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
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
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
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
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
Overview of HIPAA

Statutory Penalties

<table>
<thead>
<tr>
<th>Violation Due to:</th>
<th>Penalty Range (per violation):</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown cause</td>
<td>$100-$50,000</td>
</tr>
<tr>
<td>Reasonable cause and not willful neglect</td>
<td>$1,000-$50,000</td>
</tr>
<tr>
<td>Willful neglect (violation corrected within 30 days)</td>
<td>$10,000-$50,000</td>
</tr>
<tr>
<td>Willful neglect (violation not corrected within 30 days)</td>
<td>At least $50,000</td>
</tr>
</tbody>
</table>

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

- Company 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”
The Security Rule

Administrative Safeguards

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

Physical Safeguards

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

Technical Safeguards

- Access authorization; screensavers; encryption
- Audit controls
- Integrity measures; virus scans; firewalls
- Authentication through password management
- Transmission security
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
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.
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.
Business Associates & BAAs

Updating Business Associate Agreements

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

Peter P. Parvis
410.244.7644
ppparvis@venable.com

Thora A. Johnson
410.244.7747
tajohnson@venable.com

Julia Kernochan Tama
202.344.4738
jatama@venable.com

Jennifer S. Berman
410.244.7756
jsberman@venable.com
the road ahead for ABC CORPORATION
WHAT YOUR BUSINESS NEEDS TO DO ABOUT HIPAA—NOW

Whether you are an employer that provides health insurance for your employees, a business in the growing healthcare industry, a hospital, or other medical provider—or you provide services to any of those entities—you need to know about changes to the privacy and security rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which were made by the final omnibus HIPAA rule issued by the U.S. Department of Health and Human Services (HHS) on January 25, 2013 (the Final Regulations). These Final Regulations implement changes made under the Health Information Technology for Economic and Clinical Health Act (HITECH). Nearly every business in the healthcare industry (and the businesses providing services to those businesses) is affected by these changes.

Among other things, the Final Regulations:

- Directly subject Business Associates, including their Subcontractors (or “downstream” Business Associates), to the HIPAA security rule and many aspects of the HIPAA privacy rule.
- Require amended Business Associate Agreements between Covered Entities and Business Associates to reflect the changes made by the Final Regulations and, for the first time, Business Associate Agreements between Business Associates and their Subcontractors.
- Require Covered Entities to notify affected individuals, the federal government and the media (in certain circumstances) of any “breach” of Unsecured PHI.
- Expand an individual’s right to receive electronic copies of his or her PHI and restrict disclosures to a health plan concerning treatment for which an individual has paid out of pocket in full.
- Permit additional categories of PHI to be used in fundraising, enhance the limitations on the use of PHI for marketing, and prohibit the sale of PHI without individual authorization.
- Significantly strengthen the authority of the federal government to enforce the HIPAA privacy and security rules.

Below is a list of action items for Covered Entities and Business Associates to consider in preparing for the compliance deadline (generally, this September 23). Following the list of action items is a more detailed summary of the changes made by the Final Regulations. Venable’s HIPAA Task Force is hard at work assisting its clients in implementing the new requirements outlined in this alert, and looks forward to answering your HIPAA compliance questions. Look for an invitation regarding a webinar on the Final Regulations in the near future.

1 Key capitalized terms are defined in the Glossary at the end of this article.
Action Items for Covered Entities and Business Associates (including Subcontractors)

Except for updating “grandfathered” Business Associate Agreements, Covered Entities and Business Associates, including Subcontractors, have until September 23, 2013 to come into compliance with the Final Regulations. To do so, Covered Entities and Business Associates, including Subcontractors, must:

- Review their current privacy and security compliance program;
- Enter into, or amend, as appropriate, Business Associate Agreements to reflect the Final Regulations;
- Educate Business Associates (including Subcontractors), as necessary, about their responsibility (and the responsibility of their Subcontractors) to safeguard PHI so as to mitigate chances of agents causing upstream liability;
- Conduct a HIPAA security risk analysis and prepare/update a risk management plan. As part of this process, consider implementing encryption and destruction technologies in order to minimize the risk that PHI will be considered Unsecured PHI and, thus, able to be “breached;”
- Create processes to discover breaches of Unsecured PHI.
- Prepare/update a policy about how to handle breaches of Unsecured PHI;
- Draft/update the other HIPAA security and privacy policies;
- Update forms to reflect changes to individual rights;
- Conduct HIPAA training on the updated policies; and
- Update and distribute a Notice of Privacy Practices, as applicable.

Delayed Compliance Deadline for Grandfathered Business Associate Agreements

If a compliant Business Associate Agreement was in place before January 25, 2013, and it is not otherwise renewed or amended after March 25, 2013 (i.e., it is a “grandfathered Business Associate Agreement”), then it generally does not need to be updated to comply with the Final Regulations until September 22, 2014. Agreements that renew automatically through evergreen clauses qualify for this extended compliance date.

Changes Impacting Business Associates (including Subcontractors)

Business Associates, including Subcontractors, will be directly liable (and not simply contractually liable pursuant to their Business Associate Agreements) for complying with certain provisions of HIPAA, including:

- All of the administrative, physical, and technical standards of the HIPAA security rule in the same manner as Covered Entities.
- The use and disclosure requirements of the HIPAA privacy rule in the same manner as Covered Entities.

CAUTION: As of September 23, 2013, entities that create, receive, maintain, or transmit PHI on behalf of a Business Associate (in other words, Subcontractors) will be required to comply with all of the HIPAA provisions that apply to Business Associates because they will, in fact, be treated as Business Associates under the Final Regulations.

Moreover, Covered Entities can be held directly liable for the acts and omissions of their Business Associates that are acting within the scope of their agency. Importantly, this is the case even if the act or omission violates a provision of the Business Associate Agreement. For this purpose, the Final Regulations rely on the federal common law of agency (rather than potentially disparate state laws). An agency relationship is established where a Covered Entity has the right or authority to control its Business Associate’s conduct in the course of performing a service on behalf of the Covered Entity. Similarly, Business Associates can be held directly liable for the acts and omissions of their Subcontractors.

As such, care will need to be taken as Business Associate Agreements are updated or put in place. Where a Business Associate is acting as a Covered Entity’s agent, consideration should be given to whether indemnification provisions are appropriate.
Covered Entities and Business Associates Must Provide Notice of a Breach Involving “Unsecured” PHI

Since September 23, 2009, Covered Entities have been required to notify affected individuals within 60 days after a “breach” of Unsecured PHI is discovered. (A breach is deemed “discovered” on the first day that the “breach” is known or should reasonably have been known.) Covered Entities are also required to provide notice to HHS and, in certain circumstances, to the local media.

The threshold for determining whether an unauthorized use or disclosure of PHI constitutes a “breach” for this purpose will change as of September 23, 2013. Under interim final breach notification rules, the security and privacy of Unsecured PHI is deemed to be “breached” where the unauthorized use or disclosure of such information poses a significant risk of financial, reputational or other harm to the individual or individuals whose PHI was compromised.

As of September 23, 2013, the unauthorized acquisition, access, use or disclosure of Unsecured PHI will be presumed to be a breach for purposes of the breach notification rule, unless it can be demonstrated that there is a “low” probability that the PHI has been compromised. While certain exceptions apply to this rule, it is likely to increase the frequency with which potential breaches are reported.

CAUTION: State law may also require notice of certain breaches of health-related information. Additionally, entities that are not considered Covered Entities or Business Associates subject to HIPAA (and this notice requirement), but who maintain personal health records for consumers, are subject to Federal Trade Commission rules requiring them to provide similar notices of breaches involving such personal health records.

Individual Rights and Obligations Related to the Use and Disclosure of PHI

Rights of Individuals to Access Their PHI in Electronic Format

If an individual requests an electronic copy of his or her PHI that is maintained electronically (whether or not in an electronic health record), the Covered Entity must provide the individual with access to the electronic information in the electronic format requested by the individual. If the requested format is not readily producible, the PHI can instead be provided in a readable electronic form as agreed to by the Covered Entity and the individual. Individuals making such a request may be charged for certain (but not all) labor costs and supplies for creating the electronic media (for example, the physical media, such as a CD or USB), if the individual requests that the electronic copy be provided on portable media. The interaction of these rules with permissible charges under state law must be considered.

Mandatory Compliance with Restrictions Requested on Certain Disclosures of PHI

Health care providers must comply with an individual’s request for restrictions on the disclosure of his or her PHI if:

- The disclosure would otherwise be made to a health plan;
- The disclosure is for the purposes of carrying out payment or health care operations and is not otherwise required by law; and
- The PHI pertains solely to a health care item or service for which the health care provider has been paid in full by the individual or person other than the health plan on the individual’s behalf.

The Use of PHI in Fundraising and Marketing, and the Sale of PHI

The Final Regulations made significant changes to the rules regarding fundraising, marketing, and the sale of PHI.

The Final Regulations now permit the use of additional categories of PHI in the fundraising activities of Covered Entities. Specifically, Covered Entities may use department of service, treating physician and outcome information for their fundraising purposes. Fundraising communications (whether in person, over the phone, or written) must, however, provide individuals with clear and conspicuous instructions on how to opt out of receiving future fundraising solicitations. A Covered Entity’s Notice of Privacy Practices must be reviewed to ensure that it includes a statement that an individual has a right to opt out of receiving fundraising communications.

Covered Entities and Business Associates are prohibited from using or disclosing PHI without authorization—even if for treatment and health care operations—where the Covered Entity (or Business Associate) receives direct or indirect payment for such use or disclosure. HIPAA’s marketing restrictions have certain exceptions, including a communication made to provide refill reminders or otherwise communicate about current prescriptions where any financial remuneration received is reasonably related to the cost of making the communication.
Finally, the sale of PHI is prohibited unless an authorization is provided.

**Using or Disclosing the “Minimum Necessary” PHI**

With certain exceptions, Covered Entities and Business Associates must use “reasonable efforts” to limit their uses or disclosures of, or requests for, PHI to the minimum amount that is necessary to accomplish the intended purpose. Under HITECH, a Covered Entity is automatically deemed to comply with the minimum necessary standard if it limits its use and disclosure of PHI to a “limited data set”—which is essentially de-identified information, except that dates relating to the individual (such as birth dates and dates of hospital admission and discharge) can be included. The Final Regulations provide no further guidance on this issue, but promise it in the future.

**Rights of Individuals to Get Enhanced Accounting of Disclosures of Electronic PHI**

HITECH requires that Covered Entities that use or maintain an electronic health record will need to account for disclosures of electronic PHI for the purpose of treatment, payment, and health care operations. (Accountings for disclosures of non-electronic PHI do not need to include disclosures for treatment, payment, and health care operations.) Individuals will have the right to request an accounting of all such disclosures made in the three-year (rather than the otherwise applicable six-year) period prior to the accounting request. The Final Regulations did not address this requirement, which will not be effective until final regulations are issued on the accounting rules.

**Significantly Enhanced HIPAA Enforcement Provisions**

HITECH considerably increased the civil monetary penalties that may be assessed under HIPAA against Covered Entities and (now) Business Associates. Specifically, penalties for violations are determined with a tiered approach:

<table>
<thead>
<tr>
<th>Violation Due To:</th>
<th>Penalty Range (per violation):</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown cause</td>
<td>$100-$50,000</td>
</tr>
<tr>
<td>Reasonable cause and not willful neglect</td>
<td>$1,000-$50,000</td>
</tr>
<tr>
<td>Willful neglect (violation corrected within 30 days)</td>
<td>$10,000-$50,000</td>
</tr>
<tr>
<td>Willful neglect (violation not corrected within 30 days)</td>
<td>At least $50,000</td>
</tr>
</tbody>
</table>

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

The Final Regulations revised the factors that can be considered in determining the penalty amount and amended the definition of reasonable cause. For purposes of assessing penalties, any act or omission that a Covered Entity or Business Associate knew, or by exercising reasonable diligence would have known, violated the HIPAA privacy or security rules will be deemed to be a violation due to reasonable cause, provided the Business Associate did not act with willful neglect.

HITECH requires HHS to perform periodic audits of Covered Entities and Business Associates to ensure that they are complying with the HIPAA privacy and security rules. Under the Final Regulations, when a preliminary review of the facts in either a compliance review or a complaint investigation indicates a possible violation due to willful neglect, HHS must conduct a review to determine whether the Covered Entity or Business Associate is in compliance. HHS may conduct investigations in other circumstances in its discretion. Additionally, HHS is no longer required to resolve investigations or compliance reviews through informal means, meaning that in certain circumstances, HHS may assess penalties without negotiating with impacted Covered Entities and/or Business Associates.

Although not part of the Final Regulations, HITECH also gives state attorneys general the ability to bring civil actions on behalf of residents of their states, and clarifies that an individual who obtains or discloses PHI from a Covered Entity without authorization may be subject to criminal prosecution for a violation of HIPAA.
If you have any questions about this alert, please contact one of the members of the HIPAA Task Force.

Constance H. Baker  
chbaker@Venable.com  
410.244.7535

Jennifer Spiegel Berman  
jsberman@Venable.com  
410.244.7756

Nora E. Garrote  
negarrote@Venable.com  
703.760.1983

Todd Gustin  
tgustin@Venable.com  
410.244.7870

Thora A. Johnson  
tajohnson@Venable.com  
410.244.7747

Jessica E. Kuester  
iekuester@Venable.com  
410.244.7476

Celia E. Landgren  
celandgren@Venable.com  
410.244.7781

Kishka Ford McClain  
kmclain@Venable.com  
703.760.1610

Peter P. Parvis  
ppparvis@Venable.com  
410.244.7644

Ted L. Ramirez  
tramirez@Venable.com  
202.344.4622

Davis V.R. Sherman  
dvsherman@Venable.com  
410.244.7810

Ryan M. Sweigard  
rmsweigard@Venable.com  
410.244.7559

Julia Kernochan Tama  
jktama@Venable.com  
202.344.4738

Kishka Ford McClain  
kmclain@Venable.com  
703.760.1610

Brenda J. Tranchida  
bjtranchida@Venable.com  
410.244.7537

HIPAA Glossary

The world of HIPAA includes a vocabulary of its own. Key terms to aid in your understanding include:

**Business Associate**

Generally, a person or entity that performs functions or activities on behalf of, or certain services for, a Covered Entity that involve the use or disclosure of PHI.

Examples include third party administrators, pharmacy benefit managers, claims processing or billing companies, and persons who perform legal, actuarial, accounting, management, or administrative services for Covered Entities and who require access to PHI. They also include certain information technology providers, health information organizations, most entities that provide data or document transmission and storage services with respect to PHI to a Covered Entity, and Subcontractors that create, receive, maintain, or transmit PHI on behalf of a Business Associate.

**Business Associate Agreement**

A contract between a Covered Entity and a Business Associate or between a Business Associate and a Subcontractor that governs each party’s rights and obligations under HIPAA. Business Associate Agreements are required under the privacy rule.

**Covered Entities**

Health care providers that transmit health information in electronic form in connection with certain transactions; health plans (including employer-sponsored plans); and health care clearinghouses.

We specifically note that employers who sponsor self-insured group health plans will need to take the action items noted in this article on behalf of their health plans. For employers who sponsor fully-insured group health plans, the majority of these obligations will ordinarily fall on the insurance carrier.

**Protected Health Information or PHI**

Generally, “individually identifiable health information” that is transmitted or maintained in any form or medium, with limited exceptions. “Individually identifiable health information” includes demographic and health information that relates to an individual’s health conditions, treatment or payment and can reasonably be used to identify the individual.

**Subcontractor**

Generally, a person to whom a Business Associate delegates a function, activity, or service. A Subcontractor becomes a Business Associate under HIPAA when it creates, receives, maintains or transmits PHI on behalf of the Business Associate when performing such delegated function, activity, or service.

**Unsecured PHI**

PHI that is not rendered unusable, unreadable, or indecipherable to an unauthorized person through encryption or destruction, pursuant to guidance published by HHS.

©2013 Venable LLP. Attorney Advertising. This information is published by the law firm Venable LLP. It is not intended to provide legal advice or opinion. Such advice may only be given when related to specific fact situations that Venable has accepted an engagement as counsel to address.
Responsibility, Liability Change for HIPAA Business Associates

The Health Insurance Portability and Accountability Act (HIPAA) is a federal law that protects health information that can identify patients (protected health information or PHI). New regulations, which became effective on March 26, 2013 but have a delayed compliance date of September 23, 2013 (with some exceptions), significantly modified the HIPAA rules. It is important to understand these revised regulations because your clients, and maybe even you, may now be subject to HIPAA.

Who is Affected?

Under HIPAA, “covered entities,” i.e., health plans, health care clearinghouses, and most health care providers, must comply with HIPAA to protect the privacy of PHI and implement safeguards to ensure the confidentiality, integrity, and availability of electronic PHI (e-PHI). HIPAA allows covered entities to disclose PHI for enumerated purposes without patient authorization, including disclosures to “business associates.” Business associates are generally understood as entities that perform certain functions or activities on behalf of, or certain services for, a covered entity involving the use or disclosure of PHI. The modified rules expand the definition, responsibilities, and liability of business associates and their contractors. Whether a business associate is new to HIPAA or must re-evaluate its current compliance efforts in light of this new exposure, significant compliance costs will likely result.

Expanding the Business Associate Reach

On March 26, 2013, many entities that may be unfamiliar with HIPAA became business associates. Under the modified rules, the term now includes persons that provide data transmission services with respect to PHI to a covered entity if they “require access on a routine basis” to such PHI. The regulations specifically include health information organizations (which oversee and govern the exchange of health-related information among organizations) and e-prescribing gateways as business associates, but the reach is even broader. Any entity that provides data transmission services that include PHI for a covered entity will be a business associate unless it can meet the narrow “mere conduit exception.” This exception, for entities that transport PHI but do not access the information other than on a random or infrequent basis, was intended to exclude only those entities providing “mere courier services” (e.g., the US Postal Service or United Parcel Service) and their electronic equivalents (e.g., internet service providers providing mere data transmission services or telecommunications companies).

Similarly, entities that “maintain” or store PHI for a covered entity are now business associates, even if the entities do not view the PHI or only do so randomly or infrequently, because of their “persistent,” as opposed to “transient,” opportunity to access PHI. As a result, all data and document storage companies maintaining PHI on behalf of covered entities and business associates (in hard copy or electronic) are themselves business associates.
Subcontractors Too?

Additionally, all subcontractors of business associates, i.e., those to whom a business associate has delegated a function, activity, or service that the business associate agreed to perform for a covered entity, are now business associates if such work involves the creation, receipt, maintenance, or transmission of PHI. And, subcontractors of subcontractors are business associates. For example, a document destruction company that shreds documents containing PHI for a business associate is a subcontractor to the business associate and, therefore, a business associate itself. Additional changes make patient safety organizations and certain vendors of personal health records business associates.

More Agreements

As a result of these changes, more entities must comply with HIPAA both directly (through the rule’s new expanded liability provisions) and contractually (through what is known as business associate agreements or BAAs). HIPAA requires covered entities to obtain satisfactory assurances in the form of a contract or other arrangement (i.e., the BAA) that its direct business associates will appropriately safeguard the PHI at issue. These contracts must include many requirements set forth in the regulations. Direct business associates of covered entities must now obtain BAAs with their subcontractors, and so on as long as PHI continues to flow to entities down the chain.

Expanded Liability

In addition, all business associates, whether historically treated as such or newly so under the modified rules (including subcontractors), are now directly liable under certain HIPAA provisions, including for impermissible uses and disclosures of PHI under HIPAA’s Privacy Rule and for failing to comply with HIPAA’s Security Rule (which imposes several requirements to protect e-PHI). They also must disclose PHI as the Secretary requires for investigations and compliance audits, must make reasonable efforts to limit uses or disclosures of, or requests for, PHI to the minimum necessary, and must provide notification of breaches of unsecured PHI to covered entities. The government now can impose significant civil monetary penalties on business associates for violations. Anyone in the PHI chain can be liable in accordance with the federal common law of agency for violations based on the act or omission of any of their agents, including subcontractors, acting within the scope of their agency.

This content originally appeared in the April 15, 2013 Bar Bulletin.
Ten Things to Know About Modified Rules

If you determined that you and/or your client are business associates subject to the Health Insurance Portability and Accountability Act (HIPAA) under the final rules, here are ten things you must know about HIPAA.

• **What does HIPAA protect?** HIPAA controls uses and disclosures of protected health information (PHI) by covered entities and business associates. A covered entity includes health care clearinghouses, health plans (including employer-sponsored health plans), and health care providers that electronically transmit health information in connection with certain transactions, including billing. PHI is health information that (a) is created or received by a health care provider, health plan, employer, or health care clearinghouse; (b) relates to an individual’s physical or mental health or condition or the provision of or payment for health care; and (c) identifies or may identify an individual. There are exclusions, including workers compensation, FERPA, and employment records held in a covered entity’s role as an employer.

• **How does HIPAA impact health information that I receive in a lawsuit?** Just because a lawyer receives patient information pursuant to a subpoena or patient authorization does not necessarily subject the lawyer to HIPAA. Lawyers become HIPAA business associates by receiving PHI from covered entity clients to provide legal services.

• **Am I subject to everything in HIPAA?** No. Business associates are directly liable under HIPAA for failing to comply with the Security Rule and certain portions of the Privacy Rule (including impermissible uses, breaches, and disclosures of PHI). They are not directly obligated to do everything in the Privacy Rule, including having a Notice of Privacy Practices and a Privacy Officer. While business associates may not be directly required to have policies and procedures and to train their workforce on the Privacy Rule, they may need to do so under contract or as a practical matter to prevent impermissible uses and disclosures.

• **What is the HIPAA Security Rule?** The Security Rule establishes standards to protect electronic PHI (e-PHI) that is created, received, used, or maintained by a covered entity and, now, a business associate. These entities must ensure the confidentiality, integrity, and availability of e-PHI; identify and protect against reasonably anticipated threats to the security or integrity of the information; protect against reasonably anticipated impermissible uses or disclosures; and ensure compliance by their workforce. Among other requirements, an entity must have a Security Officer, adopt policies and procedures, and conduct a thorough assessment of the risks and vulnerabilities of its e-PHI.

• **What is the HIPAA Privacy Rule?** The Privacy Rule sets limits on the uses and disclosures of PHI with and without patient authorization and gives patients rights over their PHI (e.g., to be informed about a covered entity’s uses of PHI, to have access to, and
request corrections of, health information, to get their own information, and to request an accounting of the disclosures of PHI by covered entities or business associates).

- **What do I do if PHI is used or disclosed improperly?** If there is a “breach” of “unsecured” (i.e., unencrypted or not destroyed) PHI, covered entities must notify individuals and the government (and the media if the breach is large enough). If a breach occurs at the business associate level, business associates must notify affected covered entities. With certain exceptions, a breach is an unauthorized use or disclosure of PHI in a manner that compromises its security or privacy. Under recently revised rules effective this September, a breach is presumed unless an entity demonstrates a low probability that the PHI has been compromised through a risk assessment.

- **Is HIPAA a one size fits all rule?** No. HIPAA recognizes the great variability in covered entities and business associates. The Security Rule has several “addressable” specifications with which compliance is unnecessary if an entity documents why implementation is not reasonable and appropriate. (In such cases, the entity can adopt alternative measures.) Entities also can consider factors, including size, complexity, capabilities, and resources, in determining which security measures are appropriate to satisfy Security Rule obligations. The government also recognizes that size is a factor in the Privacy Rule.

- **What goes into a Business Associate Agreement (BAA) and where can I find one?** HIPAA regulations set forth required elements of BAAs. For example, BAAs must establish business associates’ permitted and required uses and disclosures of, and provide that business associates will not use or further disclose, PHI other than as permitted or required by the contract or by law. Business associates can create their own BAAs, but the government has provided sample language at www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html.

- **What are the penalties for violating HIPAA?** The government can impose civil monetary penalties ranging from $100 to $50,000 per violation, depending upon culpability, with a cap of $1.5 million for identical violations during a calendar year. Penalties cannot be imposed for violations not due to willful neglect that are corrected within 30 days. Criminal penalties can be assessed for knowingly obtaining or disclosing or selling PHI in violation of HIPAA.

- **Although I may have many obligations, what should be my first steps?** Business associates should assess their weaknesses in storing, transmitting, and using PHI. Lost laptops and briefcases and poor electronic security pose the biggest risks. Although encryption is not required, we recommend encrypting all portable electronic devices, including laptops, computers, and phones. Start with the required analysis and add training and common sense.

This content originally appeared in the April 15, 2013 Bar Bulletin.
EMPLOYEE BENEFITS AND EXECUTIVE COMPENSATION

QUICK FACTS

More than a dozen attorneys dedicated to employee benefits/executive compensation issues including:

- two former legislation counsels to the U.S. Congress’s Joint Committee on Taxation
- a former IRS attorney
- a former Social Security Administration attorney

HONORS AND AWARDS

Maryland Employee Benefits & Executive Compensation (Band 1), Chambers USA, 2013

Ranked in 2012-2013 U.S. News-Best Lawyers “Best Law Firms”

VENABLE: COMPREHENSIVE SUPPORT FOR DECISION MAKING

The rules governing employee benefit programs have become so incredibly complex that it’s the rare organization that can handle them on its own. We can help you meet that challenge. We bring specific employee benefits skills and experience in addition to related regulatory, tax and political know-how, all seasoned with a healthy dose of practical reality.

Our job is to help you solve problems and to make you look good.

 EMPLOYEE BENEFITS AND EXECUTIVE COMPENSATION

leaders in all aspects of benefits planning

We know what you deal with every day. We understand what you go through in applying arcane rules to the benefits and retirement savings of real people.

We help you design integrated benefit packages—piecing together all types of retirement plans with health plans, life/disability insurance, education assistance and work-balance programs—that fit your business goals and the culture of your organization.

When parts of your package need approvals by regulatory agencies, we take the lead in obtaining the clearances you need.

As you install the plan, we’re with you all the way—to transform the documents into a straightforward and practical system that you and your staff can manage with ease. As laws and regulations change, we’ll take the lead in making amendments that keep you in compliance. And should you decide to terminate or freeze a plan, we can assist you with that as well.
But organizations are always changing. Suppose you’re a business that needs to make a reduction in force.

We have designed window plans and other strategies that comply with tax, ERISA and ADEA requirements to achieve the clients’ goals. For example, when an international credit card company decided on a major reduction in force, we helped the consultants design the severance packages and worked with the actuaries to amend the company’s defined benefit plan to provide for early retirement subsidies. We also designed and assisted with the implementation of several forms of employee communications for multiple categories of employees covered by differing plan terms.

Or perhaps you’re a business that is looking to acquire other companies.

For several clients, we are regular members of the acquisition team—performing due diligence, negotiating acquisition agreements, writing proxy disclosures, harmonizing the targets’ benefits plans into the company’s structure and designing severance plans for employees who are terminated in connection with the acquisitions.

Interest rates are falling. Pension costs are rising. You need to control your liabilities.

For a consortium of grocery store chains, we crafted changes in the funding rules that apply to multi-employer pension plans. We helped guide the proposal through two House committees, two Senate committees, House and Senate floor action, and a very protracted House-Senate conference. With approval of the rule changes, the employers experienced significant reductions in costs.

While changes in multi-employer funding may not directly apply to your business, they are an example of the innovative thinking available at Venable to companies that are struggling with the escalating costs of employee benefits.

“Doing a fine job, this deep team is commended for its sophisticated and nationally informed practice.”
— Chambers USA, 2008

You’re a nonprofit already sponsoring—or thinking about starting—a 457 plan.

Our Employee Benefits and Executive Compensation attorneys have particularly deep knowledge about the specialized—and often arcane—rules that apply to nonprofits and governmental employers. We structure deferred-compensation plans and other innovative programs that supplement retirement savings, so that governments and nonprofits can attract and retain key employees. Recently, we’ve counseled clients on the final 403(b) regulations and current trends in 457 plans that may impact the design and operation of an organization’s retirement plan.

You’ve read that the Department of Labor is cracking down on disclosure issues.

That’s correct. As the Pension Protection Act of 2006 kicks into gear, the Department of Labor will be looking into what employers are disclosing to employees about how well their plans are doing. Expect greater scrutiny of fiduciary oversight of investments and the costs of plan administration. That’s likely to be followed by a wave of litigation involving fiduciary responsibility.

We’re preparing Venable clients for the onslaught—with refresher courses on fiduciary duties, due diligence and oversight, plus preventive measures that can help ensure they won’t run afoul of the new rules.

You’re aware of the push for greater transparency for executive compensation.

As advisors to boards of directors and compensation committees, we help develop and negotiate employment agreements, incentive compensation and other performance-based programs. With the disclosure rules in mind, we design plans that address all necessary reporting issues, whether these arise under the Sarbanes-Oxley Act of 2002, SEC mandates, stock exchange regulations or state “blue sky” rules.

Our Employee Benefits and Executive Compensation attorneys have a diversified national practice. We assist clients of all shapes and sizes—businesses in virtually every industry sector, 501(c)(3)s and governmental entities under 414(d)—on compensation and benefit-related issues.

We care, we listen, we become advocates for your interests. And we respond quickly.
We’ll bring you several approaches to solve the problem—and lay out the advantages and the costs of each option. Not just legal solutions, but plans made by applying know-how and business judgment to what will work best for your organization.

How can we help you? To find out, please contact us at 1.888.VENABLE or www.Venable.com.
HEALTHCARE

legal solutions that make business sense

Venable has been advising healthcare clients for more than 60 years. Our mission is to provide legal solutions that accomplish your business objectives.

To enable that mission, we draw on many disciplines within Venable—business formation and transactions, regulatory, government affairs and public policy, mergers and acquisitions, creditors’ rights, real estate, litigation, tax, employee benefits, technology/intellectual property, labor and employment and antitrust—for the experience and knowledge clients require in making sound business decisions.

EXPERIENCE ON ALL SIDES OF HEALTHCARE

We understand your goals and the priorities of everyone you deal with.

QUESTIONS WE HEAR OFTEN

How do we get what we need from federal and state government?

Healthcare is the most heavily regulated industry in America. The Patient Protection and Affordable Care Act of 2010 (ACA) represents a complete sea change (including potential opportunities) for clients and the agencies and industries that affect them. We have decades of experience dealing with agencies such as FDA, CMS, OIG and IRS. Venable lawyers have helped write and shape the laws. We know the legislators and regulators, as well as where and how to promote action.
How do we join or form a multi-hospital affiliation or joint venture?
Whatever the structure you believe will promote your business objectives, especially in the evolving context of the ACA, such ventures present significant business and legal risks. Hospitals considering any form of affiliation or joint venture should thoroughly assess the governance options and clinical acceptability, regulatory permissibility and financial viability of the venture.
Venable has performed healthcare mergers, acquisitions and affiliations of many types and understands how to address the unique business and regulatory issues that confront the institution and physicians involved.

Are we complying with Stark, Fraud and Abuse, False Claims Act and HIPAA?
Compliance is becoming even more of a challenge. The rules governing Stark and other laws continue to evolve as the agencies issue new regulations, new cases are tested in the courts, and the government reaches new settlements. The Stark rules alone cover thousands of pages, and new IRS disclosure rules may trigger significant audits. The ACA introduces further requirements for compliance plans and practices.
Ensuring that you are in compliance requires ongoing reviews of the financial relationships within and between your organization and outside parties.
Venable helps clients comply with Stark, Fraud and Abuse, False Claims Act, HIPAA and other parallel state laws by:
- preparing legal analyses of new financial relationships and implications;
- performing legal audits of existing contracts and financial relationships;
- developing compliance programs and performing in-depth training on related policies and specific vulnerabilities or areas of noncompliance; and
- representing clients in investigations and litigation related to allegations of violation of laws.

How do we obtain, use or restructure tax-exempt financing?
Venable has represented many hospital, healthcare and educational systems in tax-exempt financings, including advising hospitals on the currently difficult credit markets. Venable’s public finance attorneys provide workable solutions to meeting the requirements—“safe harbor” guidelines, the private business test, TEFRA hearings and other rules—that are required for tax-exempt bond financing.

How do we address patient care and ethical issues—such as clinical trials, privacy issues, reproductive rights, informed consent, AIDS, advance directives and guardianship?
In every area of healthcare, from neonatal clinics to hospice facilities, ethical issues in patient care have gained heightened public awareness and increased potential for costly legal actions by patients and their families. Venable attorneys bring legal and practical approaches to these ethical challenges.

How do we handle compliance with medical staff bylaws, hearings and reporting requirements in physician peer reviews?
Since the 1950’s, Venable has represented hospitals and other providers in a broad variety of disputes and disciplinary actions. We apply that experience daily as we counsel and represent clients confronted with threats to the integrity and reputation of the institution.
Venable provides:
(1) Attorneys who understand healthcare economics and its intimate connections with regulatory rules and enforcement policies;
(2) Advice that is practical—based on our experience working with providers, payors and regulators every day; and
(3) Solutions that work within the realities of healthcare—enhanced by knowledge of national, regional and local government, public policy and the business environment.

How can we help you? To find out, please contact us at 1.888.VENABLE or www.Venable.com.
PRIVACY AND DATA SECURITY

MANAGING THE RISKS OF COLLECTING AND USING DATA

For every major corporation, data privacy and security loom as critical elements of risk management. While other law firms are assembling teams to address some of the issues, no other firm has the type of experienced team we have—a team that is already providing coordinated solutions to the business, operations and legal aspects of gathering and protecting information about consumers, customers, employees and others.

MANAGING ALL THE PIECES

our integrated approach to data privacy

Policy knowledge reinforced by hands-on operational experience.

The experience our attorneys bring to clients mirrors the interwoven relationship between privacy law and the practical challenges faced by companies charged with the responsibility of collecting and protecting information.

Our work combines advice on broad policy questions and specific solutions to everyday industry problems. We offer both front-edge knowledge of the thinking of legislators and regulators and first-hand experience solving the issues that confront the executives of electronic commerce, financial services and communications companies.

Our policy work enhances our operational advice, and vice versa. We combine legal theory and practical know-how in an integrated approach to complex privacy and security issues.

When trouble strikes, we know how to deal with it.

Venable attorneys have years of experience defending clients in enforcement actions by regulatory authorities and mounting challenges to agency regulations, as well as litigating privacy issues and defending clients in class-action lawsuits.

With the increased risks and costs of privacy breaches, we place particular emphasis on issues involving the acquisition, aggregation and national and international transfer and use of personal data. For example, we have represented:

• **retailers, financial institutions and marketers** in connection with credit card and other data security breaches;
WHAT WE DO
Advice on legal compliance and risks
Defense in investigations or civil suits
Forecasts and analyses of the impact of legislative/regulatory proposals
Input at the product development stage
Investigations of privacy breaches
Privacy reviews and audits
Representation before Congress on data security, Social Security number privacy and similar issues

INDUSTRY FOCUS
Electronic publishing
Entertainment
Financial services
Healthcare
Hospitality
Marketing
Retail
Telecommunications
Transportation

- a personal Web page services provider in the Federal Trade Commission’s first case alleging failure to adhere to a privacy policy describing the use and disclosure of registration and other consumer information;
- trade associations seeking to strike down financial privacy regulations issued by the FTC, the Securities and Exchange Commission and the federal banking agencies pursuant to the Gramm-Leach-Bliley Act and challenging the national “Do Not Call” registry and related FTC telemarketing regulations;
- a major cable television company in class-action suits filed under the privacy provisions of the Cable Act;
- the Direct Marketing Association in connection with legislation and regulations concerning numerous marketing issues related to new communications technologies;
- various clients in matters pending before the Department of Homeland Security;
- a health services marketer in connection with the requirements of the Health Information Portability and Accountability Act related to pharmaceutical discount cards; and
- a global provider of Internet services on criminal compliance matters.

Because data privacy is a global issue, we operate globally.
Many of our clients collect and protect data in Canada, Latin America, Asia and the European Union. Therefore, we regularly meet with international regulators and have developed a specialist network of data protection lawyers in more than 20 countries.

Making your views known to legislators and regulators.
We are in constant contact with policy makers in the United States, where our work has had an impact on privacy and information security laws and regimes such as:
- Bank Secrecy Act and anti-money-laundering rules;
- Behavioral advertising;
- CAN-SPAM ACT;
- Children’s Online Privacy Protection Act;
- Communications Assistance for Law Enforcement Act;
- European Union Data Protection Directive;
- Fair Credit Reporting Act;
- Federal Right to Financial Privacy Act;
- Gramm-Leach-Bliley Act provisions on privacy and security of customer information;
- Health Insurance Portability and Accountability Act;
- IRS information disclosure rules;
- Office of Foreign Assets Control;
- Telecommunications Act;
- USA PATRIOT Act;
- Use of Social Security numbers; and
- U.S.-EU Safe Harbor Agreement.

Venable attorneys also help draft and implement self-regulatory programs and standards for trade associations. We are the long-standing privacy counsel to the Direct Marketing Association.

Our combined experience—mastering the intricacies of compliance with a maze of federal laws, defending clients in regulatory actions and guiding the data and privacy aspects of corporate mergers and alliances—enables us to respond quickly when new issues arise in any client’s business.

How can we help you? To find out, please contact us at 1.888.VENABLE or www.Venable.com.
Thora A. Johnson
Partner
Baltimore, MD Office

T 410.244.7747 F 410.244.7742 tajohnson@Venable.com

Thora Johnson focuses on tax-exempt organizations, employee benefits and executive compensation matters. She advises clients on the establishment and operation of tax-exempt organizations, including private foundations, public charities, trade associations, and title holding companies. She also counsels clients on the establishment and operation of qualified and non-qualified deferred compensation plans and health and welfare benefit plans. She routinely reviews and drafts employee benefit plans, summary plan descriptions, and other employee communications and negotiates vendor contracts. She regularly works with clients to structure comprehensive compliance programs and procedures to comply with the privacy and security requirements of HIPAA. She has broad expertise in health plan compliance, including ERISA, the Internal Revenue Code, HIPAA (privacy and portability), and PPACA. She has been helping employers navigate health care reform from its enactment in March 2010, and is a frequent speaker and writer on the topic.

REPRESENTATIVE CLIENTS
Ms. Johnson represents, among others, Allegis Group, Bank of America Corporation, General Dynamics Corporation, and Greater Baltimore Medical Center.

HONORS
Recognized in the 2013 edition of Legal 500, Employee Benefits and Executive Compensation
Recognized in the 2013 edition of Chambers USA (Band 2), Employee Benefits and Executive Compensation, Maryland
Recognized in the 2012 edition of Chambers USA (Band 2), Employee Benefits and Executive Compensation, Maryland
Recognized in the 2011 edition of Chambers USA (Band 2), Employee Benefits and Executive Compensation, Maryland
Recognized in the 2010 edition of Chambers USA (Up and Coming), Employee Benefits and Executive Compensation, Maryland

ACTIVITIES
Ms. Johnson is a member of the Maryland State Bar Association and its Study Group for Employee Benefits, as well as the Tax Section of the District of Columbia Bar, the Tax Section of the American Bar Association, and the American Health Lawyers Association. She also regularly assists in pro bono matters involving charitable organizations and employee benefits. She is a trustee of the Friends School of Baltimore and has served as a director of a local charity whose mission is to help individuals find and keep entry-level, nonprofessional jobs.
PUBLICATIONS

- July 2013, What Your Nonprofit Needs to Do about HIPAA – Now
- May 2013, What Your Business Needs to Do about HIPAA – Now, Employee Benefits and Executive Compensation Alert
- April 2013, Patient Protection and Affordable Care Act: The Impact on Employers
- April 2013, Association Health Plans and Health Care Reform: A Trap for the Unwary
- April 2013, Ten Things to Know about Modified Rules, Bar Bulletin
- March/April 2013, Health Coverage under the Affordable Care Act: What You [and Your Clients] Need to Know, Maryland Bar Journal
- January 2013, Limited Relief for Employers under Health Care Reform’s “Play-or-Pay” Rules, Employee Benefits and Executive Compensation Alert
- October 2012, Health Care Reform: Large Employers and the New Health Insurance Exchanges, Employee Benefits and Executive Compensation Alert
- September 2012, Private Exchanges: You Have Questions, We Have Answers, Employee Benefits and Executive Compensation Alert
- September 2012, Don’t Play and Also Pay: What Nonprofit Employers Need to Know about Navigating the Employer-Sponsored Health Coverage Mandate
- September 2012, Don’t Play and Also Pay: What Independent Schools Need to Know About Navigating the Employer-Sponsored Health Coverage Mandate, Independent School Law Alert
- September 2012, Don’t Play and Also Pay: Navigating the Employer-Sponsored Health Coverage Mandate, Employee Benefits and Executive Compensation Alert
- April 2012, New Health Plan Rules to Keep in Mind When Planning for the 2013 Open Enrollment Season, Employee Benefits and Executive Compensation Alert
- June 2011, Health Care Reform: June 30 Compliance Deadline Fast Approaching, Employee Benefits and Executive Compensation Alert
- April 2011, Health Care Reform: Form W-2 Reporting of Employer-Provided Group Health Coverage, Employee Benefits and Executive Compensation Alert
- March 2011, Health Care Reform: Another Extended Grace Period, Employee Benefits and Executive Compensation Alert
- November 2010, Year-End Wrap-Up for Benefit Plans, Employee Benefits and Executive Compensation Alert
- October 2010, Interview, “Changes to group health plans: Strictly adhere to new regs or lose time and money,” Nonprofit Business Advisor
- October 2010, Extended Grace Period Available (What internal claims procedures apply now?), Employee Benefits and Executive Compensation Alert
- September 2010, New Federal External Claims Review Procedures (What does a health plan have to do?), Employee Benefits and Executive Compensation Alert
- August 2010, New Preventive Care Coverage Rules Under Health Care Reform, Employee Benefits and Executive Compensation Alert
- August 2010, Material Changes Now, More Material Changes Coming, Employee Benefits and Executive Compensation Alert
- July 2010, Grandfathered Status For Your Group Health Plans Under Health Care Reform: What is at Stake?, Employee Benefits and Executive Compensation Alert
- July 2010, Highlights of the New “Patient’s Bill of Rights” Regulations Implementing Key Features of Federal Health Reform, Employee Benefits and Executive Compensation Alert
- May 2010, First Come, First Served: New Early Retiree Reinsurance Program, Employee Benefits and Executive Compensation Alert
- April 2010, Mental Health Benefits: More Changes Needed to Your Health Plan, Employee Benefits and Executive Compensation Alert
- March 2010, Important Changes to Form 5500 Filing Requirements, Employee Benefits and Executive Compensation Alert
- March 2010, Important April 30, 2010 Deadline for Employers Who Have Adopted Pre-Approved Retirement Plans, Employee Benefits and Executive Compensation Alert
- December 2009, Federal COBRA Subsidy Expanded, Employee Benefits and Executive Compensation Alert
- November 2009, Effective Date of Normal Retirement Age Regulations Extended for Governmental Plans, Employee Benefits and Executive Compensation Alert
- August 2009, Update on Legal Developments Affecting Employee Benefit Plans, Employee Benefits and Executive Compensation Alert
- July 2009, Looking Toward 2010 - Key Legal Changes to Keep in Mind While Designing Your 2010 Health Plans, Employee Benefits and Executive Compensation Alert
- July 2009, Important News for 403(b) Plan Sponsors, Employee Benefits and Executive Compensation Alert
- March 19, 2009, Department of Labor Issues Model Notices on COBRA Subsidy, Employee Benefits and Executive Compensation Alert
- March 2009, Supreme Court Rules Plan Documents, Not Divorce Decree, Control in ERISA Beneficiary Dispute, Employee Benefits and Executive Compensation Alert
- December 2, 2008, Year-End Checklist for Benefit Plan Sponsors, Employee Benefits and Executive Compensation Alert
- November 20, 2008, Venable Employee Benefits Lawyers Selected as Best Lawyers in America, Employee Benefits and Executive Compensation Alert
- October 28, 2008, 2009 Dollar Limits on Compensation and Benefits, Employee Benefits and Executive Compensation Alert
- October, 2008, Roundup of Important Developments Affecting Health Plans, Employee Benefits and Executive Compensation Alert
- September 25, 2008, Tax-Exempt Healthcare Prepares for 2009: Key Compensation and Reporting Points
- July 2008, More Items for Your Section 409A Compliance Checklist, Employee Benefits and Executive Compensation Alert
- March 2008, 401(k) Participants Can Sue Plan Fiduciaries For Losses To Individual Accounts, Employee Benefits and Executive Compensation Alert
- December 2007, Year-End Wrap-Up for Qualified Plans, Employee Benefits and Executive Compensation Alert
• October 26, 2007, Section 409A Final Regulations Delayed to 2009, Employee Benefits and Executive Compensation Alert
• October 2007, 2008 Dollar Limits on Compensation and Benefits, Employee Benefits and Executive Compensation Alert
• September 2007, Form 990 Executive Compensation Reporting – Prepare for Change, Employee Benefits and Executive Compensation Alert
• August 2007, Important Developments Affecting Health Plans, Employee Benefits and Executive Compensation Alert
• July 2007, DOE Cost Reimbursement Policy and Cost Accounting Standards for Pension Plan Contributions Required Under New Funding Rules, Employee Benefits and Executive Compensation Alert
• July 2007, Section 403(b) Tax-Sheltered Annuity Final Regulations Expected This Week, Employee Benefits and Executive Compensation Alert
• April 2007, Current Regulatory and Legislative Developments Could Dramatically Affect Employment and Benefit Issues for Government Contractors, Employee Benefits and Executive Compensation Alert
• April 10, 2007, Final Regulations Regarding Deferred Compensation Under Section 409A Released Today, Employee Benefits and Executive Compensation Alert
• April 3, 2007, Final Regulations Regarding Deferred Compensation Under Section 409A Expected Shortly, Employee Benefits and Executive Compensation Alert
• November 2006, Pension Protection Act of 2006: Provisions of Interest to Exempt Organizations
• October 2006, November 14th Deadline for Sending Annual Medicare Part D Notice Fast Approaching, Employee Benefits and Executive Compensation Alert
• October 2006, The IRS Extends Deferred Compensation Plan Deadlines Under §409A, Employee Benefits and Executive Compensation Alert
• September 1, 2006, Landmark Pension Reform Law Enacted: How Your Retirement Programs Will Be Affected, Employee Benefits and Executive Compensation Alert
• July 2006, Good News for Plans, Employee Benefits and Executive Compensation Alert
• May 2006, Revised Model Medicare Part D Notices Are Now In Effect, Employee Benefits and Executive Compensation Alert
• August 2005, Recent Health and Welfare Changes: New Notice Obligations, A Valuable Subsidy for Retiree Programs, and More Flexibility for FSAs, Employee Benefits and Executive Compensation Alert
• February 15, 2005, It’s Déjà Vu All Over Again: HIPAA Security Standards Take Effect on April 20, 2005, Employee Benefits and Executive Compensation Alert
• February 2005, New Automatic Rollover Rules for Mandatory Cashout Distributions from Retirement Plans, Employee Benefits and Executive Compensation Alert
• December 2004, New Definition of “Dependent” Affects Employee Benefit Plans, Employee Benefits and Executive Compensation Alert

SPEAKING ENGAGEMENTS
• August 8, 2013, The Road Map to HIPAA Compliance: What Your Nonprofit Needs to Know
• July 23, 2013, Evaluating Your Nonprofit’s Options under the Affordable Care Act: The Pros and Cons of Health Insurance Alternatives for Your Employees
• July 18, 2013, The Road Map to HIPAA Compliance
• July 17, 2013, The Road Map to HIPAA Compliance
• May 2, 2013, “The Changing Landscape for Employer Health Plans” at the 40th Annual Head Start Conference
• April 22, 2013 - April 25, 2013, ACG InterGrowth 2013
• January 24, 2013, The Changing Landscape for Employer Health Plans: What Employers and Plan Sponsors Need to Know
• July 24, 2012, “The Supreme Court’s Ruling on the Affordable Care Act and What it Means for Your Health Plans” for Kelly Benefit Strategies
• June 29, 2012, After the Supreme Court Healthcare Ruling: What’s Your Next Move?
• February 8, 2011, Legal Quick Hit: “International Grantmaking: Avoid Legal Pitfalls When Doing Good Overseas” for the Association of Corporate Counsel’s Nonprofit Organizations Committee
• September 16, 2010, “Healthcare Reform 2.0: Redesigning Your Health Plan and Open Enrollment” webinar hosted by Venable LLP
• April 22, 2010, Health Care Reform: What It Means for Employers and the Health Plans They Sponsor (Webinar)
• October 1, 2009, The Changing HIPAA Landscape: Seminar on October 1, 2009 in Baltimore, MD
• September 23, 2009, The Changing HIPAA Landscape: Seminar on September 23, 2009 in Washington, DC
• April 20, 2009, Mid-Year Seminar of the International Municipal Lawyers Association
• February 10, 2009, Legal Quick Hit: Lobbying Tax Rules for 501(c)(3) Organizations - A Refresher
• October 1, 2008, The New IRS Form 990: What Does it Mean for Your Organization?
• September 22, 2008, The New IRS Form 990: What Does It Mean for Your Nonprofit Organization?
• May 22, 2008, The New IRS Form 990: What Does It Mean for Your School?
• May 19, 2008, New IRS Form 990 Audio conference
• April 2008, “Unrelated Business Income Tax and Form 990-T” sponsored by the Maryland Association of CPAs
• September 2006, “HIPAA for Employers and HR Departments” at Lord Fairfax Community College
• August 10, 2006, Goodbye Medical Savings Accounts, Hello Health Savings Accounts, Health Reimbursement Accounts and Flexible Spending Accounts
• 2004, “Health Savings Accounts” sponsored by insurance brokerage firm Armfield, Harrison & Thomas
• February 26, 2003, National Business Officers Associations Annual Meeting “HIPAA”
• 2002, In-house HIPAA seminar to Society for Human Resource Management
Peter P. Parvis helps clients identify their goals and objectives and strategies to achieve them; structures those strategies to avoid the mine field of regulations, and criminal and civil penalties which are the hallmark of modern health care; and assists clients in implementing the chosen strategies.

Experienced and known for his knowledge of legal details, Mr. Parvis offers clients the benefits of his long and successful record in the rapidly changing field of health care. He has spearheaded efforts to consolidate medical resources for efficiency and quality care. His experience in having represented all elements of the pharmaceutical and DME field, hospitals, other institutional providers, physicians, and payors, including Blue Cross Associations and HMOs, provides the necessary base to advise clients in how best to protect and position themselves in the frequently chaotic health care environment. Mr. Parvis was named one of Baltimore’s outstanding lawyers by Baltimore magazine.

SIGNIFICANT MATTERS

Mr. Parvis represented clients in the House Energy and Commerce Committee’s 2003-2004 investigation into pharmaceutical pricing and the Medicaid system; and the Federal Trade Commission’s 2005 study of the competitive impact of the PBM industry’s practices, with particular focus on the ownership of mail order pharmacies.

Mr. Parvis, Bill Coston and other Venable lawyers, on behalf of a national entity, brought a federal action which resulted in declaring a state Medicaid system’s two-tiered approach that paid chain pharmacies substantially less than smaller pharmacies for identical drugs unlawful under the federal Medicaid Act and the U.S. Constitution. See Wal-Mart Stores, Inc. v. Knickrehm, E.D. Ark (June 7, 2000).

HONORS

- Listed in *The Best Lawyers in America*, Health Care, (Woodward/White, Inc.) 1993-present
- Recognized in the 2013 edition of *Chambers USA*, (Band 2), Healthcare, Maryland
- Recognized in the 2012 edition of *Chambers USA*, (Band 2), Healthcare, Maryland
- Recognized in the 2011 edition of *Chambers USA*, (Band 2), Healthcare, Maryland
- Recognized in the 2010 edition of *Chambers USA*, (Band 2), Healthcare, Maryland
- Recognized in the 2009 edition of *Chambers USA*, (Band 3), Healthcare, Maryland
- Recognized in the 2008 edition of *Chambers USA*, (Band 3), Healthcare, Maryland
- Recognized in the 2007 edition of *Chambers USA*, (Band 3), Healthcare, Maryland
- Recognized in the 2006 edition of *Chambers USA*, (Band 3), Healthcare, Maryland
- Selected for inclusion in *Maryland Super Lawyers* 2009 - 2013
Julia Kernochan Tama is an associate in the firm’s Regulatory Affairs group, where she focuses her practice on privacy and data security matters including financial and health privacy, marketing and advertising, and emerging issues related to the Internet and new media. Ms. Tama advises on compliance with existing laws and regulations, represents clients facing government inquiries or enforcement actions by agencies such as the Federal Trade Commission, and advocates on behalf of clients concerned about the impact of proposed legislation or agency regulation. Ms. Tama also counsels companies responding to potential data security breaches.

Prior to joining Venable, Ms. Tama served as Judiciary Committee Counsel to U.S. Senator Charles E. Schumer (D-NY), where her portfolio included privacy, data security, consumer protection, child Internet safety, foreign intelligence surveillance, and homeland security issues. Drawing on her years on Capitol Hill, Ms. Tama provides clients with insight into the legislative process, as well as substantive experience in legislative drafting, analysis and negotiation. Ms. Tama’s familiarity with committee hearings and investigations equips her to advise clients responding to congressional scrutiny.

**PUBLICATIONS**

- June 2013, The Download - June 2013, The Download
- December 20, 2012, It’s Beginning to Look a Lot Like… COPPA, All About Advertising Law Blog
- November 2012, Mobile Data Privacy: Snapshot of an Evolving Landscape, Journal of Internet Law
- August 2012, FTC Modifies COPPA Rule Proposal, Advertising Alert
- August 2012, The Download - August 2012, The Download
- June 2012, The Download - June 2012, The Download
- February 2012, The Download - February 2012, The Download
- December 2011, The Download - December 2011, The Download
- October 2011, The Download - October 2011, The Download
- May 2011, Special Report: Summary of FTC Request for Comments on Updating Its "Dot Com Disclosures: Information About Online Advertising", The Download
EDUCATION
J.D., Yale Law School, 2005
M.P.A., Woodrow Wilson School of Public and International Affairs, Princeton University, 2005
B.A., Swarthmore College, 1998
Phi Beta Kappa

• May 10, 2011, Top Five Privacy and Data Security Issues for Nonprofit Organizations
• March 2011, The Download - March 2011, The Download
• January 2011, The Download - January 2011, The Download
• November 2010, The Download - November 2010, The Download
• August 2010, The Download - August 2010, The Download
• April 2010, The Download - April 2010, The Download
• February 2010, The Download - February 2010 - Developments in E-Commerce, Privacy, Marketing, and Information Services Law and Policy, The Download
• November 2009, The Download - November 2009 - Developments in E-Commerce, Privacy, Marketing, and Information Services Law and Policy, The Download
• September 2009, The Download - September 2009 - Developments in E-Commerce, Privacy, Marketing, and Information Services Law and Policy, The Download
• July 2009, Self-Regulatory Principles for Online Behavioral Advertising

SPEAKING ENGAGEMENTS
• August 8, 2013, The Road Map to HIPAA Compliance: What Your Nonprofit Needs to Know
• July 18, 2013, The Road Map to HIPAA Compliance
• July 17, 2013, The Road Map to HIPAA Compliance
• June 5, 2013, "The State of Mobile in the DAA Program: Key Challenges for Cross-Industry Self-Regulation" at the First Annual DAA Summit
• September 6, 2012, "Privacy and Information Security Update” for the ABA Section of Antitrust Law
• July 19, 2012, Legal Quick Hit: "Geolocation Data Privacy: Where Are We, and Where Are We Going?” for the Association of Corporate Counsel
• May 3, 2012, Legal Quick Hit: "New Developments in Mobile Privacy” for the Association of Corporate Counsel
• February 1, 2012, "California 'Shine the Light' Law: Could Data Sharing Put You in Class Action Crosshairs?” for the Direct Marketing Association
• May 10, 2011, Legal Quick Hit: “Top Five Privacy and Data Security Issues for Nonprofits” for the Association of Corporate Counsel’s Nonprofit Organizations Committee
• March 26, 2011, "Online Advertising and Privacy” at Yale Law School’s ISP conference "From Mad Men to Mad Bots: Advertising in the Digital Age"
• June 14, 2010, "Understanding the New Regulations” for International Association of Privacy Professionals Practical Privacy Series, "Privacy in the New Healthcare Era"
• September 23, 2009, The Changing HIPAA Landscape: Seminar on September 23, 2009 in Washington, DC
Jennifer Spiegel Berman
Associate
Baltimore, MD Office

410.244.7756 F 410.244.7742 jsberman@Venable.com

Jennifer Berman is a member of the firm’s Employee Benefits and Executive Compensation Group. She handles a broad range of employee benefits and executive compensation matters, including tax-qualified retirement plans, executive compensation arrangements, cafeteria plans, and health and welfare benefits plans. Ms. Berman regularly counsels clients regarding ongoing employee benefit compliance issues and assists clients in developing and implementing compliance programs. She advises covered entities and business associates on HIPAA and HITECH compliance matters, including developing and updating privacy and security policies, business associate agreements and notification of breach protocols. Among other things, Ms. Berman routinely negotiates service contracts and drafts employee benefit plans, summary plan descriptions and employee communications. She also reviews client benefit programs for compliance with the Internal Revenue Code, ERISA, HIPAA, COBRA, ACA, wellness plan rules and other applicable statutes. Ms. Berman has become a leader in analyzing health care reform developments and frequently serves as a speaker and commentator on a wide variety of health care reform and employee benefits issues.

ACTIVITIES
Ms. Berman is Co-Chair of the Maryland State Bar Association Employee Benefits Study Group. She is also a member of the American Health Lawyers Association and the Society for Human Resource Management.

PUBLICATIONS
- July 2013, What Your Nonprofit Needs to Do about HIPAA – Now
- June 27, 2013, After DOMA: Impacts on Tax and Benefits Planning, Tax Bulletin
- May 2013, What Your Business Needs to Do about HIPAA – Now, Employee Benefits and Executive Compensation Alert
- March/April 2013, Health Coverage under the Affordable Care Act: What You [and Your Clients] Need to Know, Maryland Bar Journal
- January 2013, Limited Relief for Employers under Health Care Reform’s "Play-or-Pay" Rules, Employee Benefits and Executive Compensation Alert
- October 2012, Health Care Reform: Large Employers and the New Health Insurance Exchanges, Employee Benefits and Executive Compensation Alert
- September 2012, Private Exchanges: You Have Questions, We Have Answers, Employee Benefits and Executive Compensation Alert
- September 2012, Don’t Play and Also Pay: What Nonprofit Employers Need to Know about Navigating the Employer-Sponsored Health Coverage Mandate