or disclosure of the PHI is permitted by the Privacy Rule.
- The research could not practicably be conducted without access to and use of the PHI.
- The research could not practicably be conducted without the requested waiver.

De-Identification of Data

- To de-identify PHI information, all of the following 18 identifiers must be removed:

(1) names;
(2) geographic subdivisions smaller than a state;
(3) elements of dates (except year) for dates directly related to an individual (including birth date, admission date, discharge date, date of death, and all ages over 89 and all elements of dates (including year) indicative of such age);
(4) telephone numbers;
(5) fax numbers;
(6) electronic mail addresses;
(7) Social Security numbers;
(8) medical record numbers;
(9) health plan beneficiary numbers;
(10) account numbers;
(11) certificate/license numbers;
(12) vehicle identifiers and serial numbers;
(13) device identifiers and serial numbers;
(14) web Universal Resource Locators ("URLs");
(15) Internet Protocol address numbers;
(16) biometric identifiers, including finger and voice prints;
(17) full face photographic images and any comparable images; and
(18) any other unique identifying number, characteristic, or code.

Limited Data Sets

- A limited data set may be disclosed or used by a covered entity only pursuant to a "data use agreement" providing for protection of the data (which constitutes PHI).
- A limited data set may not contain any of the 18 specified identifiers, except;
  - (1) town, city, state, and zip code information
  - (2) dates and ages, and
  - (3) unique identifying numbers, characteristics, or codes that are not among any of the other 18 identifiers.

Individual Authorizations

A valid individual authorization must contain, among other things:

- Identification of the PHI to be disclosed or used, the person(s) authorized to disclose or use the PHI, and the person(s) who may receive it;
- Disclosure of certain rights of individual (*e.g.*, right to revoke the authorization, limits on right of access to research data);
- Description of purposes for disclosure or use – may *not* be for unspecified future research; and
- Statement that providing the authorization is not a condition of eligibility for obtaining treatment (except as part of research) or *for obtaining health care benefits*.

CMS Statements Regarding Privacy

The CMS draft guidance states that:

- "All necessary measures should be taken to ensure patient privacy. When appropriate, there should [be] institutional review and informed consent."
- "In general, we would seek to use de-identified data for all analyses, and all necessary procedures will be followed to ensure full protection of patient confidentiality."

Unanswered Questions

- Could CMS obtained IRB waivers of the HIPAA authorization requirement?
- Can de-identified data be useful for CMS?
- Could CMS reasonably identify the future research to be conducted for purposes of HIPAA privacy authorizations?
- How could CMS avoid the requirement that health care benefits may not be conditioned on obtaining an authorization?