VENABLE LLP

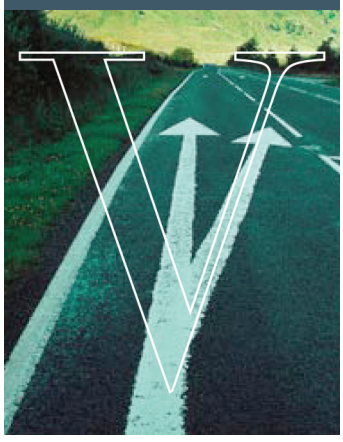
what your business needs to do about the new HIPAA rules

Whether you are an employer that provides health insurance for your employees, a business in the growing health care industry, or a hospital or other medical provider, you need to know about some key changes to the privacy and security rules under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), which have been substantially broadened under the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act").

Among other changes, the HITECH Act:

- Requires Covered Entities[1] to notify affected individuals, the federal government, and the media (in certain circumstances) of a Breach involving Unsecured PHI;
- Directly subjects Business Associates to the HIPAA security rule and certain aspects of the HIPAA privacy rule;
- Creates new obligations related to the use and disclosure of PHI, including parameters on what is the "minimum necessary" PHI that can be used or disclosed in any particular circumstance, and enhanced rights for individuals regarding their PHI; and
- Significantly strengthens the authority of the federal government to enforce the HIPAA privacy and security rules.

The following is a brief description of each of these new requirements and a summary of the necessary action items that you should take in order to comply with them.



[1] Key capitalized terms not otherwise defined are listed in the Glossary at the end of this article.

Effective September 23, 2009— Covered Entities and Business Associates Must Provide Notice of a Breach Involving "Unsecured" PHI

Effective immediately, Covered Entities must notify affected individuals no later than 60 days after a Breach of Unsecured PHI has been discovered.

So…What is a Breach Involving Unsecured PHI That Will Trigger These New Notice Requirements?

- A **"Breach"** is the unauthorized acquisition, access, use or disclosure of PHI that compromises the security or privacy of such information.

  Note there are some important exceptions to this definition. Specifically, a Breach does *not* include:

  (1) A situation where the Covered Entity maintains a good faith belief that the recipient of the information could not reasonably have been able to retain the disclosed information; or

  (2) Certain unintentional access or disclosure within the workplace; or

  (3) An incident that does not pose a significant risk of financial, reputational, or other harm to the individual.

- **"Unsecured PHI"** is PHI that is not rendered unusable, unreadable, or indecipherable to an unauthorized individual through encryption or destruction, pursuant to guidance published by the US Department of Health and Human Services (DHHS).

- A Breach is deemed **"discovered"** on the first day that the Breach is known or should reasonably have been known to the Covered Entity (or in some cases, its Business Associate).

If There Is a Breach of Unsecured PHI, Who Has to Do What in Order to Meet the New Notice Obligations?

If a Business Associate discovers a Breach of Unsecured PHI, it must notify the Covered Entity of the Breach and identify each affected individual, so that the Covered Entity, in turn, can notify each affected individual. Alternatively, the Business Associate can be contractually obligated to notify such individuals directly on behalf of the Covered Entity if the terms of the contract between the Covered Entity and the Business Associate—otherwise known as a **"Business Associate Agreement"**—have been amended to specifically shift this responsibility from the Covered Entity to the Business Associate.

If a Covered Entity discovers a Breach of Unsecured PHI, it must notify each affected individual.

Regardless of whether the Business Associate or Covered Entity discovers a Breach of Unsecured PHI, the Covered Entity has the obligation to notify the local media of Breaches involving 500 or more individuals in a given state or jurisdiction. In addition, the Covered Entity must notify DHHS of all Breaches of Unsecured PHI, regardless of the number of affected individuals. If a Breach involves 500 or more individuals, DHHS must be notified immediately; otherwise, such Breaches must be cataloged and only need to be submitted to DHHS annually.

DHHS has posted forms and instructions on its website for reporting breaches to it. They can be found at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html.

CAUTION: 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.

ACTION ITEMS TO COMPLY WITH BREACH NOTIFICATION REQUIREMENTS

- ☐ Evaluate current administrative, physical and technical safeguards utilized for PHI, and consider implementing encryption and destruction technologies in order to minimize the risk that your PHI will be considered "Unsecured PHI"
- ☐ Create processes to discover Breaches of Unsecured PHI
- ☐ Develop a policy about how to handle Breaches of Unsecured PHI
- ☐ Update other related privacy and security policies, including those on safeguards; mechanisms for reporting breaches; mitigation measures; complaint procedures; sanctions; and training
- ☐ Amend Business Associate Agreements to address DHHS guidance on encryption and destruction and allocate responsibility for the notice obligations
- ☐ Train workforce on the notice of breach requirement

Effective February 17, 2010 And Beyond— Business Associates Directly Subject to the Security Rule and Aspects of the Privacy Rule

Business Associates will be directly liable (and not simply contractually liable pursuant to Business Associate Agreements) for complying with:

- 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.

CAUTION: As of February 17, 2010, two new groups of businesses will also be deemed to be Business Associates!

- Entities that transmit PHI on behalf of Covered Entities, such as regional health information organizations, health information exchanges, and e-prescribing gateways; and
- Vendors that contract with Covered Entities to allow the Covered Entities to offer a personal health record to patients as part of their electronic health record.

ACTION ITEMS TO COMPLY WITH DIRECT LIABILITY OF BUSINESS ASSOCIATES

For Business Associates

- ☐ Create or update HIPAA security and privacy policies
- ☐ Conduct HIPAA security risk analysis and prepare risk management plan
- ☐ Amend Business Associate Agreements to reflect new direct liability

For Covered Entities

- ☐ Amend Business Associate Agreements to reflect new direct liability of the Business Associates

Effective February 17, 2010 and After— New Obligations Related to the Use and Disclosure of PHI

Using or Disclosing the "Minimum Necessary" PHI

Under HIPAA, a Covered Entity must limit its use or disclosure of PHI to the minimum amount that is necessary to accomplish the intended purpose.

Up until now, a Covered Entity had to use "reasonable efforts" to limit its use or disclosure of PHI to the minimum amount necessary. DHHS is in the process of developing guidance about what satisfies the minimum necessary standard. However, as of February 17, 2010 (and until this further guidance is issued), a Covered Entity will automatically be 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.

New Mandatory Compliance With Restrictions Requested on Certain Disclosures of PHI

As of February 17, 2010, Covered Entities will be required to 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 for the purposes of carrying out payment or health care operations (unless the use or disclosure is 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.

New Rights of Individuals to Access Their PHI in Electronic Format

As of February 17, 2010, Covered Entities that use or maintain an electronic health record for an individual's PHI will need to be able to provide that individual with a copy of his or her PHI in an electronic format, if the individual requests it. Individuals making such a request may only be charged for labor costs associated with providing the requested information.

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

As early as January 1, 2011, Covered Entities and Business Associates 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 operation. (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.

Covered Entities may elect to provide disclosures on behalf of Business Associates, or provide the individual with a list of its Business Associates, in which case, the Business Associate would be responsible for providing the accounting of the disclosures.

ACTION ITEMS TO COMPLY WITH NEW OBLIGATIONS REGARDING USE AND DISCLOSURE OF PHI

- ☐ Create processes to track disclosures of electronic PHI for treatment, payment and health operations purposes
- ☐ Update privacy policies on the use and disclosure of PHI to satisfy the minimum necessary standard, comply with the new requirements on restrictions that may be requested, provide access to PHI in electronic format, and provide an accounting of disclosures of electronic PHI
- ☐ Update Business Associate Agreements to require use of Limited Data Sets, where practicable, and identify which party will be responsible for complying with the new individual rights to request restrictions on certain disclosures of PHI, obtain access to PHI in an electronic format, and obtain an accounting of disclosures of electronic PHI
- ☐ Update and distribute notice of privacy practices to reflect changes to policies
- ☐ Create or update internal training materials

Effective February 17, 2009 for Covered Entities and February 17, 2010 for Business Associates—Significantly Enhanced HIPAA Enforcement Provisions

- The HITECH Act considerably increases the civil monetary penalties that may be assessed under HIPAA against Covered Entities (and Business Associates as of February 17, 2010). Specifically, penalties are to be determined with a new tiered approach:

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)	$10,000-$50,000
Willful neglect (violation not corrected)	$50,000

There is a cap of $1,500,000 for violations of an identical privacy or security requirement per calendar year.

- In time, individuals who are harmed may be able to receive a percentage of penalties that are imposed.

- The HITECH Act reaffirms that an individual who obtains or discloses PHI from a Covered Entity or Business Associate without authorization may be subject to criminal prosecution for a violation of HIPAA.

- State attorneys general are now authorized to initiate civil actions in federal court for injunctive relief or monetary damages on behalf of a state resident.

- The HITECH Act requires DHHS to perform periodic audits of Covered Entities and Business Associates to ensure that they are complying with the HIPAA privacy and security rules.

ACTION ITEMS TO ENHANCE RISK MANAGEMENT AND DEFENSIVE POSITION IN RESPONSE TO ENHANCED ENFORCEMENT

- ☐ Review security and privacy compliance programs and update as required
- ☐ Take affirmative steps to identify and mitigate HIPAA violations
- ☐ Review and update complaint processes and policies
- ☐ Regularly conduct HIPAA training

HIPAA Glossary

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

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.

Business Associate
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.

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

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.

About Venable

One of *American Lawyer*'s top 100 law firms, Venable LLP has attorneys practicing in all areas of corporate and business law, complex litigation, intellectual property and government affairs. Venable serves corporate, institutional, governmental, nonprofit and individual clients throughout the U.S. and around the world from its offices in California, Maryland, New York, Virginia, and Washington, D.C.

Business Transactions Team

We take the time to understand your business—what's important to you personally and what's critical for success in the next stage of your enterprise. Our attorneys have the skills and experience needed to create pragmatic solutions grounded in the context of your business and industry. Working with your team, we knit together complete solutions, drawing on experience throughout Venable—blending the political and regulatory insights of former regulators and policymakers with the real-world experience of Venable business lawyers, including former corporate dealmakers and inside counsel. Whether your transaction involves the creation of a joint venture, a merger or acquisition, a buyout or the restructuring of a troubled company, Venable attorneys are skilled at moving swiftly to close the deal. Every aspect, from antitrust analysis to tax strategy, is part of a collaborative effort of our team and your advisors, accountants and investment bankers.

Employee Benefits and Executive Compensation Team

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 help our clients 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 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. Whether it is designing integrated benefit packages to fit the business goals and culture of an organization or ensuring clients stay in compliance as laws and regulations change, we become advocates for our clients' interests.

Healthcare Team

Venable has been advising healthcare clients for more than 40 years. Our mission is to provide legal solutions that make good business sense. We draw on many disciplines within Venable—business transactions, regulatory, 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. Venable's Healthcare Practice attorneys understand healthcare economics and its intimate connections with regulatory rules and enforcement policies; offer advice that is practical, based on our experience working with providers, payors and regulators every day; and provide solutions that work within the realities of healthcare, enhanced by our knowledge of regional and local politics and the business environment.

Privacy and Data Security Team

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. 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.