VENABLE® LLP

The Road Map to HIPAA Compliance: What Your Nonprofit Needs to Know

Thursday, August 8, 2013, 12:30 p.m. – 2:00 p.m. ET
Venable LLP, Washington, DC

Moderator:
Jeffrey S. Tenenbaum, Esq., Venable LLP
Panelists:
Thora A. Johnson, Esq., Venable LLP
Kelly A. DeMarchis, Esq., Venable LLP
Jennifer Spiegel Berman, Esq., Venable LLP

VENABLE LLP

Upcoming Venable Nonprofit Legal Events

August 21, 2013 – The IRS Final Report on Nonprofit Colleges and Universities: Lessons for All Tax-Exempt Organizations

September 18, 2013 – Keeping Up with Technology and the Law: What Your Nonprofit Should Know about Apps, the Cloud, Information Security, and Electronic Contracting

VENABLE® LLP

Agenda

- Overview of HIPAA
- Privacy Rule
- Notice of Breach
- Security Rule
- Business Associates & Business Associate Agreements
- Notice of Privacy Practices
- Training
- Next Steps
- Q&A

VENABLE LLP

Overview of HIPAA

Evolution

- Health Insurance Portability and Accountability Act of 1996 ("HIPAA")
  - Privacy Rule (April 2003)
  - Standard Electronic Transactions – to achieve a more efficient health care system (October 2003)
  - Security Rule (April 2005)
- Health Information Technology for Economic and Clinical Health Act of 2009 ("HITECH")
  - Notification of Breach (February 2010)
  - Final Omnibus Rule

VENABLE LLP

Overview of HIPAA

Final Omnibus Rule

- Published in Federal Register – January 25, 2013
- Effective Date – March 26, 2013
- Compliance Date – September 23, 2013
- Transition Period – Up to September 22, 2014 for Certain Contracts

VENABLE® LLP

Overview of HIPAA

Final Omnibus Rule

- Privacy & Security
  - Marketing
  - Sale of protected health information (PHI)
  - Fundraising
  - Right to request restrictions
  - Electronic access
  - Business Associates
- Notice of Breach
- Enforcement
- GINA
- Other
  - Notice of privacy practices (NPP)
  - Research
  - Decedents
  - Student immunizations

Overview of HIPAA

Glossary

- Covered Entity
  - Health care provider who bills, etc. using electronic medium
  - Health Plan (public or private, self-insured or insured)
  - Clearinghouse (billing service, repricing company, etc.)
  - Medicare Prescription Drug Plan Sponsors
- Business Associate
  - Entity that creates, receives, maintains, or transmits PHI on behalf of a covered entity
  - Enumerated service providers (*e.g.*, lawyers, actuaries & consultants)
  - Subcontractors

VENABLE LLP

Overview of HIPAA

Glossary

- Protected Health Information ("PHI")
  - Individually Identifiable Health Information
    - Health information, including demographic information
    - Relates to past, present, or future physical or mental health condition, provision of healthcare, or payment for provision of healthcare, and
    - Does or may identify the individual
    - In any form (oral, written or electronic)
  - In the possession of a covered entity or business associate

Overview of HIPAA

Compliance Package

- Privacy and security policies and procedures
- Designation of privacy and security officers
- Business associate agreements
- Training
- Notice of privacy practices
  - Only applies to covered entities

VENABLE LLP

Overview of HIPAA

Statutory Penalties

Violation Due to:	Penalty Range (per violation):
Unknown cause	$100-$50,000
Reasonable cause and not willful neglect	$1,000-$50,000
Willful neglect (violation corrected within 30 days)	$10,000-$50,000
Willful neglect (violation not corrected within 30 days)	At least $50,000

A $1.5 million annual cap applies for violations of an identical privacy or security requirement.

VENABLE LLP

Overview of HIPAA

Resolution of Agreements

- Five Resolution Agreements and Corrective Action Plans Negotiated in 2012 ($4.85 million)
- Two Resolution Agreements and Corrective Action Plans Negotiated in 2013 ($450,000)
- Expect continued growth and emphasis on significant cases – remain small proportion of all the cases OCR reviews
- Enforcement of compliance with new provisions after September 2013 – continue to enforce with respect to existing provisions not subject to change

From the U.S. Department of Health and Human Services, Office for Civil Rights

Overview of HIPAA

Audit Program

- Completed audits of 115 entities
  - 61 Providers, 47 Health Plans, 7 Clearinghouses
- Total 979 audit findings and observations
  - 293 Privacy
  - 592 Security
  - 94 Breach Notification
- Small entities struggle with all three areas
- Help identify compliance areas of greatest weaknesses
- Evaluation underway to guide OCR in making audit a permanent part of enforcement efforts

From the U.S. Department of Health and Human Services, Office for Civil Rights

VENABLE LLP

The Privacy Rule

The Use and Disclosure of PHI

- PHI can be used/disclosed for treatment, payment and health care operations
- PHI can be used/disclosed for any purpose pursuant to a valid authorization
- PHI can also be used/disclosed for certain other purposes consistent with policy objectives
  - *e.g.*, public health activities, law enforcement, otherwise required by law
- Generally subject to minimum necessary standard

VENABLE LLP

The Privacy Rule

Restrictions on Marketing

- Marketing = a communication about a product or service that encourages recipients to purchase or use the product or service
- Authorization required
- Exceptions
  - A promotional gift of nominal value provided by a covered entity
  - A face-to-face communication made by a covered entity to an individual
  - Refill reminders (and similar communications) if remuneration does not exceed cost to the individual
  - No remuneration

VENABLE LLP

The Privacy Rule

Restrictions on the Sale of PHI

- Sale of PHI
  - Includes remuneration received directly or indirectly from entity to whom PHI is disclosed
  - Not limited to financial remuneration
- Requires an authorization that states that the entity is being paid to sell PHI
- Excludes
  - Research, or other permitted disclosure, if remuneration is limited to a reasonable cost-based fee to cover the cost to prepare and transmit PHI; or
  - Fee is otherwise expressly permitted by law

VENABLE LLP

The Privacy Rule

Fundraising

- Fundraising for the covered entity is part of "health care operations"
- Covered entities and any institutionally-related foundation can use the following to raise funds:
  - Demographic patient information
  - Dates of service
  - Treating physician information
  - Department of service information*
  - Outcome information*

* Use is limited to permit filtering

VENABLE LLP

The Privacy Rule

Fundraising

- Must disclose opportunity to opt-out of fundraising in notice of privacy practices
- Notice of privacy practices MUST be provided prior to receiving a fundraising solicitation of any type
- Each solicitation (oral or written) must contain opt-out information
  - Must be "clear and conspicuous"
- Opt-out mechanism cannot impose a burden on the recipient
- *Simple, quick and inexpensive*
  - Requiring mailing a letter to opt-out IS not permitted

VENABLE LLP

The Privacy Rule

Fundraising

- Covered entity may not condition treatment or payment on individual's decision
- Must have a system to track and apply opt-outs
  - Covered entity must honor opt out (no further fundraising communications permitted)
- Flexibility provided in scope of opt out and method to opt back in is permitted

VENABLE® LLP

The Privacy Rule

Right to Request Restrictions / Alternative Communications

- Individuals can request that covered entities and business associates disclose PHI in an alternative method, and they can restrict disclosure of their PHI
- For alternative methods, covered entities and business associates are generally required to comply
- For requested restrictions, covered entities and business associates are generally NOT required to comply, except where an individual requests a restriction on:
  - Disclosure of PHI to a health plan for purposes of payment or operations (not treatment)
  - Where the PHI relates to an item/service for which the provider has been paid in full out of pocket

VENABLE LLP

The Privacy Rule

Right to Request Restrictions / Alternative Communications

- Must have system that accommodates requests in a timely manner
- Potential problem areas
  - What if the check bounces?
  - Can provider collect full balance before providing services?
  - What does the patient have to tell the provider?
  - Does this apply to Medicare?
  - Can the patient pick and choose what is restricted?
  - Part of a bundled service?

VENABLE LLP

The Privacy Rule

Right to Access / Amend

- Individual may inspect/obtain copies of their own PHI in a designated record set
- If patient asks for his/her PHI in a particular electronic format, covered entity MUST provide it if possible
- Must provide copies to designated third party upon receipt of written request
- State laws limit per page charges, but HIPAA limits charges to cost of compliance
- Individuals may also request that inaccurate PHI be amended

VENABLE LLP

The Privacy Rule

Right to an Accounting of Disclosures

- Currently an individual has a right to an accounting of disclosures going back 6 years, but subject to multiple exceptions, including disclosures made for treatment, payment and health care operations
- New HITECH rule will require electronic disclosures for prior 3-years to be included in accounting (no exception for treatment, payment or health care operations)
  - Delayed effective date, awaiting guidance

VENABLE LLP

Notice of Breach

Federal and State Requirements

- Most state laws have breach notification statutes for personal information, but few cover health data
- HHS Omnibus Rule finalizes (with amendments) nationwide breach notification standards for PHI
- Federal Trade Commission issued similar notification rule for:
  - Vendors of “personal health records”
  - Related entities such as advertisers on vendors’ sites
  - Third party servicers to vendors and related entities
- For “dual role” entities, either HHS or FTC rule applies depending on role in which organization suffered breach

Notice of Breach

Overview

- Notification to certain parties is required following discovery of a breach of "unsecured" PHI
- "Unsecured" = not rendered unusable, unreadable, or indecipherable to unauthorized persons under HHS guidance, currently:
  - Encryption
  - Destruction

VENABLE LLP

Notice of Breach

Whom to Notify

- Business associate notifies covered entity
  - May notify individuals if arranged with covered entity
  - Must provide certain information about breach
- Covered entity notifies:
  - Individuals
  - HHS Secretary
    - Same time as individuals if 500 or more individuals (will be posted online)
    - Annual log if fewer than 500 individuals
  - Media notice, for breach involving more than 500 residents of jurisdiction

VENABLE LLP

Notice of Breach

What Is a "Breach"?

- Acquisition, access, use or disclosure of PHI
  - Not permitted by HIPAA Privacy Rule
  - And compromises the security or privacy of the PHI
- If the HIPAA Privacy Rule is violated, a breach is presumed unless the covered entity or business associate demonstrates low probability of compromise based on risk assessment of:
  - Nature and extent of PHI
  - Unauthorized person involved
  - Whether PHI was actually acquired or viewed
  - Extent of risk mitigation

VENABLE LLP

Notice of Breach

What Is Not a "Breach"?

- Unintentional acquisition, access or use by workforce member, if in good faith and within scope of authority, and no further use or disclosure (*i.e.*, not snooping)
- Inadvertent disclosure to a colleague who is also authorized to access PHI, and no further use or disclosure
- Disclosure where there is a good faith belief that the unauthorized person was not reasonably able to retain the information

VENABLE LLP

Notice of Breach

Notice to Individuals

- To individuals (or their representatives) whose information is reasonably believed to have been accessed, acquired, used or disclosed without authorization
- Use plain language
- Include certain required information (*e.g.* description of breach, dates, types of information involved)

VENABLE LLP

Notice of Breach

Notice to Individuals

- Provide via:
  - First-class mail
  - E-mail if individual has agreed
  - If insufficient contact information, substitute notice via telephone or media
  - Urgent telephone notice in some cases
- Translation to other languages or formats if required

VENABLE LLP

Notice of Breach

When to Notify

- "Without unreasonable delay" and no later than 60 days after "discovery of breach" (even if investigation is ongoing)
- Clock starts for a business associate breach depending on relationship:
  - For independent contractor, 60 days from notification to covered entity
  - For agent, 60 days from business associate's own discovery
- Law enforcement delay is possible

Notice of Breach

When is a Breach "Discovered"?

- "Discovery" means first day on which breach is known or by exercising reasonable diligence would have been known to any employee, officer, or agent
- Organization should have in place:
  - Systems for detecting breach
  - Training and policies to ensure that breaches are reported to management by any employee

The Security Rule

- Electronic PHI ("ePHI"): PHI transmitted by or maintained in an electronic media
  - Including hard drive, disk, CD and internet
  - Excluding paper fax
- Must ensure confidentiality of ePHI and protect against reasonably anticipated threats
- 18 Standards (*i.e.*, safeguards): administrative, physical, technical
- 36 Implementation specifications: some mandatory, others "addressable"

VENABLE® LLP

The Security Rule

Administrative Safeguards

- Policies & procedures
- Personnel designations
- Risk analysis & management plan
- Access control & management
- Training

VENABLE® LLP

The Security Rule

Physical Safeguards

- Workstation use & security
- Control access to facility
- Device & media controls

VENABLE LLP

The Security Rule

Technical Safeguards

- Access authorization; screensavers; encryption
- Audit controls
- Integrity measures; virus scans; firewalls
- Authentication through password management
- Transmission security

VENABLE LLP

The Security Rule

Risk Analysis

- Review data
  - Type of data
  - Storage location
  - Persons with access
  - Access procedures
  - Audit logs
  - Encryption
- Gap Analysis
- Implement appropriate security measures

VENABLE® LLP

Business Associates & BAAs

New Rules for Business Associates

- Business Associates must comply with the Security Rule's technical, administrative, and physical safeguard requirements
- Business Associates must comply with use or disclosure limitations expressed in its contract and in the Privacy Rule
- Business Associate definition includes Health Information Organizations, E-prescribing Gateways, others who perform data transmission services requiring access to PHI on a routine basis, and PHR vendors providing services to covered entities
- Subcontractors of a Business Associate are now defined as Business Associates
  - Business Associate liability flows to all subcontractors

VENABLE LLP

Business Associates & BAAs

Timing Considerations

- Final HIPAA/HITECH rules were effective on March 26, 2013.
- By September 23, 2013, Business Associates have to meet all obligations under new rules, except:
  - If an existing BAA was in place prior to 1/25/2013 and the agreement was not renewed prior to 3/25/2013, the parties have until 9/22/2014 to modify the BAA.

VENABLE® LLP

Business Associates & BAAs

Updating Business Associate Agreements

- Identify existing agreements and any gaps
- Review existing terms
- Update for final rules

VENABLE® LLP

Notice of Privacy Practices

- Must be maintained and distributed by covered entities
- Describes
  - Use and disclosure of PHI
  - Individual rights
  - Legal duties regarding PHI

Notice of Privacy Practices

Key Changes

- NPP must include:
  - Purposes that require authorization (sale of PHI, marketing, and psychotherapy notes)
  - Right to opt out of receiving fundraising communications
  - Requirement to agree to restrict disclosure of health information to health plan if individual pays out of pocket in full (providers only)
  - Right to receive notice of breach
  - Genetic information may not be used for underwriting purposes (health plans that underwrite only)

VENABLE LLP

Training

- Workface members with access to PHI must be trained on HIPAA privacy & security policies and procedures
- Best practices:
  - Formal training on an annual basis
  - Updates/refreshers as needed
- Document:
  - Attendees
  - Date/time of training
  - Subject of training

VENABLE LLP

Next Steps

- Perform a risk analysis
- Review and revise policies and procedures
  - Don't forget to also update any HIPAA forms (*e.g.*, notice of breach assessment forms)
- Update/negotiate business associate agreements
- Adopt systems to detect breach and Incident Response Plan
- Train workforce
- Update notice of privacy practices
  - Only applies to covered entities

VENABLE® LLP

Questions?

Jeffrey S. Tenenbaum, Esq.
jstenenbaum@Venable.com
t 202.344.8138

Kelly A. DeMarchis, Esq.
kademarchis@Venable.com
t 202.344.4722

Thora A. Johnson, Esq.
tajohnson@Venable.com
t 410.244.7747

Jennifer Spiegel Berman, Esq.
jsberman@Venable.com
t 410.244.7756

To view Venable's index of articles, presentations, and upcoming programs on nonprofit legal topics, see www.Venable.com/nonprofits/publications, www.Venable.com/nonprofits/recordings, www.Venable.com/nonprofits/events.

VENABLE® LLP