Risks and Trends in HIPAA Compliance

Health Care Compliance Association
Managed Care Conference
February 9-11, 2014
Scottsdale, AZ

Thomas D. Bixby
Thomas D. Bixby Law Office LLC
tbixby@tbixbylaw.com
(608) 661-4310

Topics

Breach Notification Rule

- New standards under Omnibus HIPAA Amendments
- Reporting trends

Privacy Rule

- Compliance Challenges

Administrative Simplification Transactions

- Compliance certification

Breach Notification Rule

Omnibus HIPAA Amendments

New breach notification standard

- Presumption
- Low probability of
- Compromise

Old breach notification standard

- *No presumption*
- Significant risk of
- Financial, reputational, or other harm

Omnibus HIPAA Amendments

New breach risk assessment

- Nature & extent of PHI
- Unauthorized person
- Actually acquired
- Risk mitigation

Old breach risk assessment

- Type & amount of PHI
- Recipient's obligations
- Risk mitigation

Reporting Trends

Breaches Affecting 500 or More Individuals

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. These breaches are now posted in a new, more accessible format that allows users to search and sort the posted breaches. Additionally, this new format includes brief summaries of the breach cases that OCR has investigated and closed, as well as the names of private practice providers who have reported breaches of unsecured protected health information to the Secretary. The following breaches have been reported to the Secretary:

Full DataSet CSV format (18 KB) - XML format (57 KB)

Select a column head to sort by that column. Select again to reverse the sort order. Select an individual record to display it in full below the table.

Filter: 736 records showing

Name of Covered Entity	State	Individuals Affected	Date of Breach	Type of Breach	Location of Breached
1st response Medical Transpot Corp.	MD	552	06/15/2012-10/01/2012	Unauthorized Access/Disclosure	Desktop Computer
ABQ HealthPartners	NM	778	2012-12-20	Theft	Laptop
Accendo	AZ	175,350	2011-01-01	Unauthorized Access/Disclosure	Paper
Access Counseling, LLC	IN	566	2013-08-23	Theft	Laptop
Access Medical Group	PR	7,606	2012-01-11	Theft	Laptop
ACO of Puerto Rico	PR	5,000	03/05/2013 - 07/16/2013	Unauthorized	Network Server

Reporting Trends

Must report to HHS "in manner specified"

- Name of covered entity (and business associate)
- Date of breach & number of affected people
- Categories of type of breach
- **Brief description of the breach**
- Date for notice of breach
- Attestation

Reporting Trends

Total breaches reported (500 or more)

- 2009: 51
- 2010: 212
- 2011: 159
- 2012: 167
- 2013: 145 (as of December 31)
- 2013 about the same as 2012 from 9/23 – 12/31

Reporting Trends

Brief description of breach

- Overall: 13% have some brief description
- 2010: 34%
- 2011: 7%
- 2012: 1%
- 2013: <1%

Privacy Rule

Compliance Challenges

Deficit Reduction Act of 2005

State Medicaid Programs (vendors)

Third-party liability request for data

- Entire eligibility file (*i.e.* all members)
- Multiple states
- Multiple data elements
- Multiple years
- Ongoing data production

Deficit Reduction Act of 2005

Requires* third party to:

- Accept Medicaid right of assignment;
- Accept claims submitted within 3 years of service;
- Disclose information about eligible individuals

Deficit Reduction Act of 2005

All premised on: SSA § 1902*

(a) A State plan for medical assistance must [provide]—

. . . .

(I) that the State shall provide satisfactory assurance to the Secretary that the State has in effect laws requiring health insurers . . . as a condition of doing business in the State, to:

(i) provide, with respect to individuals who are eligible [for Medicaid], [eligibility] information . . . in a manner prescribed by the Secretary;

** 42 U.S.C. § 1396a(a)(25)(I).*

Deficit Reduction Act of 2005

Disclose for DRA request if:

- **State law specifically requires disclosure of:**
  - Entire eligibility file;
  - Requested data elements.
- **If request is from another State:**
  - State law applies to out-of-State insurers;
  - State has jurisdiction

FSAs, HRAs, and HSAs

Claim integration with FSAs, HRAs, HSAs

- Submit claims to administrator for FSA/HRA/HSA reimbursement

Application of Privacy Rule?

- Permissible disclosures?
- Business associate relationships?

FSAs, HRAs, and HSAs

FSAs & HRAs

- Group health plans
- Subject to HIPAA—covered entities

Disclosure for payment activities

- Minimum necessary *(claims of members enrolled in both plans)*
- Administrator is business associate of FSA/HRA

FSAs, HRAs, and HSAs

Implications for self-funded account

- Same responsibilities as for major-medical plan

Implications for insured account

- FSA/HRA not insurance contract
- Group health plan that must meet *all* Privacy Rule requirements

FSAs, HRAs, and HSAs

Health Savings Account

- Personal account (*i.e.*, 401(k))
- Not sponsored or controlled by employer
- Not a health plan (or business associate)

No disclosure to administrator permitted

- Except pursuant to written authorization
- No business associate relationship

Administrative Simplification Compliance Certification

ACA Certification of Compliance

Certify by 12/31/2013 with respect to:

- Eligibility for a health plan transactions;
- Claims status transactions;
- Remittance advice transactions (including EFT transactions)

Health plan *fully* complies with applicable:

- Transactions Rule standards (implementation guides)
- Operating Rules

ACA Certification of Compliance

Certification must:

- Cover business associates;
- Include “end-to-end” testing with trading partners

Severe penalties for non-compliance

- Failure to file: $1/covered life/day **(maximum $20/covered life)**
- Fine doubles for inaccurate or incomplete certification

Certification Process

As of 12/31/2013 . . .

- No Rule;
- No proposed rule;
- No guidance on how to certify compliance

Notice of Proposed Rulemaking

- Published 1/2/2014
- Proposed deadline for certification now 12/31/2015

Proposed Certification Process

Outsource process to CAQH-CORE

- Committee on Operating Rules for Information Exchange
- Established operating rules adopted by HHS
- Nonprofit alliance of health plans, clearinghouses, trade assocs

Reporting based on *Health Plan Identifier*

- Controlling health plans (by 11/5/2014)
- Certification not applicable to subhealth plans

Proposed Certification Process

Submission requirements

- Number of covered lives
- Attestation of compliance
- Evidence of end-to-end testing

Submission covers Business Associates

Must submit to HHS 1/1/2015-12/31/2015

Two Certification Options

CORE Certification Seals

- CORE Pledge (attestation of compliance)
- Compliance with all CORE (including non-HIPAA) standards
- Complete testing by CORE-authorized vendor

HIPAA Credential

- Attestation of compliance
- Testing with trading partner >30% of transactions
- Must list up to 25 trading partners (name, e-mail, phone)

Medicare Compliance Program Audit Proposal

Questions?

Thomas D. Bixby
Thomas D. Bixby Law Office LLC
tbixby@tbixbylaw.com
(608) 661-4310