Complying with the HIPAA Privacy Rule: Problems and Perspectives

Stacey Tovino, JD, PhD
Lehman Professor of Law
Director, Health Law Program
UNLV William S. Boyd School of Law
Roadmap

- Overview of the HIPAA Privacy Rule

- Compliance Problems and Perspectives
  - Regulatory complexity
  - Revenue generation
  - Mobile technology and portable records
The Health Insurance Portability and Accountability Act of 1996 (HIPAA)


- Administrative Simplification: HIPAA §§ 261-264

- Relevant provision: HIPAA § 264
The HIPAA Privacy Rule
45 C.F.R. Part 164, Subpart E
(45 C.F.R. §§ 164.500-.534)
Four Components of the HIPAA Privacy Rule

- What level of patient permission must be obtained before a covered entity can use or disclose a patient’s information? Look in the Use and Disclosure Requirements (45 C.F.R. 164.502 - 164.514).

- What can the patient know about his or her health information and how it has been used, and how can the patient further protect his or her information? Look in the Individual Rights provisions (45 C.F.R. 164.520 – 164.528).

- What paper-work and other administrative requirements must covered entities satisfy to help them protect the privacy of patients’ health information? Look in the Administrative Requirements (45 C.F.R. 164.530).

- To whom is a covered entity or business associate required to report certain breaches of unsecured protected health information? Look in the Breach Notification Requirements (45 C.F.R. 164.400-.414).
The Application of the HIPAA Privacy Rule
45 C.F.R. § 164.500(a)

- Who has to comply?
  - Covered entities (and now business associates)

- What information is protected?
  - Protected Health Information (PHI)
Covered Entities

45 C.F.R. §§ 160.102(a), 164.104(a), 164.500(a)

- All health plans
- All health care clearinghouses
- Those health care providers who transmit health information in electronic form in connection with a standard transaction
Individually Identifiable Health Information (IIHI)
45 C.F.R. § 160.103

- Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

- Relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

- That identifies the individual; or

- With respect to which there is a reasonable basis to believe the information can be used to identify the individual.
PHI Exclusions

- in education records protected by FERPA;
- in student treatment records excluded by FERPA;
- in employment records held by a covered entity in its role as an employer; and
- regarding a person who has been deceased for more than 50 years.
Patient Permission Requirements

1. No prior patient permission
   - Treatment 164.506
   - Payment 164.506
   - Health care operations 164.506
   - Public policy activities 164.512

2. Prior (oral) agreement 164.510

3. Prior written authorization 164.508
Compliance Problems and Perspectives

- Regulatory complexity → paper compliance
- Revenue generation → intentional or knowing breaches
- Mobile technology and portable records → negligent breaches
Ex. 1:

Disclosures of PHI for the recipient’s HCO activities
Regulation: A covered entity may disclose PHI to another covered entity for the health care operations of the entity that receives the information if:

- each entity has or has had a relationship with the individual who is the subject of the PHI being requested; and
- the PHI pertains to such relationship; and
- the disclosure is for a purpose listed in paragraph (1) or (2) of the definition of health care operations or for the purpose of health care fraud and abuse detection or compliance.

Diagram: CE1 → CE2 for CE2’s Health Care Operations if the three criteria above are met.
Ex. 2:

Marketing Uses and Disclosures
Marketing:

(1) Except as provided in paragraph (2) of this definition, marketing means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.

(2) Marketing does not include a communication made:

   (i) To provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, only if any financial remuneration received by the covered entity in exchange for making the communication is reasonably related to the covered entity’s cost of making the communication.

   (ii) For the following treatment and health care operations purposes, except where the covered entity receives financial remuneration in exchange for making the communication:

       (A) For treatment of an individual by a health care provider, including case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual;

       (B) To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; or

       (C) For case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment.
(3) Authorization required: Marketing. (i) Notwithstanding any provision of this subpart, other than the transition provisions in §164.532, a covered entity must obtain an authorization for any use or disclosure of protected health information for marketing, except if the communication is in the form of:

(A) A face-to-face communication made by a covered entity to an individual; or

(B) A promotional gift of nominal value provided by the covered entity.

(ii) If the marketing involves financial remuneration, as defined in paragraph (3) of the definition of marketing at §164.501, to the covered entity from a third party, the authorization must state that such remuneration is involved.
Ex. 3:

Law Enforcement Disclosures
45 C.F.R. § 164.512(f)(1)-(6)

1. Pursuant to process and as required by law
2. Limited information to identify and locate
3. Victims of a crime
4. Decedents
5. Crime on premises
6. Reporting crime in an emergency
Compliance Problems and Perspectives

- Regulatory complexity → paper compliance

- Revenue generation → intentional or knowing breaches
New York Hospital to Pay $2.2 Million Over Unauthorized Filming of 2 Patients

NewYork-Presbyterian Hospital has agreed to pay a $2.2 million penalty to federal regulators for allowing television crews to film two patients without their consent — one who was dying, the other in significant distress. Regulators said on Thursday that the hospital allowed filming to continue even after a medical professional asked that it stop.
When Federal Privacy Rules and Fundraising Desires Meet: An Advisory on the Use of Protected Health Information in Fundraising Communications

Purpose

This compliance advisory addresses the HIPAA Privacy Rule requirements for the use, disclosure and sharing of Protected Health Information (PHI) for fundraising communications. The Advisory assumes that the reader has an understanding of the HIPAA Privacy Rule and would benefit from an in-depth discussion of the rule’s requirements related to fundraising. The first section of the Advisory is in a Question and Answer format that provides quick answers to common questions about HIPAA requirements and fundraising. The second section is an in-depth discussion that is an excellent resource for more detailed information and includes suggested templates for communicating with patients, cites to Federal statutes and regulations, and relevant HIPAA definitions.

The information provided is meant to be advisory. Readers are advised to consider their own compliance environment and seek specific legal advice from their institution’s counsel prior to implementing the suggestions contained herein. It is also important to become familiar with your state’s requirements, which may be more stringent than those of Privacy Rule. However, a discussion of state-level privacy/confidentiality rules related to fundraising is outside the scope of this advisory.

Questions and Answers: HIPAA Privacy Requirements and Fundraising Communications
Compliance Problems and Perspectives

- Regulatory complexity ➔ paper compliance

- Revenue generation ➔ intentional or knowing breaches

- Mobile technology and portable records ➔ negligent breaches
Theft of employee iPhone results in $650,000 HIPAA fine

Most of us have lost a smartphone or tablet, but most of us aren’t carrying around patient information. And if you are going to carry PHI (protected health information) you’d better make certain that you adequately protect that data.

That’s the lesson to come out of the settlement last week between the Catholic Health Care Services of the Archdiocese of Philadelphia (CHCS) and the U.S. Department of Health and Human Services Office for Civil Rights (OCR).

The settlement includes a monetary payment of $650,000 and corrective action.
FOR IMMEDIATE RELEASE
April 22, 2014

Stolen laptops lead to important HIPAA settlements

Two entities have paid the U.S. Department of Health and Human Services Office for Civil Rights (OCR) $1,975,220 collectively to resolve potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules. These major enforcement actions underscore the significant risk to the security of patient information posed by unencrypted laptop computers and other mobile devices.

“Covered entities and business associates must understand that mobile device security is their obligation,” said Susan McAndrew, OCR’s deputy director of health information privacy. “Our message to these organizations is simple: encryption is your best defense against these incidents.”

OCR opened a compliance review of Concentra Health Services (Concentra) upon receiving a breach report that an unencrypted laptop was stolen from one of its facilities, the Springfield Missouri Physical Therapy Center. OCR’s investigation revealed that Concentra had previously recognized in multiple risk analyses that a lack of encryption on its laptops, desktop computers, medical equipment, tablets and other devices containing electronic protected health information (ePHI) was a critical risk. While steps were taken to begin encryption, Concentra's efforts were incomplete and inconsistent over time leaving patient PHI vulnerable throughout the organization. OCR’s investigation further found Concentra had insufficient security management processes in place to safeguard patient information. Concentra has agreed to pay OCR $1,725,220 to settle potential violations and will adopt a corrective action plan to evidence their remediation of these findings.
Massachusetts General Hospital will pay the U.S. government $1 million to settle what the feds are calling "potential violations of the HIPAA Privacy Rule," according to a statement issued by the U.S. Department of Health and Human Services. The case involves patient information that an employee left on the subway.

This marks the second fine related to HIPAA noncompliance in a week. The first fine, imposed on Cignet Health, was a $4.3 million civil penalty, mostly for failing to cooperate with an investigation.

The settlement follows a probe by HHS' Office for Civil Rights, which enforces HIPAA rules that require healthcare providers to protect the privacy of patient information through administrative, physical and technical safeguards.

"We hope the healthcare industry will take a close look at this agreement and recognize that OCR is serious about HIPAA enforcement. It is a covered entity's responsibility to protect its patients' health information," OCR Director Georgina Verdugo said in a statement.

The possible HIPAA violation occurred after a Mass General employee left the documents on a subway in March 2009. The documents consisted of protected health information for 192 patients of MGH's Infectious Disease Associates outpatient practice, which includes HIV/AIDS patients. The investigation found that Mass General failed to implement "reasonable, appropriate safeguards to protect the privacy of PHI" removed from Mass General's premises and disclosed, potentially violating the HIPAA rule.
Complying with the HIPAA Privacy Rule: Problems and Perspectives

Stacey Tovino, JD, PhD
Lehman Professor of Law
Director, Health Law Program
UNLV William S. Boyd School of Law