WHITEPAPER

HITECH Act and the HHS Rules

An Assessment of the New Healthcare Privacy Regulations

Revision 2.0
March 2011
Incorporating the HHS Breach Notification Interim Final Rule

idexperts®

According to a 2010 study by the Ponemon Institute, data breaches are costing the healthcare industry nearly $6 billion a year,[1] risking the medical and financial well being of breach victims and the credibility and future business of the healthcare provider. To help protect against breach of personal medical information, the Health Insurance Portability and Accountability Act (HIPAA), enacted in 1996, set standards for medical privacy that went into effect over the next 10 years. The American Recovery and Reinvestment Act (ARRA), signed by President Obama in February 2009, put into law new privacy requirements that experts have called "the biggest change to the healthcare privacy and security environment since the original HIPAA privacy rule."[2]

Title XIII of ARRA, the Health Information Technology for Economic and Clinical Health (HITECH) Act, seeks to streamline healthcare and reduce costs through the use of health information technology. The HITECH Act dedicates over $31 billion in stimulus funds for healthcare infrastructure and the adoption of electronic health records (EHR), including funding for the meaningful use incentive programs. To ensure that privacy and data security go hand in hand with the digitization of health records, healthcare organizations must be in compliance with the HIPAA Privacy and Security Rules (45 CFR Parts 160 & 164) by establishing a risk management process and conducting annual risk assessments.

The HITECH Act also imposes new requirements, including:

- Extension of the HIPAA privacy and security requirements to include business associates.
- Expansion of contractual obligation for security and privacy of PHI to subcontractors of business associates.
- Specific thresholds, response timeline, and methods for breach victim notification.
- Tiered increase in penalties for violations of these rules, some of them mandatory, with potential fines ranging from $25,000 to as much as $1.5 million, effective immediately.
- Provisions for more aggressive enforcement by the federal government.
- Explicit authority for state Attorneys General to enforce HIPAA rules and to pursue HIPAA criminal and civil cases against HIPAA-covered entities (CEs), employees of CEs, or their business associates.
- Requirement for the Department of Health and Human Services (HHS) to conduct mandatory audits.

Unlike HIPAA, the HITECH Act allowed only one year for most provisions to be enforced, with some provisions immediately effective as of the February 17, 2009, enactment date and some that became effective a few months later.

On September 23, 2009, the Department of Health and Human Services issued guidelines on the HITECH Act, known as the Interim Final Rule for Breach Notification.[3] This rule, among other things, includes a controversial "harm threshold" that gives CEs the responsibility for determining whether notification is required. The HHS submitted a Final Rule for review to the Office of Budget and Management, only to withdraw it in July 2010. While the Final Rule is anticipated in 2011, the provisions in the Interim Final Rule remain in effect, and must be followed for compliance. Healthcare organizations and their BAs need to act now to implement compliance systems and processes.

The Edicts and the Impacts

The HITECH Act's privacy and security obligations — and the associated HHS rules — create requirements that affect every aspect of your operations, and compliance could entail considerable resources and cost. It is critical to understand the requirements and their impact, so you can protect your organization while minimizing expenses.

Changes to Medical Privacy Requirements

While HITECH extends the privacy provisions of HIPAA, there are fundamental changes in the areas of accountability, data breach notification, consumer access, and use of personal health information. New rules by the Department of Health and Human Services have also added privacy requirements.

Accountability

The HITECH Act imposes new levels of accountability for medical privacy, and it extends accountability far beyond previous requirements.

Under HIPAA, healthcare organizations — "covered entities" (CEs), in HIPAA parlance — were required to be in compliance with current federal and state laws regarding data security, but they were not actively audited, and there was no defined penalty structure for companies that had neglectful privacy practices.

Under the HITECH Act, the Secretary of the Department of Health and Human Services (HHS) is directed to conduct periodic audits to ensure compliance with the new rules. There is an increased, tiered penalty structure, with fines ranging from $25,000 to $1.5 million, and penalties are mandatory for cases of "willful neglect." All violations occurring after the February 2009 enactment date are subject to the increased penalties. "Proof of harm" is no longer required to levy penalties or further mandates, and interpretation of breach cases (for example, what constitutes "willful neglect") and determination of penalties will be made by individual state Attorneys General.

HITECH also extends privacy and security requirements beyond HIPAA-covered entities. Business associates of an organization holding Personal Health Information (PHI)[4] are bound by the same requirements as the CE. (This requirement may help mitigate risks for both healthcare consumers and CEs. According to PriceWaterhouseCoopers, 52 percent of organizations report that business partners weakened by the recent economic downturn pose the greatest increase in security risk.[5])

HITECH is still the "federal floor" on medical privacy: it does not supersede state laws that are more stringent. However, it does give state Attorneys General explicit authority to enforce HIPAA rules and to pursue HIPAA criminal and civil cases against employees of CEs or their business associates.

Breach Notification

The HITECH Act defines a breach — with certain exceptions — as "the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information." Under HIPAA, breach notification requirements were fairly loose:

- State security breach laws typically mandated notification only for breach of electronic PHI such as computer records.
- After a data breach, the burden of notification fell on "data owners," a general definition excluding any organization that did not technically "own" the data.
- If the data owner determined that it had an obligation to notify of a data breach, it was required only to send letters to the affected individuals within "a reasonable amount of time," leaving the details to state laws that tended to be ambiguous as to the content and distribution of the notifications.

Under HITECH, the administrative burden of proof (45 CFR §164.414) is placed on the covered entity, which now has the obligation to document and investigate all breaches that are discovered on or after September 15, 2009 and to notify according to this new subpart. First, the HIPAA-covered entities must provide notification within 60 days when PHI in any form or medium is breached, not just electronic records. The rules clarify that a breach is officially discovered on "the first day it is known to the HIPAA-covered entity or business associate or should reasonably have been known." The notification requirements are specific in terms of content, timing, and obligations to ensure contact with affected individuals, and there is an imposed burden of proof on the HIPAA-covered entity that suffered the breach to demonstrate that all required notifications were made, and that telephone notifications were made in urgent situations. If a business associate experiences a breach, it must notify the covered entity immediately and facilitate the CE's investigation.

The obligation to notify falls on any HIPAA-covered entity that "accesses, maintains, retains, modifies, records, stores, destroys or otherwise holds, uses or discloses unsecured protected health information."

Should a breach impact more than 500 individuals, the CE is required to provide "contemporaneous" notice to the Secretary of the Department of Health and Human Services (HHS), making the breach notice public. Additionally, if 500 or more individuals are affected in a single state or jurisdiction, notice must be provided to prominent media outlets. In cases of less than 500 individual records, the entity must maintain a log of such breaches and submit the log annually, within 60 days of the end of the calendar year, to the Secretary of the Department of HHS, which will publish the information on a public web site. Public disclosure obligation can be required even at a much lower threshold than previously. For example, if 10 or more individuals affected by the breach have out-of-date contact information, the CE must post a notice on its Web site and in major print or broadcast media in geographic areas where the individuals are likely to reside. The bottom line is that all breach incidents, regardless of size, will become part of the public record and made available through HHS.

Under the Interim Final Rule, the notification requirements changed yet again with the addition of the "harm threshold" — in which a breach ''poses a significant risk of financial, reputational, or other harm to the individual.''[6] A covered entity is responsible for determining if a breach crosses that threshold, and if notification is required. The Rule also requires documentation supporting an organization's decision to notify or to not notify.

Consumer Access

The HITECH Act gives individuals clear access rights to their own health records, and it gives them the right to restrict disclosure of PHI if they pay for the healthcare services themselves.

Use of PHI

HITECH requires CEs and their business associates to limit the use and disclosure of PHI to the "minimum set" necessary to accomplish the intended purpose. CEs and their business associates are also prohibited from selling PHI without explicit, documented authorization from the individual whose information is contained in the record.

HITECH Act/HHS Rules Privacy Requirements and Impacts

	HITECH Requirement/HHS Rules	Impact	Effective Date
Accountability	Increased and mandatory penalties for privacy and security violations	• Violations can bring fines up to $1.5 million	February 17, 2009
	State Attorneys General have explicit authority to enforce HIPAA and HITECH regulations	• Higher likelihood of enforcement and penalties	February 17, 2009
	Business associates (BAs) of HIPAA-covered entities (CEs) are bound by the same HIPAA privacy and security requirements as CEs	• Business associates must bring business systems and processes into compliance with HIPAA privacy and security requirements • CEs must revise contracts with BAs to reflect HIPAA requirements	February 17, 2010
	Subcontractors will likely be bound by the same HIPAA requirements as business associates who have contracts with a covered entity	• Business associates should prepare to enter into business associate contracts with their subcontractors that implement current requirements, and that are flexible for the future	Proposed in the Notice of Proposed Rulemaking and the pending Final Rule
Breach Notification	Mandatory notification of breach victims within 60 days	• Healthcare providers need breach response plans in place • Penalties for failure to notify	September 15, 2009
	Obligation to notify of breach extends to business associates of CEs	• BAs need breach response plans in place • BAs are subject to the same penalties as CEs	September 15, 2009
	All breach incidents become part of public record through the Department of Health and Human Services (HHS)	• CEs must report ALL breach incidents to HHS either "contemporaneously" or annually, based on the size of the breach	February 17, 2010
	New "harm threshold" provision requires CEs to determine if notification is required	• CEs must have processes in place for determining if a breach meets the "harm threshold" criteria • CEs need to conduct and document an incident risk assessment supporting their decision to notify or not notify	September 23, 2009

Consumer Access	Individuals are guaranteed prompt access to their own health records	• Healthcare providers must be able to quickly access and deliver all electronic and other information in an individual's health record	February 17, 2010
	Individuals can restrict disclosure of their records when they pay for their own medical services	• Healthcare providers must institute effective checks on distribution of individual patients' PHI	February 17, 2010
Use of PHI	CEs and their BAs must limit the use and disclosure of PHI to the "minimum set" necessary to accomplish the intended purpose	• CEs and BAs need an accurate inventory of PHI used in their business processes • CEs and BAs need to review procedures and determine how to meet "minimum set" requirements	February 17, 2010

Organizational and Business Impacts of HITECH and the HHS Rules

The requirements of the HITECH Act and the HHS rules have had considerable impact on HIPAA-covered healthcare organizations and possibly an even greater impact on their business associates that were not previously covered.

The first and most obvious impact is increased risk of litigation and fines. With heightened oversight and enforcement, and significantly greater penalties for non-compliance, CEs and their business associates will want to prepare to comply with these new requirements. A number of state Attorneys General and state agencies have already exercised their authority under HITECH to prosecute offenders:

- In 2010, the Connecticut Attorney General sued Health Net of Connecticut for the breach of 446,000 members' PHI and financial information — and for waiting six months to notify the affected population and the authorities. The company settled for $250,000, plus it established a $500,000 reserve for victims' claims. In addition, the Connecticut Insurance Department fined the insurer $375,000. Health Net also settled a complaint with the Vermont Attorney General for $55,000 for the same breach.

- In another case, the California Department of Public Health fined the Lucile Packard Children's Hospital at Stanford $250,000 for allegedly reporting a data breach 11 days late. California has been especially aggressive in levying fines for breaches — $675,000 against five hospitals in a single day.

According to the International Association of Privacy Professionals (IAPP)[7], the other major challenges posed by ARRA for healthcare organizations are:

- Re-evaluation of existing practices in light of the new requirements: Because penalties and breach notification requirements now impact all forms of PHI, CEs will need to reassess where and how this information is used and stored throughout their organizations, and also how to de-identify it to meet "minimum set" requirements. Meeting new security requirements needs a thorough risk assessment which may involve significant overhaul of business processes, new personnel processes and security training, possibly major changes to IT systems, and even changes to the physical facility.

- Designing and implementing a business associate strategy: The HITECH Act requires security requirements to be written into agreements between CEs and their business associates, and this will naturally require significant legal and contract administration efforts. But because CEs and their business associates are now mutually accountable for security violations and breaches, businesses will also need to review with each partner how they exchange, use, and protect information. Both processes and data system interfaces may need to be overhauled.

- Dealing with breach notification issues: One likely impact of the HITECH requirements will be that organizations suffering small-scale data breaches will now be obligated to notify in each instance, and to keep detailed proof of notification, causing significant effort and cost.

Planning for Compliance

Unlike HIPAA, the HITECH Act and the HHS rules do not allow 10 years for compliance. Increased enforcement of HIPAA requirements and breach notification requirements are effective now, so there is no time to waste in planning for compliance.

Three immediate steps will provide a solid and comprehensive foundation for compliance with these regulations:

- Conduct a thorough, annual risk-based assessment of current privacy and security policies and practices related to your PHI assets and lifecycle.

- Investigate, document, and track all privacy and security incidents using tools and objective incident assessment procedures.
- Create and implement a comprehensive incident response plan for data breach notification.

Given the time and effort it takes to achieve compliance, it helps to have tools in place to support your plan. ID Experts offers a Healthcare Incident Response Plan — to help you establish a documented plan before an incident — and an incident assessment and reporting tool called RADAR™ that helps demonstrate readiness and supports your compliance when an incident happens. These tools also support any covered entity's compliance requirements to qualify for meaningful use incentive funds.

Data Breach Protection

A recent survey by PriceWaterhouseCoopers revealed that only 40 percent of organizations in North America have an accurate inventory of where personally identifiable information (PII) in their custody is stored[8], and with the complex web of organizations involved in providing healthcare services, this is even more of an issue in the healthcare industry. The obvious problem here is that you can't adequately protect information if you don't know you have it. In fact, the Ponemon Institute reports that 58 percent of healthcare organizations "have little or no confidence" in their ability to identify "all patient data loss or theft."[9]

Risk-based assessment gives an accurate inventory of the PII/PHI data you hold and all internal and external workflows where the information is used. It provides a comprehensive view into PII/PHI-specific risks throughout your IT systems, organization, policies and processes, and it identifies BAs that have access to the information. With this assessment and inventory in hand, you will be prepared to ensure that information is "secured" — in other words, protected through a technology or methodology specified by the Secretary of Health and Human Services pursuant to the HITECH Act. Proper data security will protect patients and it helps you avoid breach notification requirements that apply to "unsecured PHI."[10] It will also help you identify which business partnerships pose the highest breach risk, enabling your legal team to prioritize contract revision and your operations team to review and strengthen those processes.

According to Kirk Nahra of Wiley Rein LLP, the HITECH approach of mixed state and federal oversight also "creates realistic risks of differing standards and inconsistent action from state to state."[11] An expert risk-based assessment will include regulatory review to determine applicable federal and state privacy regulations, including how HITECH will apply to various business activities, from direct services to marketing. To ensure continued compliance, experts recommend an annual risk-based assessment that addresses PHI privacy and security obligations.

Implementing systems and processes to meet HITECH requirements may be costly, and an accurate picture of data usage and risks will enable you to prioritize privacy protection strategies and expenditures to achieve the best protection for the investment. And with costly penalties for non-compliance, bringing in an expert to conduct risk-based assessment provides a fast, accurate means to achieve compliance. This expert assessment is crucial, since more than half of organizations surveyed in a recent HIMSS Analytics report say that their assessments do not include all aspects of the security environment.[12]

ID Experts offers privacy and regulatory risk assessment and mitigation by IAPP-certified experts, providing insight into your PII/PHI data-specific risks, recommendations on policies and procedures, and best practices on managing PHI to reduce your organization's exposure to a data breach.

Data Breach Response

In healthcare, trust is critical. In addition to penalties and other risks of non-compliance, data breaches hurt your organization's credibility and can carry huge medical and financial risks to the people whose data is lost. And under HITECH, the number of data breaches discovered is bound to increase. According to one industry expert, that number already has grown.[13] To date, there are about 240 incidents on the HHS list of data breaches that affect more than 500 individuals.

An effective breach response process can help restore credibility and avoid litigation. Given the need for HITECH and HIPAA compliance, the 60-day window for breach notification, and the high penalties for non-compliance, effective breach planning is now even more critical.

For many organizations, the best way to meet new requirements and avoid fines and investigations is to work with a breach response specialist who can help ensure full compliance with HITECH, HIPAA, and state requirements. The best of these vendors can provide turn-key notification services, including call centers and mail notification, with experience creating tailored notification and advisory services for breach victims with special needs, such as elderly patients or those with mental health issues or physical disabilities. They can track delivery of breach notification, providing you with proof of compliance. They can also provide recovery services for individuals who become victims of identity crime, helping victims restore their medical identities to pre-theft status and helping your organization retain client trust and credibility and avoid costly litigation.

Under the Interim Final Rule, your organization is responsible for determining if a breach crosses the "harm threshold" for the people whose data is lost or compromised. Whether or not you choose to notify, you'll need documentation to support your decision. The ID Experts RADAR tool steps you through documentation and evaluation of a privacy or security incident, to help you determine whether the incident is indeed a breach and whether notification is required based on the "harm threshold" criteria.

Preventive Care for Your Organization

The HITECH Act and HHS rules create new requirements that affect every aspect of your operations: business and healthcare processes; information technology and data security, retention, and monitoring; contracts and business relationships. With increased enforcement and costly penalties, there is no time to waste in planning for compliance.

A risk-based assessment offers the fastest, most effective, and most cost-effective approach to preparing for timely compliance and risk mitigation. Additionally, putting in place a breach response plan that meets your needs under the new HITECH and HHS obligations will save time and money, and protect your business reputation. By engaging expert help, you can get started on these first steps towards compliance and preparedness in the event of an incident at a very reasonable expense and with minimal disruption to your organization. The most important step is to get started now.

About ID Experts®

ID Experts is the leader in comprehensive data breach solutions that deliver the most positive outcomes. The company has managed hundreds of data breach incidents, protecting millions of affected individuals, for leading healthcare organizations, corporations, financial institutions, universities and government agencies. In healthcare, the company contributes to relevant legislation and rules including HITECH and is a corporate member of HIMSS. ID Experts is active with organizations that advocate for privacy for Americans including ANSI/Identity Theft Prevention, Identity Management Standards Panel and the International Association of Privacy Professionals. For more information, visit www2.idexpertscorp.com.

Contact Us

ID Experts®
Lincoln Center One
10300 SW Greenburg Road, Suite 570
Portland, OR 97223

p: 866.726.4271
f: 800.298.8457
www2.idexpertscorp.com
info@idexpertscorp.com

1. "Benchmark Study on Patient Privacy and Data Security," November 9, 2010, Ponemon Institute LLC.
2. Kirk J. Nahra, Wiley Rein LLP, and Rick Kam and Mahmood Sher-Jan, ID Experts. "Ready for Data Breaches Under the HITECH Act?" Webinar. May 27, 2010.
3. See "Breach Notification for Unsecured Protected Health Information; Interim Final Rule" at http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf.
4. In the context of medical privacy laws, this is also sometimes called Protected Health Information (PHI) or Individually Identifiable Health Information (IIHI).
5. "Findings from the 2011 Global State of Information Security Survey." PriceWaterhouseCoopers.
6. See "Breach Notification for Unsecured Protected Health Information; Interim Final Rule" at http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf.
7. Deven McGraw and Kirk J. Nahra. "Healthcare Privacy and the New Federal Stimulus Package: Understanding the Requirements." Presentation to the International Association of Privacy Professionals. March 5, 2009.
8. "Findings from the 2011 Global State of Information Security Survey." PriceWaterhouseCoopers.
9. "Benchmark Study on Patient Privacy and Data Security," November 9, 2010, Ponemon Institute LLC.
10. See "Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals" (http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html) for guidelines on securing PHI.
11. Kirk J. Nahra. "A New HIPAA Era Emerges." Wiley Rein LLP, February 2009.
12. 2009 HIMSS Analytics Report:"Taking a Pulse on HITECH, Are Hospitals and Business Associates Ready?" November 17, 2009.
13. "ITRC 2010 Data Breach Report Indicates Mandatory Reporting on Horizon," by Denise Richardson, January 4, 2011, http://www.givemebackmycredit.com

© 2011 ID Experts®. All rights reserved.