

What's Keeping Health Care Leaders Up at Night?

Privacy breach detection, notification and accounting of disclosure are on the minds of many.

By Kurt Long

Posted on November 4, 2009

Privacy legislation is requiring health care entity leaders to think differently about how to protect the privacy data of its patients. And, in the case of a breach, these leaders must be equipped to meet legal requirements of notification, tracking and disclosing information about the breach, and demonstrating its willingness and ability to comply with the law. What is keeping health care leaders up at night is how to establish the *right* entity-wide privacy and security plan. One that safeguards against inappropriate access to physical records and puts in place foundational technologies and processes to ensure vulnerabilities are eliminated.

On Feb. 17, 2009, the American Recovery and Reinvestment Act (ARRA), the Health Information Technology for Economic and Clinical Health Act (HITECH) and its associated privacy provisions were signed into law. This ensured that health care entities could no longer turn a blind-eye to inappropriate access of electronic patient records such as "snooping" and other patient-damaging access behaviors. These behaviors also include identity theft and medical identity theft. ARRA HITECH marks a new beginning for U.S. patient rights, which require health care entities to operate under greater transparency and catch-up with their health care peers globally. (Two examples are the United Kingdom Freedom of Information Act and the Ontario Privacy and Freedom of Information Act.)

To ensure compliance, health care leaders must understand ARRA HITECH. ARRA of 2009 Division A/Title XIII/Subtitle D on Privacy may appear complicated, but in fact can be distilled into easy to understand operational principles:

1. **Patients have a right to know who has accessed their personal health information (PHI).** A patient's right to know who has accessed their PHI is now clearly defined in Subtitle D Accounting of Disclosure. Correspondingly, health care entities now have clarification in their obligations to service patient requests. HIPAA outlines almost identical obligations, but ARRA HITECH provides specificity and is backed by increased enforcement risk and punitive down-side.
2. **Breach is clearly defined and notification is required.** Subtitle D defines a privacy breach as "unauthorized acquisition, access, use or disclosure of protected health information that compromises the security or privacy of such information ..." In the event of a privacy breach, under ARRA HITECH, health care entities are now required to notify the patients impacted, the Federal government and under well defined conditions, major media outlets. Furthermore, the "burden of proof" is now on the covered entity to show all notifications were made and without unnecessary delay. In accordance with ARRA HITECH. The breach notification rule went into effect as of Sept. 23, 2009.
3. **Enforcement, Audits and Fines.** ARRA HITECH is specific in terms of fines, which escalate as a health care entity demonstrates willful neglect. Subtitle D outlines increased systematic enforcement and periodic congressional reporting. In parallel, systematic U.S. Health and Human Service HIPAA audits began in 2007, the Piedmont HIPAA being the first, demonstrating that health care entity's forward-looking plans for privacy do not matter. Health care entities must operationalize their privacy and security plans into technologies and business processes to avoid the consequences of material short-comings. In a demonstration of the Federal government's commitment to health care privacy, Health and Human Services (HHS) and the Federal Trade Commission (FTC) issued a press release on Feb. 18, 2009, one day after ARRA was signed into law, announcing that CVS had agreed to pay \$ 2.25 million. Additionally they agreed to toughen their security practices as part of a settlement with regard to potential HIPAA violations. The payment was 22 times larger than the previous largest HIPAA related settlement which was \$ 100,000, paid by Providence Health & Services.

In addition to ARRA HITECH privacy provisions, as of Nov. 1, 2009, the FTC Identity Theft Red Flags Rule will apply to health care entities. Under the "Red Flags Rule," entities must identify and operationally detect patterns that provide a suspicion of identity theft related activities. The health care entity is further obligated to spell out specific actions they will take when identity theft occurs as well as continually updating their program. The FTC implemented this ruling because of an epidemic of well documented identity theft incidents during 2007 and 2008.

The Federal Government is not alone in legislating to improve privacy for patients. State governments are passing legislation requiring health care entities provide a greater level of transparency in regards to privacy breach notification. The states are levying fines and penalties to institutions and individuals involved in privacy breaches. California Senate Bill 541 and Assembly Bill 211 became law Jan. 1, 2009, and enforcement has resulted in fines thus far totaling \$ 437,000 for Kaiser Permanente in well documented cases of privacy lapses at their Bellflower Medical Center. Additional states are following the California lead.

Health care entities that turn a blind-eye to patient privacy rights and the curtailment of privacy breaches now face serious business downsides. These include media exposure and associated public relation damages, patient visibility and associated lawsuit risks, Federal government fines as well non-compliance with HHS Office of Civil Rights, the FTC and state law.

Privacy and Security Plans are the Elephant in the Room

HIPAA legislation was foreshadowing of the current legislative climate that would mandate and enforce compliance of the protection of patient privacy information. Patient privacy was becoming a top priority for government. Amid this culture, many leading health care organizations should have deployed an entity-wide privacy and security plan, established safeguards against inappropriate access to physical records and put in place foundational technologies and processes relating to laptop encryption, tape encryption, authentication, firewalls, anti-virus, secure e-mail, data-in-motion encryption and secure remote access. Health care leaders have long known these are gaping security holes that must be addressed.

Under ARRA HITECH and an invigorated Federal focus on health care privacy, "the minimum necessary" is no longer an option. If your health care entity has not put in place these minimum privacy and security safeguards and you are responsible for privacy, compliance or security, your entity is at risk. However, the risk is not eliminated simply by meeting the above security minimums. Health care entities still have vulnerability in relation to the risks associated with wide-scale access to PHI from dozens, if not hundreds of applications. Wide-scale PHI access through EHRs and applications provide significant vulnerabilities related to privacy breaches from snooping to medical identity theft. When asked, health care executives report they are a little afraid to check-in to their own facilities because they intuitively know that employees, consultants, affiliated physicians, temporary contractors and various other parties can likely access their sensitive medical records.

As health care leaders grapple with the worries of protecting their entities against a breach, and filling the gaping privacy and regulatory risk of broad-scale access to PHI through their dozens, if not hundreds of EHRs and applications, they also recognize that breach detection, Accounting of Disclosure, Breach Notification are all related and can be addressed by an integrated set of technologies and processes. Leveraging these technologies and processes will ensure compliance and eliminate the risks that keep them up at night.

Leading the Patient Privacy & Compliance Charge

It appears that dramatically more health care entities are taking action to protect patient privacy and meet privacy obligations after the passage of ARRA HITECH. Health care's leading institutions are creating a culture of "patient privacy and compliance" by putting in place fundamental technologies that enable them to automate their Accounting of Disclosure responsibilities, detect health care privacy breaches, leverage their training and sanctioning processes.

More specifically, leading institutions are:

- Fulfilling their Accounting of Disclosure responsibilities by automating privacy auditing reporting across all of their health care applications that access PHI, recognizing they must be able to deliver back on 3 years of data from when the patient makes the request
- Stamping out inappropriate access to patient records by automating the proactive detection of privacy breaches related to identity theft, medical identity theft, employee-patient snooping, as well as VIP, friends, family and neighbor snooping
- Establishing a forensically sound repository of all electronic health record audit logs and core systems which access PHI
- Lastly, leading health care institutions are incorporating the results from the above into their existing training and sanctioning processes on an on-going basis. Taken all together, these actions are creating a culture of privacy and compliance which provides strong deterrents for privacy breaches.

Kurt Long is the CEO of FairWarning. He has penned more than 15 articles on privacy and has served as a privacy expert on more than ten industry panels.