

# Fifth National HIPAA Summit West

## Accounting of Disclosures of PHI

Paul T. Smith,  
Partner,  
Hooper, Lundy & Bookman, P.C.

Hooper, Lundy & Bookman

# Accounting under the Privacy Rule

- Individuals have right to accounting of disclosures of PHI
- From written or electronic records
- Whether or not in designated record set
- Includes disclosures by business associates
- Goes back six years from request
- Includes
  - Date
  - Name of recipient, and address if known
  - Description of PHI disclosed
  - Statement of purpose of disclosure
- Must be provided within 60 days of request (with one 30-day extension)

Hooper, Lundy & Bookman, P.C.

# Accounting under the Privacy Rule

- Does not apply to disclosures:
  - For treatment, payment and health care operations (TPO)
  - To the individual
  - Incident to permitted disclosures
  - Pursuant to authorization
  - To which individual has right to object (directory, friends & family)
  - For national security or intelligence purposes
  - To correctional institutions or law enforcement custodians
  - In a limited data set

Hooper, Lundy & Bookman, P.C.

# What's Left?

- Required by law
- Public health activities
- Victims of abuse & neglect
- Health oversight activities
- Legal proceedings
- Law enforcement
- Decedents
- Disclosures in violation of the Privacy Rule
- Organ procurement
- Research
- Threat to public safety
- Military & veterans' activities
- Workers' compensation

Hooper, Lundy & Bookman, P.C.

# HHS Request for Information

May 3, 2010

The responses indicated that almost 30 covered entity respondents have received no requests for an accounting of disclosures and more than 90 covered entity respondents have received less than 20 requests since the Privacy Rule's 2003 compliance date.

76 Fed. Reg. 31428

Hooper, Lundy & Bookman, P.C.

# Accounting under the HITECH Act

- Removed the TPO exception for disclosures made through an electronic health record, but limited look-back to three years
- Required HIT Policy Committee to make recommendations on standards for technologies as part of a qualified electronic health record to allow for accounting of disclosures for TPO
- Following adoption of these standards, required HHS to publish regulations “on what information shall be collected about each disclosure”
- Regulations to take into account--
  - The interests of individuals in learning the circumstances under which their health information is being disclosed
  - The administrative burden of accounting for such disclosures

Hooper, Lundy & Bookman, P.C.

# Accounting under the HITECH Act

- Covered entity may—
  - Include disclosures by business associates, or
  - Provide contact information for business associates, in which case the business associate must provide the accounting

The term “electronic health record” means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.

Hooper, Lundy & Bookman, P.C.

# Accounting under the HITECH Act

- Compliance dates:
  - EHR acquired on or before January 1, 2009:
    - January 1, 2014
  - EHR acquired after January 1, 2009:
    - January 1, 2011
- Secretary may extend these dates up to two years

Hooper, Lundy & Bookman, P.C.



# Certification Standards

- Initial meaningful use criteria issued July 28, 2010, 75 Fed. Reg. 44590
- Recognized that “significant technical and policy challenges remain unresolved”
- Adopted a certification criterion as “optional,” to provide guidance:

*Record treatment, payment, and health care operations disclosures.*  
The date, time, patient identification, user identification, and a description of the disclosure must be recorded for disclosures for treatment, payment, and health care operations

Hooper, Lundy & Bookman, P.C.

# Certification Standards

We anticipated that a “description of the disclosure” would, at the present time, be a free text field that would have included any information that could be readily and electronically associated with the disclosure. For example, we envisioned that some descriptive information could be included such as the words “treatment,” “payment,” or “health care operations” separately or together as a general category. We also assumed that . . . EHR . . . developers could find innovative ways to associate certain electronically available information with the disclosures, such as, to whom the disclosure was made. 75 Fed. Reg. 44624.

Hooper, Lundy & Bookman, P.C.

# HIPAA Security Rule

Technical Safeguards (§ 164.312(b)):

*Standard: Audit controls.* Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

Administrative Safeguards (§ 164.308(a)(1)(ii)(D)):

*Implementation specification: Information system activity review* (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. 45 CFR 164.308(a)(1)(ii)(D).

No requirement regarding content or retention period

Hooper, Lundy & Bookman, P.C.

# Proposed Regulations

- Issued May 31, 2011
- Comment period expired August 1, 2011
- Would—
  - Modify the existing rule for written accounting
  - Add a more comprehensive “access report” for electronic data
- Would go into effect:
  - For written accounting, 240 days after publication of final rule
  - For access report:
    - EHR acquired on or before January 1, 2009:
      - January 1, 2014 (no extension)
    - EHR acquired after January 1, 2009:
      - January 1, 2013 (2-year extension)

Hooper, Lundy & Bookman, P.C.

# Proposed Regulations

- Written accounting
  - Would apply only to disclosures from designated record set
  - Would go back only 3 years
- Individual could limit it, e.g., to a particular period, type of disclosure or recipient
- Would have to be provided within 30 days (with one 30-day extension)

Hooper, Lundy & Bookman, P.C.

# Proposed Regulations

Would apply to disclosures in red--

- Required by law
- Public health activities
  - Except child abuse
  - Unless required by law
- Victims of abuse & neglect
- Health oversight activities
- Legal proceedings
- Law enforcement
- Disclosures in violation of the Privacy Rule
  - Unless reported under data breach notification regulations
- Decedents
- Organ procurement
- Research
- Threat to public safety
- Military & veterans' activities
  - Unless required by law
- Workers' compensation
  - Unless required by law

Exceptions other than TPO would continue to apply

Hooper, Lundy & Bookman, P.C.

# Proposed Regulations

- Access Report
  - Would have to indicate who has *accessed* PHI in an *electronic designated record set* held by the CE or a BA within three years prior to the request
    - No option to provide list of business associates
    - Would affect only business associates holding designated record set
  - Would not be limited to electronic health record
  - Would include internal access (i.e., use) as well as disclosure
  - Would have to include
    - Date and time of access
    - Name of natural person, if available, otherwise entity having access
    - Description of information accessed, if available
    - Description of action if available, e.g., create, modify, access or delete
  - Would not have to include the purpose

Hooper, Lundy & Bookman, P.C.

# Proposed Regulations

The process of creating a full accounting of disclosures is generally a manual, expensive, and time consuming process for covered entities and business associates. In contrast, we believe that the process of creating an access report will be a more automated process that provides valuable information to individuals with less burden to covered entities and business associates. By limiting the access report to electronic access, the report will include information that a covered entity is already required to collect under the Security Rule.

76 Fed. Reg. 31429

Hooper, Lundy & Bookman, P.C.



# Proposed Regulations

Gives this example of an access report:

| <u>Date</u> | <u>Time</u> | <u>Name</u>  | <u>Action</u> |
|-------------|-------------|--------------|---------------|
| 10/10/2011  | 02:30 p.m.  | John, Andrew | Viewed        |

Hooper, Lundy & Bookman, P.C.

# Proposed Regulations

- Access Report
  - Would have to be in a format understandable to the individual
    - Machine readable or hard copy, as requested by individual
  - CE would have to allow individual to limit report to a specific date, time period or user
  - Would have to be provided within 30 days, with one 30-day extension
  - CE would have to provide one report free every 12 months
    - Charge for additional reports limited to reasonable, cost-based fee

Hooper, Lundy & Bookman, P.C.

# Questions?

## Speaker Contact Information:

- Paul Smith: [psmith@health-law.com](mailto:psmith@health-law.com), 415-875-8488

Hooper, Lundy & Bookman, P.C.