



# Control Essentials

## HITECH ACT Stronger Enforcement of Health Information Security



The Health Information Technology for Economic and Clinical Health (HITECH) Act was enacted on February 17, 2009. The HITECH Act expanded the reach of the Health Insurance Portability and Accountability Act (HIPAA) and the HIPAA Security and Privacy Rules. It also imposed breach notification requirements on HIPAA covered entities, their business associates, and all other entities that handle health information. The HITECH Act also increased penalties and resources for enforcement.

This article summarizes the new breach notification and enforcement provisions, focusing on HIPAA covered entities and business associates.

### New Breach Notification Requirements

#### **Breach**

The HITECH Act defines the term *breach* to mean the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.

#### **New Requirements**

The HITECH Act adds more requirements and stronger provisions than many state security breach notification laws. Unlike many state breach notification laws, the HITECH Act applies to breaches involving both electronic and paper records. The HITECH Act also covers medical information while most state laws focus on other types of sensitive personal information that can be used to commit financial fraud.

#### **Regulations and Enforcement**

The Department of Health and Human Services (HHS) and the Federal Trade Commission (FTC) are responsible for issuing and enforcing final regulations to ensure compliance with the HITECH Act. HHS is responsible for HIPAA “covered entities” and their “business associates.” The FTC is responsible for other entities that handle health information which were not covered by HIPAA, such as vendors of personal health records, related entities and third party service providers. HHS regulations define HIPAA “covered entities” as health plans, health care clearinghouses and health care providers who transmit any health information in electronic form. HHS regulations also define “business associates” in detail.



In general, they include persons and businesses which perform or assist in performing functions involving the use or disclosure of individually identifiable health information, such as claims processing, quality assurance, billing and benefit management.

HHS' preliminary guidance specifies the technologies and methodologies that make protected health information unusable, unreadable or undecipherable to unauthorized individuals. According to the preliminary guidance, breach notification requirements apply only to breaches of unsecured protected health information (PHI). This means health information that is not encrypted or otherwise indecipherable. Therefore, the proper implementation of security technologies, methodologies and logical as well as physical security controls will provide a "safe harbor," resulting in covered entities and business associates not being required to provide the notification otherwise required in the event of a breach. However, covered entities and business associates still must comply with all other federal and state statutory and regulatory obligations that may apply following a breach.

Enforcement of the new breach notification requirements will start 30 days after publication of interim final regulations which must be issued by August 17, 2009.

Additionally, the FTC issued its proposed rule requiring vendors of personal health records to notify individuals and the FTC when they discover a breach of security of individually identifiable health information. Also, a third party service provider--following the discovery of a breach of security--must provide notice of the breach to a senior official at the vendor of personal health records or PHR related entity to which it provides services, and obtain acknowledgment from such official that such notice was received. This proposed rule shall apply to breaches of security that are discovered on or after September 18, 2009.

## **Notification Requirements**

Below is a summary of key notification requirements with respect to HIPAA-covered entities and business associates:

- The HITECH Act requires covered entities to notify individuals whose unsecured protected health information has been, or is reasonably believed to have been, accessed, acquired, or disclosed as a result of a breach.
- Business associates must notify covered entities of any breach of which they become aware. Such notice shall include the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, or disclosed during such breach.
- A breach is considered discovered by a covered entity or by a business associate as of the first day on which such breach is known to such covered entity or business associate.
- Notification of the security breach must be made quickly and in no case later than 60 calendar days after the discovery of the breach.
- The covered entities or business associates involved have the burden of demonstrating that all notifications were made as required.
- The notice of a breach to the individuals involved must be made in the following manner:
  - Written notification by first-class mail to the individual at the last known address.
  - If there is insufficient contact information, provide notification via other media such as a posting on the Web site or notice in major print or broadcast media.



- In the case of possible imminent misuse of the unsecured protected health information, the entity must contact the affected individuals via phone or other means as appropriate.
- Notice must be provided to prominent media outlets serving a state or jurisdiction if the breach covers more than 500 residents of such state or jurisdiction.
- Covered entities must notify HHS of any breach. Security breaches of 500 or more individuals must be reported immediately.
- Covered entities need to maintain a log of security breaches and annually submit the log to HHS documenting the security breaches that occurred during the year.
- HHS will post on their Web site all covered entities that experienced a security breach of 500 or more individuals.
- The notification must include:
  - A brief description of the security incident, date of the breach and the date the breach was discovered.
  - A description of the types of data involved in the security breach.
  - The steps individuals should take to protect themselves from potential harm resulting from the breach.
  - A brief description of what the entity involved is doing to investigate the breach, to mitigate losses, and to protect against any further breaches.
  - Contact information for individuals to ask questions or obtain additional information.
- Notification may be delayed if law enforcement determines such notice would jeopardize an on-going investigation.
- HHS is required to submit an annual report to the U.S. Senate and House regarding the number of and nature of breaches reported to HHS and actions taken in response to such breaches.

The FTC proposed rule has very similar notification requirements that would apply to vendors of personal health records and third party service providers.

### **HITECH Act Enforcement**

Following is a summary of enforcement actions for the new HITECH Act:

- The HITECH Act makes any violation of its new requirements and prohibitions subject to HIPAA's civil and criminal penalties.
- The HITECH Act also requires HHS to conduct periodic audits.



## **HIPAA Civil Money Penalties**

- The HITECH Act increased the maximum civil penalties for all violations.
- The minimum penalties were also increased and tiered according to the level of knowledge and the egregiousness of the neglect. If the person did not know of the violation and could not have known by reasonable diligence, the minimum penalties are \$100 per violation, up to \$25,000 per calendar year.
- If the person did not know of the violation and could not have known by reasonable diligence, the minimum penalties are \$100 per violation, up to \$25,000 per calendar year.
- If the violation was due to a reasonable cause and not to willful neglect, the minimum penalties are \$1,000 per violation, up to \$100,000 per calendar year.
- If the violation was due to willful neglect, but is corrected within 30 days of discovering it or when with reasonable diligence the person would have known, the minimum penalties are \$10,000 per violation, up to \$250,000 per calendar year.
- If the violation was due to willful neglect, and the violation is not corrected within 30 days of discovering it or when with reasonable diligence the person would have known, the minimum penalties are \$50,000 per violation, up to \$1.5 million per calendar year.
- The HITECH Act increased the maximum civil penalties for all violations regardless of knowledge or level of neglect.
- The maximum penalties are \$50,000 for each violation, up to \$1.5 million per year for all such violations of an identical requirement or prohibition.

## **State Attorney Generals**

- The HITECH Act also authorizes state attorneys general to bring civil actions on behalf of the residents of their states.
- The state attorneys general may sue to stop violations or to obtain money for the residents of their states.

## **HIPAA Criminal Penalties**

- The HITECH Act clarified that criminal HIPAA penalties apply not just to “covered entities” but also to employees and other individuals.
- Persons who knowingly use, obtain, or disclose individually identifiable health information are subject to criminal penalties.



- The maximum criminal fines and imprisonment depend on the specifics of the offense.
- Knowing
  - Maximum \$50,000 fine & 1 year imprisonment
- With false pretenses
  - Maximum \$100,000 fine & 5 years imprisonment
- With intent to sell, transfer or use for gain or harm
  - Maximum \$250,000 fine & 10 years imprisonment

### **The Future of Health Information**

The HITECH Act will lead to increased use of electronic health information. It also increased health information security requirements and enforcement. For more information contact Enterprise Risk Management at (305) 447-6750, or email [info@emrisk.com](mailto:info@emrisk.com), or visit our website [www.emrisk.com](http://www.emrisk.com).

This newsletter should not be construed as legal advice, and readers should consult legal counsel.

## ***ERM wants to hear from YOU....***

With this edition of our newsletter, we're rolling out a new format and new features. Tell us what you think!

What features or topics would you like to see covered in future issues? Who else should receive this newsletter?

Your feedback is welcome and encouraged. Please send your comments to [editor@emrisk.com](mailto:editor@emrisk.com).

## Enterprise Risk Management: *At a Glance*

ERM brings clients the highest level of expertise to assess and address risks, comply with standards and regulations and mitigate risks, using integrated and reasonably priced security services and solutions.

Our practice provides organizations with the tools they need to address the compliance and risk management issues of today, as well as the broader and ever-increasing security challenges of the future.

### Services

- IT Security
- Regulatory Compliance
- IT Audit
- Computer Forensics
- Risk Management
- Attestation

### Certifications

- Certified Public Accountant (CPA)
- Certified Information Systems Security Professional (CISSP)
- Certified Information Systems Auditor (CISA)
- Certified Information Systems Manager (CISM)
- Certified Information Technology Professional (CITP)
- GIAC Security Essentials Certification
- GIAC Systems and Network Auditor
- Qualified Security Assessor (QSA)
- Approved Scanning Vendor (ASV)

### Some of our Clients

- ABN-AMRO Private Banking
- Bacardi-Martini, Inc.
- Bancafe International
- Banco Industrial de Venezuela
- Banco ITAU
- Bank United
- Caja Madrid Bank
- Carnival Cruise Lines, LLC
- CitiBank
- Coconut Grove Bank
- Commerce Bank
- E-data Financial
- Florida International University
- Florida Power & Light Company
- Heico Aerospace
- Helm Bank
- Knight Ridder
- Nova Southeastern University
- Rinker Materials
- Rudy, Exelrod & Zieff, LLP
- Seabourn Cruise Line
- TecniCard, Inc.
- The International Bank of Miami
- TransAtlantic Bank
- U.S. Century Bank

For more information, visit [www.emrisk.com](http://www.emrisk.com)

E-mail: [info@emrisk.com](mailto:info@emrisk.com)

Phone: 305-447-6750

800 Douglas Road

North Tower, Suite 835

Coral Gables, FL 33134

**enterprise risk management**

*The Control Professionals*