



HITECH and HIPAA: Missteps Will Cost You and Your Patients

By Kathleen LePar, Vice President Professional Services and Rachel Hudspeth, Senior Consultant

Health Information Technology (HIT) is constantly evolving and morphing to meet the needs and demands of the global healthcare community. For several decades there have been optimistic dreams of some form of a national, or potentially global, electronic health record (EHR). With the passage of time and each new administration in the United States, the view of this dream is becoming more clear.

As this dream becomes closer to reality, new rules, regulations and consumer laws will be necessary to assure the public that medical records are secure and their privacy is being maintained. In fact, the privacy and security of the EHR has come into question, when, for all intents and purposes, an EHR should prove to be much safer than the paper versions that found themselves in everyone's hands. So now is time to dust off the Health Insurance Portability and Accountability Act of 1996 (HIPAA) compliance policies and, yes...take them seriously!

Health Information Technology for Economic and Clinical Health Act (HITECH)

HITECH was passed by Congress on February 13, 2009 and was signed into law by President Obama on February 17, 2009. This bill was designed to address four major objectives that advance the use of HIT, such as EHRs, by:

1. Requiring the government to take a leadership role to develop standards by 2010 that allow for the nationwide electronic exchange and use of health information to improve quality and coordination of care.
2. Investing \$20 billion in HIT infrastructure and Medicare and Medicaid incentives to encourage doctors and hospitals to use HIT to electronically exchange patients' health information.
3. Saving the government \$10 billion and generating additional savings throughout the health sector through improvements in quality of care and care coordination and reductions in medical errors and duplicative care.
And now, the quietly slid-in nuances and, by the way, long-awaited teeth to HIPAA...
4. Strengthening federal privacy and security law to protect identifiable health information from misuse as the healthcare sector increases use of HIT.

As a result of this legislation the Congressional Budget Office estimates that approximately 90% of doctors and 70% of hospitals will employ comprehensive EHRs within the next decade. Due to the anticipated increase of EHRs, many people have voiced concern over the future privacy and security of an individual's healthcare record, and the mainstream media has possibly added to a national apprehension. Thus the importance of shoring up HIPAA compliance within your facility is a top priority, not only to calm the nerves of the public, but also to ensure compliance with the legal requirements.

In order to give HIPAA teeth, stricter requirements, along with stiffer penalties for non-compliance, are being imposed. HITECH is certainly not the old HIPAA we knew and gave lip service to – not even close. Even though we are still misspelling the acronym, the one thing that will not be misspelled is the healthcare organization's name on the federal Department of Health and Human Services (DHHS) Website or when given to the media when breaches are encountered (if a breach affects more than 500 individuals of a particular state).

HITECH amends the civil monetary penalty (CMP) provisions for HIPAA violations to include tiered increases in amounts as follow.

- **Tier A** is for violations in which the offender did not realize he or she violated the Act and would have handled the matter differently if he or she had. This results in a \$100 fine for each violation, and the total imposed for such violations cannot exceed \$25,000 for the calendar year.
- **Tier B** is for violations due to reasonable cause, but not "willful neglect." The result is a \$1,000 fine for each violation, and the fines cannot exceed \$100,000 for the calendar year.
- **Tier C** is for violations due to willful neglect that the organization ultimately corrected. The result is a \$10,000 fine for each violation, and the fines cannot exceed \$250,000 for the calendar year.
- **Tier D** is for violations of willful neglect that the organization did not correct. The result is a \$50,000 fine for each violation, and the fines cannot exceed \$1,500,000 for the calendar year.

As well as increased penalties under HITECH, patients will now be able to have their medical privacy breach allegations heard in court. HITECH will enable State Attorney Generals to begin the pursuit of civil actions regarding HIPAA violations that threaten or adversely affect an individual. This potential exposure to covered entities for penalties, fines and damages is significantly increased under HITECH.

Timelines for compliance with the new amendments to HIPAA guidelines are as follows.

Upon HITECH enactment (February 17, 2009)

Application of new tiered civil penalties based on the nature of HIPAA violations, up to \$50,000 per violation and an annual maximum of \$1.5 million (Section 13410).

Within 180 days of enactment (August 17, 2009)

DHHS and the Federal Trade Commission (FTC) will promulgate interim final regulations on notification of breaches. The FTC rules will apply to breach notification by Personal Health Records (PHRs) that are not covered by HIPAA or business associate agreements (Section 13402, 13407).

24 months post-enactment (February 17, 2011)

Clarification of ability to pursue civil penalties when criminal penalties are not pursued (Section 13405).

36 months post-enactment (February 17, 2012)

The Secretary of the DHHS is obligated to establish regulations that will allow individuals harmed by privacy and security violations to receive a percentage of any CMP or monetary settlement collected with respect to such offense.

Just a Glimpse of How HITECH Will Affect Your Current HIPAA Policies and Procedures

Accounting of Disclosures with EHRs

The use and disclosure of Protected Health Information (PHI) through EHRs by covered entities is required to provide individuals with an accounting, when requested, for the prior three-year period. Uses and disclosures of PHI through EHRs include treatment, payment and healthcare operations. Covered entities with EHRs may need to begin accounting for disclosures as early as January 1, 2011, depending on when they acquire and begin use of EHR.

Access Rights (Electronic Format)

The HIPAA Privacy Rule is amended now to allow individuals the right to obtain access to their PHI in electronic format, when requested, if the covered entity maintains an EHR. HITECH also permits individuals to designate another person or entity to be the recipient of the transmittal of such electronic PHI.

Security Breach Notification Requirements

Currently HIPAA does not directly obligate covered entities to notify patients of unauthorized uses or disclosures of their PHI. Covered entities have used their discretion to determine whether their duties to mitigate known harm that could result from unauthorized use or disclosure would trigger the duty to notify patients. HITECH removes most of this discretion, mandating notification in certain circumstances. Now covered entities, business associates and vendors who handle PHRs are required to comply with breach notification requirements. Violations of this requirement by vendors would be treated as an unfair and deceptive act or practice in violation of the FTC.

WARNING: if a breach affects more than 500 individuals of a particular state, notification must also be provided to prominent media outlets following the discovery of the breach.

Business Associates

HITECH affects business associates and requires that all comply with the administrative, physical and technical safeguard requirements, to include policies and procedures of how PHI is handled. If the requirements are not met, monetary penalties can be assessed directly against the business associate.

A business associates is defined as a person who performs functions or activities on behalf of, or provides the specified services to or for, an organized healthcare arrangement in which the covered entity participates. A business associate may be a covered entity. The definition of business associate excludes a person who is part of the covered entity's workforce [45 CFR160].

Obviously the above requirements/changes are only examples and do not reflect the comprehensive listing within the official HITECH Act.

Why You Need to Prepare

Audits will be common, not exceptional.

HITECH requires DHHS to conduct periodic audits of both covered entities and business associates to ensure HIPAA compliance. If your organization were audited tomorrow, how would you fare with the new regulations?

- Are you aware of the expanded scope of HIPAA under the new HITECH provisions?
- Have you identified all of the State Breach Laws with which you may need to comply, including the Federal Breach Notification Policy concerning patients who live in different states?
- When was the last time you took a solid look at your HIPAA policies and compliance with HIPAA?
- Have you identified risks to your organization in regard to breaches?

- Are your employees aware of all changes, including their responsibility and the penalties that they can incur as a result of noncompliance?
- Will your patients feel that their PHI is just that, protected?

Potential areas of the DHHS Audit include:

- Red Flag Rules
- Breach Notification
- Compliance Program
- Existing business associate agreements. Do you need to review and/or revise?
- Policies and procedures regarding all changes in HIPAA
- Training Program

The deadlines for the majority of the HIPAA legislation is February 2010, and, while you may think that this is doable, remember that time flies, and there is a lot to be done. Of course you may feel that the HIPAA compliance efforts that you took part in years ago are pristine and diligently followed, and, if that is the case, I applaud you.

Even better, if that is the case, your organization should survive the ad hoc audits by DHHS. However,

if that is not the case, this is the time to come to your senses and do it right; inform your employees that each and every one of them will be held accountable and identify the best strategies for compliance. If you have existing holes, this is the time to plug them and put in processes that will ensure that your patients' EHRs are secured and privacy is placed at the top of your priorities.

If you are considered a business associate, you must certainly understand that your work is cut out for you, as your organization does not have the same lengthy timeline as the covered entities did with the original HIPAA, so it is strongly suggested that you start now to ensure compliance.

One last thought

Due to the economic times the industry is experiencing, fines due to the lack of preparation and clear understanding of the new requirements are a price that you cannot afford to pay. *What could be worse - exposing your patients' PHI, by rendering it UNPROTECTED?*

Kathleen LePar, RN, MBA, is a Vice President for Beacon Partners. Rachel Hudspeth is a Senior Consultant. For more insight on HIPAA and HITECH, please contact klepar@beaconpartners.com or rhudspeth@beaconpartners.com.

Beacon Partners is one of the fastest-growing privately-held healthcare management consulting firms, coaching organizations in the development of strategies that are centered on maximizing Enterprise Yield performance. To achieve top levels of performance, an organization must factor strategic direction, physician alignment, economic incentives and overall market impact. Our experience has proven that focus on these critical success factors will strengthen an organization's position in the market and, ultimately, improve the patient's experience with the provider.

Please visit <http://www.beaconpartners.com> and Beacon Partners' special healthcare informational portal, <http://www.spotlightonhealthcare.com>.

1.800.4BEACON | www.beaconpartners.com
BOSTON • SAN FRANCISCO • TORONTO