

## HIPAA Update – What You Don't Know *Can Hurt You*

By [Marion K. Jenkins, PhD, FHIMSS](#), QSE Technologies



When most people in healthcare hear HIPAA they think, “Been there, done that.” After all, HIPAA was originally passed nearly 15 years ago, and in the years between 1996 and 2003, when HIPAA Privacy compliance was finally made mandatory, countless hours were devoted to seminars and workshops and consulting engagements to make practices HIPAA compliant. So by 2003 most everyone got fairly satiated with – and numb towards – HIPAA compliance.

But the original HIPAA act pertained only to *paper* records. The HIPAA Security Rule, which wasn't put into place until 2005, covers *electronic* records, known as electronic protected health information (EPHI). Most practices just assumed either that they were already compliant, by virtue of all their HIPAA Privacy efforts, or assumed that their IT people understood the HIPAA Security rule and had made their systems compliant. Or they bought a HIPAA Security-compliant software application and felt they were done with that.

This has caused many medical facilities to largely ignore or minimize the importance of HIPAA Security Rule compliance.

But HIPAA *Security* compliance is anything but a foregone conclusion, and all medical facilities would be well-advised to reevaluate their HIPAA Security compliance status, especially in light of recent regulatory and market developments.

The ARRA/HITECH act (American Reinvestment and Recovery Act/Health Information Technology for Economic and Clinical Health), which was signed in February of 2009, was intended to stimulate the wider adoption of information technologies within healthcare. But with increased adoption, concerns were raised anew about the security of electronic patient records. Therefore with ARRA/HITECH, new security rules were introduced that have a large potential impact on all medical entities (known as Covered Entities, or CEs). CEs include not only typical medical practices but also imaging centers; ambulatory surgery centers (ASCs), physician-office surgery suites and specialty hospitals.

Here are the major reasons why all CEs need to redouble their HIPAA Security Rule compliance efforts:

### **Significantly Higher fines:**

The 2005 version of HIPAA Security capped fines at a maximum of \$250,000. Although this was a significant amount, the new fines are even higher – up to \$50,000 for each violation, with a maximum fine of \$1.5 million per year.

### **More onerous breach reporting requirements:**

Under the new 2009 requirements, if a data breach involves 500 electronic patient records, the CE must not only notify all the patients involved, but it must also contact the

Secretary of Health and Human Services, plus notify the local media. So in addition to the increased fine, there is significantly higher risk due to bad public relations exposure.

**Business Associate Agreements (BAA):**

You need to examine your BAA language to reflect the new 2009 Rule updates. The CE may now be legally responsible for actions and negligence of its business associates relative to HIPAA Security breaches.

**Increased scrutiny of physician-owned facilities:**

With the debate over healthcare reform, much attention has been focused on physician-owned facilities such as ambulatory surgery centers. Many in the healthcare establishment would like nothing more than to give ASCs and similar entities a black eye. Therefore ASCs are particularly susceptible to increased scrutiny and unfavorable action due to HIPAA Security violations.

**The new HIPAA rules apply regardless of use of EMR and/or HITECH funds:**

Many people believe that if they do not use or plan to use an EMR, they are not covered by the new rules. Additionally, some people believe that the new rules only apply if their facility is trying to qualify for funds from ARRA/HITECH. This is incorrect. The new rules apply to any EPHI. It does not matter if it is part of an EMR or not, or whether it is part of a qualified EMR system being used to possibly gain reimbursement funds.

**Civil charges, with additional financial penalties, can apply:**

In addition to the significantly higher fines from the Department of Health and Human Services (HHS), the new rules allow states' attorneys general to pursue violators on behalf of victims. Therefore there is even more financial motivation for potential victims – and even higher potential financial risk for CEs – for non-compliance.

**What should Covered Entities do?**

All CEs should review their HIPAA Security Rule compliance and make sure they are still compliant, and if any issues are found, they need to be addressed quickly at the highest level of management within the organization. It is not sufficient to assume that your IT resources – whether internal employees or outside contractors – understand HIPAA Security compliance and are able to protect your facility. You need to periodically review your HIPAA compliance, and rely on independent, outside resources if necessary, who are familiar with the new rules.

**I am using a HIPAA-compliant software application. Isn't that sufficient?**

No. It is entirely possible to implement and use an otherwise HIPAA-compliant software package in a completely non-compliant way. In fact this is far too commonplace in actual practice.

**What does the HIPAA Security Rule actually say?**

The HIPAA Security Rule is very complicated, but at the same time it is rather vague; for example it does not specify the specific technologies that should be used to secure EPHI.

The rule contains 42 specifications, broken down into three primary areas: Administrative, Physical and Technical. Each specification is defined as either “required” or “addressable.” Distilled down to the basics, the HPA Security Rule basically states that a CE must take every reasonable technical and operational action to ensure that it protects against the unauthorized access, theft or destruction of EPHI, both from inside and outside the CE.

### **What is EPHI?**

EPHI deals with electronic patient data – in any form – that is generated, stored or passes through any of your facility’s IT systems. This includes laptops, desktops, servers, data storage systems, USB drives, CD/DVD-ROMs, smart phones, PDAs, voicemail systems and many types of fax machines and scanners. It covers data that is stored within or transmitted outside the CE, including not only the obvious things like patient files, it also includes dictation, emails, file attachments, remote access, and even the reuse and/or disposal of old computers and media.

### **An Inside Job:**

Unauthorized access to EPHI covers the obvious things – outside hackers, identity thieves and the like – but it also covers unauthorized access from within a facility. One of the HIPAA Security Rule requirements is that every CE must be able to track – by specific user – who accesses specific EPHI, including date and time. There have been recent news episodes where employees accessed the records of Britney Spears, Farrah Fawcett and Nadya Suleman, the so-called “octomom.”

### **The most common HIPAA Security risks:**

Based on hundreds of IT assessments in medical facilities around the country, here are the most common HIPAA Security threats we have seen:

1. Un-patched or out of date operating systems.
2. “Weak” or shared user names/passwords, like “nurse” or “front desk” for logins.
3. Lack of formal user security policy.
4. Use of web-based emails (G-mail, Hotmail, etc.). These email systems are not secure and should not be used.
5. Lack of updated, business-class anti-virus, anti-spyware, anti-adware software.
6. Unsecured or poorly-secured wireless.
7. Lack of good data storage and backup system(s).
8. Laptops that move in and out of the facility (especially physicians’ “personal” machines)
9. EPHI stored on local workstations/laptops or on portable media (CDs, USB drives, etc.)
10. Poorly-designed remote access methods, including weak firewalls.

The positive effects of the HIPAA Privacy Rule are debatable. Certainly some of the processes and procedures have benefitted some patients and some providers. However, if you look at the list of most common risks above, and if you examine the

HIPAA Security Rule in detail, you will find that HIPAA Security represents industry best practices. In fact it is a good framework for any business, not just in healthcare.

### **Summary**

HIPAA Security represents a risk to most medical entities. With the passage of ARRA/HITECH in 2009, this risk is significantly increased. New reporting requirements and higher fines apply, even if a CE isn't using an EMR and even if a CE is not attempting to get stimulus funds under ARRA/HITECH. In light of this, all CEs should re-evaluate their HIPAA Security Rule compliance, and not assume that their existing IT resources have this covered satisfactorily. HIPAA Security Rule compliance represents good business technology practice, and has applicability outside of healthcare.

*Marion K. Jenkins, PhD, FHIMSS, is founder and CEO of QSE Technologies, which provides IT consulting and implementation services for medical facilities nationwide. Learn more about QSE Technologies at [www.qsetech.com](http://www.qsetech.com).*