Oregon Healthcare News

orhcnews.com | Articles, Interviews and Statistics for the Healthcare Executive

HITECH "Check-up": Where are you on the Road to Compliance?

By Paul Frisch
Senior Compliance Consultant
Apgar and Associates, LLC

Readers of the Oregon Healthcare News are undoubtedly familiar with changes to HIPAA included in the HITECH Act, creating new privacy and security requirements and enhancing current enforcement tools. This article is intended to help organizations take a step back to reasonably ensure they are compliant with HIPAA/HITECH and if not, what key risk areas to address first.

As often is the case, many who are intimately involved with compliance sometimes miss critical compliance issues within our own organizations. Following are key provisions that change the compliance landscape and a roadmap that can assist in a timely meeting of compliance requirements.

- Business associates are now subject to HIPAA security rule and the use and disclosure provisions of the privacy rules and are directly subject to civil and criminal penalties;
- Breaches of unsecured protected health information (PHI) now require written notice to individuals of the breach and the US Department of Health and Human Services (HHS), Office for Civil Rights (OCR);
- Individuals can now request an electronic copy of medical or claims records maintained by providers or other covered entities;
- New civil enforcement authority has been granted to state attorneys general;
- OCR is required to conduct privacy and security compliance audits of covered entities and business associates of all sizes; and
- Civil penalties for HIPAA violations have increased up to $50,000 per violation, and up to a maximum of $1.5 million for the same type of violation per calendar year.

Congress vested OCR with the power and means to significantly increase HIPAA enforcement activities and, in some cases, enforcement is mandated. As an example, when a complaint is filed with OCR and alleges willful neglect, OCR must investigate. February 17, 2010 was the deadline for adopting most of the new HITECH related policies, procedures and practices. Even though OCR recently published a draft rule clarifying the meaning of privacy, security and enforcement changes that is not yet in effect, many provisions of HITECH are in effect now. It is not wise to delay compliance activities until after the OCR rule has been finalized (likely not until the end of 2010).

Audits and Potential Enforcement Actions

OCR is required to regularly audit covered entities and business associates to assess HIPAA/HITECH compliance which may result in

formal or informal rule enforcement as an audit outcome. It is likely OCR will publish information about the new audit program the latter part of this year with audits starting in 2011.

Now that state attorneys general have the authority to bring suit in federal district court against any individual or entity violating the rules on behalf of state residents and potentially seek damages on behalf of residents, the Connecticut Attorney General has used the new enforcement power to do just that involving Health Net. It is likely the healthcare industry will see more such actions in the not too distant future.

Enhanced Civil Penalties

Civil penalties are now a maximum of $50,000 per incident and a maximum of $1.5 million per calendar year for any violation. OCR's new draft rule, while not final, does include information regarding how OCR intends to enforce HIPAA/HITECH privacy and security requirements. OCR indicated it is likely if a covered entity or business associate is found guilty of willful neglect, enforcement will move immediately from informal to formal. There has been a clear line drawn between unknowingly or inadvertently violating the rules and knowingly violating the rules.

Movement to formal enforcement means covered entities or business associates may find themselves required to adhere to a formal corrective plan, subject to higher civil penalties or both. It has been said that willful neglect may be difficult to prove. That is not necessarily true.

As an example, the first HIPAA security rule administrative simplification requirement is to conduct a risk analysis on a periodic basis. Most healthcare organizations have not conducted a risk analysis or have not for some time. This can relatively easily be viewed as willful neglect – the organization knew it was required to conduct a risk analysis periodically but did not. This is a case where ignorance is no longer an excuse.

Security Breach Notification Requirements

As most healthcare organizations know, HITECH created the first comprehensive breach notification requirements for the breach of PHI. HITECH and the related rule require individual notification, OCR notification and potentially media notification in the event of a breach.

If a breach occurs and it involves 500 individuals or more, OCR is currently posting the names of entities experiencing the breach on a public web site. Breach notification aside, announcement of a breach of PHI is a good way for an organization to find its way onto the radar of OCR and state attorneys general, open the door to law suits, become a headline in local and national media and damage the reputation of the organization. Often regulatory costs associated with breaches and other security events are small in comparison to things like legal risk and business or brand damage.

How much progress have covered entities and business associates made?

Here is a brief checklist to self-assess whether a healthcare organization may be in violation of the HIPAA Privacy and Security Rule and potentially guilty of "willful neglect." A "no" answer places the organization in the "non-compliant" or "guilty" column.

1. I have conducted a risk analysis and developed the appropriate mitigation plans within the last year.
2. I have performed a privacy and security compliance audit of my organization within the last year and regularly conduct periodic audits.
3. I am familiar with and have implemented HHS's guidance for securing PHI.
4. I have a privacy and security officer.
5. Our policies and procedures address HIPAA Privacy and Security Rule requirements;
6. We have proof all workforce members attend regular on-going privacy and security training at least annually.
7. We consistently document efforts to reasonably ensure the privacy and security of PHI.
8. Our disaster recovery and emergency mode operations plans are up to date, regularly tested and workforce members know their responsibilities in the event of a disaster.

What are some "next steps"?

The top risks facing most covered entities and business associates that need to be addressed quickly include:

- Conducting a risk analysis
- Conducting an annual compliance audit and periodic audits
- Reasonably ensuring policies and procedures are current, accurate, enforceable and communicated

- Reasonably ensuring privacy and security training is current and accurate, all new workforce members are trained and refresher training is conducted annually
- Disaster recovery and emergency mode operations plans that address technical and business requirements and assure that the plans are regularly tested and updated
- Amending Business Associate Contracts (BAC) to reasonably ensure a business associate's compliance with and knowledge of all relevant provisions of the regulation
- Encrypting Electronic PHI when transmitted across the Internet and on laptops and other portable media that leaves the office

Many organizations are not compliant with HIPAA and HITECH. If external assistance is required in the areas of compliance assistance and auditing, or organizations are considering outsourcing compliance duties, one option is to contact Apgar & Associates, LLC to obtain a review of current privacy and security compliance programs and determine if you are interested in contracting out all or a part of your compliance activities. Apgar & Associates, LLC offers, among other services, virtual compliance officer services which give healthcare organizations access to compliance support. For more information, see our web site at www.apagarandassoc.com.

Paul Frisch is the Senior Compliance Consultant for Apgar and Associates, LLC. He can be reached at paulfrisch@apgarandassoc.com.

Chris Apgar, CISSP
President

Phone: 503-977-9432
Fax: 503-245-2626
Mobile: 503-816-8555
E-mail:
capgar@apgarandassoc.com

10730 SW 62nd Place
Portland, OR 97219
http://www.apgarandassoc.com

Apgar & Associates, LLC

Quality Compliance Resources

Apgar & Associates, LLC offers the highest quality service assisting healthcare organizations establish sound privacy and security programs, meet regulatory requirements, address legal and regulatory issues and assist in planning deployment of health information technology, electronic health records, personal health records and health information exchange planning. Check out Apgar & Associates, LLC's web sites for a full list of services offered.

Check out enhanced virtual compliance officer services for organizations of all sizes

Reprinted with permission from the Oregon Healthcare News. To learn more about the Oregon Healthcare News visit orhcnews.com.