

## **How to ensure security compliance with HIPAA**

*Advice by Marcia J. Wilson / May 1, 2003*

The Health Insurance Portability and Accounting Act (HIPAA) Privacy Rule became effective April 14 [2003], which means it's time to pay attention if you haven't done so already.

HIPAA is a set of federal regulations intended to protect and simplify the exchange of health care data. Compliance deadlines have been stretched out over the next few years. Compliance means doing everything in your power to follow the letter and spirit of the law without going out of business.

The HIPAA Privacy Rule is federal law, and anyone not in compliance can face up to \$250,000 in fines and jail time of up to 10 years. The rule applies to electronic protected health information -- essentially, patients' medical records and other personal health care information. It affects companies that transmit protected health information in electronic form, which includes health plans, health care clearinghouses and health care providers. These organizations are referred to as "covered entities."

Full compliance will require that these entities understand the threats and liabilities to this protected data and that they implement a wide variety of safeguards and security best practices. Where should these health care companies start, if the urgent has driven out the merely important? There are so many drivers in today's world that compliance, however imminent, seems to be very far away.

Let's break it down so it's not so overwhelming. According to the law, the entities must maintain reasonable and appropriate safeguards in three areas: administrative, physical and technical. Let's take a closer look.

### **Administrative**

Start at the top. The administrative portion is 50% of the rule. Advocates of top-down policy suggest that this is the right place to begin. What is the security management process of the organization, and who has responsibility for it? If the organization hasn't already done so, establish a chief privacy officer. The chief privacy officer would be responsible for establishing policy and procedure for employees and others who have access to the health care data.

Security awareness and training is the critical next step. If employees aren't aware of or don't understand the policy, it's of no use. Incident-handling also needs to be factored into the equation. An incident response team should be established in conjunction with the position of privacy officer to develop policy and procedure. This team can be responsible for contingency planning as well, depending on the size of the organization. Contingency planning is needed to provide an alternative plan once a breach has occurred. Document everything, plan on keeping that data for six years plus, and you're almost there.

## Physical safeguards

Physical safeguards include physical access to the facility, workstation accessibility, workstation security, and device and media control. Are you using wireless technology? Have you secured it? Is it possible to join the network from the parking lot? The wireless issue can fall under both physical and technical safeguards. Also, how do you dispose of or move the electronic media, (the tape backups and the disk storage) that contains this confidential data?

## Technical

The technical standards address access, authentication, authorization, auditing, integrity and the transmission of sensitive data. Here are some questions to ask:

- ▷ Who gets access to data?
- ▷ How do you know that those with access are who they say they are?
- ▷ Do they have the appropriate level of authorization?
- ▷ Are you keeping track of who does what and when?
- ▷ Do you have assurance of data integrity?
- ▷ When you transmit data over an electronic communications network, can anyone else get access to it?
- ▷ Are other parties (partners and other health organizations with which you share information) in compliance?

The chief privacy officer would be responsible for establishing clear and consistent standards throughout the organization by understanding which kinds of information are critical, how to maintain the confidentiality of the information and how to support the integrity, reliability and availability of the data. An independent information security audit can provide a baseline from which to work toward compliance. Understanding what is and what isn't working is a step in the right direction. Consider these security best practices:

- ▷ Obtain an annual independent evaluation of information security and practices.
- ▷ Ensure that information security policies are founded on a continuous risk management cycle.
- ▷ Implement controls that assess information security risks.
- ▷ Promote continuing awareness of information security risks.
- ▷ Continually monitor and evaluate information security policy.
- ▷ Control the effectiveness of information security practices.
- ▷ Provide a risk assessment and report on the security needs of the organization's systems.

Before running off and hiring a big consulting firm to implement an automated medical records systems that's supposed to make HIPAA go away, take a step back and breathe deeply. Have an independent risk assessment performed that will allow you to establish a baseline for your company's general security posture, and work from there.

Remember that this rule is about reasonable and appropriate effort to secure confidential health information. As we count down to HIPAA, we can eat the elephant one bite at a time.

### Source of article:

<http://www.computerworld.com/securitytopics/security/story/0,10801,80812,00.html>