VENABLE® LLP

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

August 8, 2013

Venable LLP

Washington, DC

Moderator:

Jeffrey S. Tenenbaum, Esq., Venable LLP

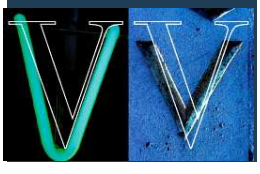
Panelists:

Thora A. Johnson, Esq., Venable LLP

Kelly A. DeMarchis, Esq., Venable LLP

Jennifer Spiegel Berman, Esq., Venable LLP

Presentation



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

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

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.

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

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

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?

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

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 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

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
- 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"

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

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

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?

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.

Speaker Biographies

VENABLE® LLP

our people

Jeffrey S. Tenenbaum

Partner

Washington, DC Office

T 202.344.8138 F 202.344.8300

jstenenbaum@Venable.com

Jeffrey Tenenbaum chairs Venable's Nonprofit Organizations Practice Group. He is one of the nation's leading nonprofit attorneys, and also is an accomplished author, lecturer, and commentator on nonprofit legal matters. Based in the firm's Washington, DC office, Mr. Tenenbaum counsels his clients on the broad array of legal issues affecting charities, foundations, trade and professional associations, think tanks, advocacy groups, and other nonprofit organizations, and regularly represents clients before Congress, federal and state regulatory agencies, and in connection with governmental investigations, enforcement actions, litigation, and in dealing with the media. He also has served as an expert witness in several court cases on nonprofit legal issues.

Mr. Tenenbaum was the 2006 recipient of the American Bar Association's Outstanding Nonprofit Lawyer of the Year Award, and was an inaugural (2004) recipient of the *Washington Business Journal*'s Top Washington Lawyers Award. He was one of only seven "Leading Lawyers" in the Not-for-Profit category in the prestigious 2012 *Legal 500* rankings, and one of only eight in the 2013 rankings. Mr. Tenenbaum was recognized in 2013 as a Top Rated Lawyer in Tax Law by *The American Lawyer* and *Corporate Counsel*. He was the 2004 recipient of The Center for Association Leadership's Chairman's Award, and the 1997 recipient of the Greater Washington Society of Association Executives' Chairman's Award. Mr. Tenenbaum was listed in *The Best Lawyers in America 2012* and *2013* for Non-Profit/Charities Law, and was named as one of Washington, DC's "Legal Elite" in 2011 by *SmartCEO Magazine*. He was a 2008-09 Fellow of the Bar Association of the District of Columbia and is AV Peer-Review Rated by *Martindale-Hubbell*. Mr. Tenenbaum started his career in the nonprofit community by serving as Legal Section manager at the American Society of Association Executives, following several years working on Capitol Hill as a legislative assistant.

AREAS OF PRACTICE

Tax and Wealth Planning
Antitrust
Political Law
Business Transactions Tax
Tax Controversies and Litigation
Tax Policy
Tax-Exempt Organizations
Wealth Planning
Regulatory

INDUSTRIES

Nonprofit Organizations and Associations
Credit Counseling and Debt Services
Financial Services
Consumer Financial Protection Bureau Task Force

GOVERNMENT EXPERIENCE

Legislative Assistant, United States House of Representatives

BAR ADMISSIONS

District of Columbia

REPRESENTATIVE CLIENTS

AARP
American Academy of Physician Assistants
American Alliance of Museums
American Association for the Advancement of Science
American Bureau of Shipping
American College of Radiology
American Institute of Architects
Air Conditioning Contractors of America
American Society for Microbiology
American Society for Training and Development
American Society of Anesthesiologists
American Society of Association Executives
American Staffing Association
Association for Healthcare Philanthropy

EDUCATION

J.D., Catholic University of America, Columbus School of Law, 1996

B.A., Political Science, University of Pennsylvania, 1990

MEMBERSHIPS

American Society of Association Executives

California Society of Association Executives

New York Society of Association Executives

Association of Corporate Counsel
Association of Private Sector Colleges and Universities
Automotive Aftermarket Industry Association
Brookings Institution
Carbon War Room
The College Board
Council of the Great City Schools
Council on Foundations
CropLife America
Cruise Lines International Association
Foundation for the Malcolm Baldrige National Quality Award
Gerontological Society of America
Goodwill Industries International
Homeownership Preservation Foundation
The Humane Society of the United States
Independent Insurance Agents and Brokers of America
Institute of International Education
International Association of Fire Chiefs
Jazz at Lincoln Center
The Joint Commission
LeadingAge
Lincoln Center for the Performing Arts
Lions Club International
Money Management International
National Association of Chain Drug Stores
National Association of Music Merchants
National Athletic Trainers' Association
National Board of Medical Examiners
National Coalition for Cancer Survivorship
National Defense Industrial Association
National Fallen Firefighters Foundation
National Fish and Wildlife Foundation
National Hot Rod Association
National Propane Gas Association
National Quality Forum
National Retail Federation
National Student Clearinghouse
The Nature Conservancy
NeighborWorks America
Peterson Institute for International Economics
Professional Liability Underwriting Society
Project Management Institute
Public Health Accreditation Board
Public Relations Society of America
Recording Industry Association of America
Romance Writers of America
Texas Association of School Boards
Trust for Architectural Easements
United Nations High Commissioner for Refugees
Volunteers of America

HONORS

Recognized as "Leading Lawyer" in the 2012 and 2013 editions of *Legal 500*, Not-For-Profit

Listed in *The Best Lawyers in America 2012* and *2013* for Non-Profit/Charities Law, Washington, DC (Woodward/White, Inc.)

Recognized as a Top Rated Lawyer in Taxation Law in *The American Lawyer* and *Corporate Counsel*, 2013

Washington DC's Legal Elite, *SmartCEO Magazine*, 2011

Fellow, Bar Association of the District of Columbia, 2008-09

Recipient, American Bar Association Outstanding Nonprofit Lawyer of the Year Award, 2006

Recipient, *Washington Business Journal* Top Washington Lawyers Award, 2004

Recipient, The Center for Association Leadership Chairman's Award, 2004

Recipient, Greater Washington Society of Association Executives Chairman's Award, 1997

Legal Section Manager / Government Affairs Issues Analyst, American Society of Association Executives, 1993-95

AV® Peer-Review Rated by *Martindale-Hubbell*

Listed in *Who's Who in American Law* and *Who's Who in America*, 2005-present editions

ACTIVITIES

Mr. Tenenbaum is an active participant in the nonprofit community who currently serves on the Editorial Advisory Board of the American Society of Association Executives' *Association Law & Policy* legal journal, the Advisory Panel of Wiley/Jossey-Bass' *Nonprofit Business Advisor* newsletter, and the ASAE Public Policy Committee. He previously served as Chairman of the *AL&P* Editorial Advisory Board and has served on the ASAE Legal Section Council, the ASAE Association Management Company Accreditation Commission, the GWSAE Foundation Board of Trustees, the GWSAE Government and Public Affairs Advisory Council, the Federal City Club Foundation Board of Directors, and the Editorial Advisory Board of Aspen's *Nonprofit Tax & Financial Strategies* newsletter.

PUBLICATIONS

Mr. Tenenbaum is the author of the book, *Association Tax Compliance Guide*, published by the American Society of Association Executives, and is a contributor to numerous ASAE books, including *Professional Practices in Association Management*, *Association Law Compendium*, *The Power of Partnership*, *Essentials of the Profession Learning System*, *Generating and Managing Nondues Revenue in Associations*, and several Information Background Kits. He also is a contributor to *Exposed: A Legal Field Guide for Nonprofit Executives*, published by the Nonprofit Risk Management Center. In addition, he is a frequent author for most of the nonprofit industry organizations and publications and other media, having written or co-written more than 500 articles on nonprofit legal topics.

SPEAKING ENGAGEMENTS

Mr. Tenenbaum is a frequent lecturer for ASAE and many of the major nonprofit industry organizations, conducting over 40 speaking presentations each year, including many with top Internal Revenue Service, Federal Trade Commission, U.S. Department of Justice, Federal Communications Commission, and other federal and government officials. He served on the faculty of the ASAE Virtual Law School, and is a regular commentator on nonprofit legal issues for *The New York Times*, *The Wall Street Journal*, *The Washington Post*, *Los Angeles Times*, *The Washington Times*, *The Baltimore Sun*, *ESPN.com*, *Washington Business Journal*, *Legal Times*, *Association Trends*, *CEO Update*, *Forbes Magazine, The Chronicle of Philanthropy, The NonProfit Times* and other periodicals. He also has been interviewed on nonprofit legal issues on Voice of America Business Radio, Nonprofit Spark Radio, and The Inner Loop Radio.

VENABLE® LLP

our people

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.

AREAS OF PRACTICE

Employee Benefits and Executive Compensation

Tax and Wealth Planning

Healthcare

Business Transactions Tax

Tax Controversies and Litigation

Tax Policy

Tax-Exempt Organizations

Wealth Planning

INDUSTRIES

Nonprofit Organizations and Associations

BAR ADMISSIONS

Maryland

District of Columbia

EDUCATION

J.D., *with honors*, University of Maryland School of Law, 1996

Notes & Comments Editor, *Maryland Journal of International Law and Trade*

M.A., Middlebury College, 1993

B.A., *magna cum laude*, Brown University, 1992

Phi Beta Kappa

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.

VENABLE® LLP

our people

Kelly A. DeMarchis

Associate

Washington, DC Office

T 202.344.4722 F 202.344.8300

kademarchis@Venable.com

Kelly A. DeMarchis is an associate in the firm's Regulatory Affairs Practice Group, where she advises and represents clients on issues related to privacy and e-commerce.

Ms. DeMarchis has expertise in U.S. and global personal data privacy issues. She has provided advice to companies responding to data breach and has extensive experience assisting clients in becoming compliant with a number of U.S. privacy statutes, including state breach notification laws, HIPAA, the Fair Credit Reporting Act and others. She has also worked with clients on questions related to global data privacy.

Ms. DeMarchis also concentrates her practice on e-commerce for both online and bricks-and-mortar clients, and has provided advice to clients on many related statutes, such as the Computer Fraud and Abuse Act, the Digital Millennium Copyright Act, the Electronic Communications Privacy Act, CAN-SPAM, E-SIGN, the Communications Decency Act and the Stored Communications Act.

Ms. DeMarchis has extensive expertise in the laws governing remote gaming and gambling and has represented both gaming operators and online payment processors.

Ms. DeMarchis has litigated these issues and has extensive experience with internal investigations into a variety of matters.

AREAS OF PRACTICE

Privacy and Data Security

Advertising and Marketing

Advertising and Marketing Litigation

Regulatory

INDUSTRIES

Cybersecurity

BAR ADMISSIONS

District of Columbia

Pennsylvania

COURT ADMISSIONS

U.S. Court of Appeals for the Sixth Circuit

U.S. District Court for the Western District of Pennsylvania

EDUCATION

J.D., University of Virginia School of Law, 2004

Business Editor, *Virginia Environmental Law Journal*

A.B., Philosophy and English, Duke University, 2000

VENABLE® LLP

our people

Jennifer Spiegel Berman

Associate

Baltimore, MD Office

T 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.

AREAS OF PRACTICE

Employee Benefits and Executive Compensation

BAR ADMISSIONS

District of Columbia

Maryland

EDUCATION

J.D., *cum laude*, University of Pennsylvania Law School, 2006

- Editor-in-Chief, *Journal of Labor and Employment Law*
- Recipient, The George Shechtman Prize, Contracts
- Recipient, The M.H. Goldstein Memorial Prize, Best Paper in Labor Law

B.A., *magna cum laude*, University of Pennsylvania, 2004

MEMBERSHIPS

Co-Chair, Maryland State Bar Association Employee Benefits Study Group

American Health Lawyers Association

Society for Human Resource Management

Additional Information

VENABLE® LLP

AUTHORS:

Peter P. Parvis
ppparvis@Venable.com
410.244.7644

Thora A. Johnson
tajohnson@Venable.com
410.244.7747

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*.

VENABLE® LLP

AUTHORS:

Peter P. Parvis
ppparvis@Venable.com
410.244.7644

Thora A. Johnson
tajohnson@Venable.com
410.244.7747

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*.

VENABLE® LLP

Articles

July 2013

What Your Nonprofit Needs to Do about HIPAA – Now

AUTHORS

Thora A. Johnson

Peter P. Parvis

Jennifer Spiegel Berman

Jessica E. Kuester

DOWNLOADABLE FILES

- What Your Nonprofit Needs to Do about HIPAA – Now

RELATED PRACTICES

Healthcare

RELATED INDUSTRIES

Nonprofit Organizations and Associations

ARCHIVES

2013 2009 2005
2012 2008 2004
2011 2007 2003
2010 2006

Whether your nonprofit entity is an employer that provides health insurance to your employees, an organization in the growing health care 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 organization in the health care industry (and every service provider to those organizations) is affected by these changes.

Among other things, the Final Regulations:

- Directly subject Business Associates,[1] 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 Protected Health Information (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, September 23, 2013). Following the list of action items is a more detailed summary of the changes made by the Final Regulations.

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 which 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 (new) Business Associates. Specifically, penalties for violations are determined with a tiered approach:

Violation Due to:	**Penalty Range (per Violation):**
Unknown cause	$100-$50,000
Reasonable cause and not willful neglect	$1,000-$50,000
Willfull 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.

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.

HIPAA Glossary

The world of HIPAA includes a vocabulary of its own. Key terms that may aid in your understanding include the following:

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.

Click here to view the PDF version of this article.

VENABLE LLP

wellness program alert

Please contact any of the authors below if you have questions regarding this alert.

Authors:

Thora A. Johnson
tajohnson@Venable.com
410.244.7747

Jennifer Spiegel Berman
jsberman@Venable.com
410.244.7756

Laura A. Taylor
lataylor@Venable.com
410.244.7657

Is Your Wellness Program Healthy? Final HIPAA Wellness Regulations Issued

The Departments of Labor, Treasury, and Health and Human Services recently issued final regulations on incentive-based wellness programs under the HIPAA nondiscrimination rules. The HIPAA nondiscrimination rules generally prohibit group health plans from discriminating against participants based on their health. The new regulations, which are effective for plan years beginning on or after January 1, 2014, supersede regulations issued in 2006 and set out a safe harbor under which plans may discriminate based on health-related factors (such as medical conditions, claims experience, and the receipt of health care) in order to promote health and prevent disease.

Participatory Wellness Programs

There are two types of wellness programs: participatory programs and health-contingent programs. Participatory wellness programs either do not provide a reward or do not include any conditions for obtaining a reward that are based on satisfying a health-related requirement. Examples of participatory wellness programs include reimbursing employees for gym memberships, free diagnostic testing programs with a reward for mere participation (and with no outcome-based rewards), and education programs with rewards for attendance. Participatory wellness programs are not required to meet the standards set forth under the final regulations because they do not discriminate based on a health status factor, and thus do not need special protection from the otherwise applicable HIPAA nondiscrimination rules. They must simply be offered to all similarly situated individuals.

Health-Contingent Wellness Programs

In contrast, health-contingent wellness programs, which require individuals to satisfy a standard related to a health factor in order to receive a reward, must meet certain criteria to avoid being deemed discriminatory under HIPAA. Specifically, the program must satisfy five requirements.

1. Individuals must be offered the opportunity to qualify for the reward at least once per year.
2. The maximum reward that can be offered is limited to 30% (up from 20% under the 2006 regulations) of the total cost of coverage under the plan (with up to an additional 20% reward permissible for programs designed to prevent or reduce tobacco use).
3. The program must be reasonably designed to promote health or prevent disease.
4. The program must offer a “reasonable alternative standard” to obtain the reward.
5. The availability of a “reasonable alternative” to qualify for the reward must be disclosed in all plan materials describing the wellness program.

Reasonable Alternative Standard

Aside from the increase in the maximum permissible reward, the biggest change to the rules regarding health-contingent wellness programs relates to the requirement to provide a “reasonable alternative standard” to obtain the reward. Specifically, the final regulations create two new subcategories of health-contingent wellness programs: activity-only programs and outcome-based programs.

Activity-only programs require an individual to perform or complete an activity related to a health factor in order to qualify for a reward. Activity-only wellness programs do not, however, require an individual to attain or maintain a specific health outcome. Examples of activity-only programs include walking challenges or diet programs. Alternatively, outcome-based programs are programs that require an individual to meet or maintain a specific health outcome to earn a reward. Examples of outcome-based programs include programs that reward individuals for meeting a certain BMI or not using tobacco products.

As noted above, health-contingent programs are generally required to offer a reasonable alternative standard in order to qualify for a reward. Activity-only programs are required to offer a reasonable alternative to only those individuals who request such an accommodation and are able to demonstrate that it is unreasonably difficult or medically inadvisable for them to satisfy or attempt to satisfy the activity generally required to receive the reward. Thus, for example, if a walking program requires employees to walk 30 minutes a day in order to receive a reward, and an employee is unable to walk due to an injury, then the plan must provide a reasonable alternative by which the employee can attain the reward. For instance, the alternative might be attending a health and fitness educational program; or, if the injury is temporary in nature (such as a broken leg), the plan may waive the standard until the injury is healed.

In the case of outcome-based programs, reasonable alternatives must be offered to any individual who requests an accommodation (regardless of whether they can show it would be unreasonably difficult or medically inadvisable to meet the program's otherwise applicable criteria). For example, if an outcome-based weight loss program requires that employees maintain or achieve a BMI of less than 30 to qualify for a reward and an employee does not wish to or cannot achieve that BMI, then a reasonable alternative might be walking 150 minutes a week. Of course, this alternative would need to comply with the activity-based rules.

Moreover, the following special rules (among others) apply to reasonable alternatives.

1. If the reasonable alternative is an educational program, the plan must help the individual locate an appropriate program and may not require the individual to pay the cost of the program.
2. The time commitment associated with any reasonable alternative must be reasonable.
3. If the reasonable alternative is a diet program the individual cannot be required to pay a membership or registration fee (but can be charged the cost of food).
4. If an individual's physician says a particular plan standard is not medically appropriate for the individual, the plan most provide a reasonable alternative that is deemed medically appropriate by the individual's physician.

Preparing for 2014

Now is a good time to review and re-evaluate your current wellness programs and prepare them for any changes required in 2014. In addition to the HIPAA rules discussed above, there are also other laws that may apply to both your participatory and health-contingent wellness programs, including ERISA and the ADA. If you have any questions about your wellness plans, please contact one of Venable's employee benefits attorneys.