Information By Design
Technology for Business Performance

Are You Hip with HIPAA?

With the Obama administration's focus on healthcare, you can bet there will be renewed interest in HIPAA compliance. Failure to comply could generate stiff fines for healthcare providers, and in fact, already has.

HIPAA stands for Health Insurance Portability and Accountability Act. HIPAA was enacted by Congress in 1996. Title II of HIPAA establishes national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. It provides guidelines to help ensure privacy. Health care agencies that don't take HIPAA standards seriously risk compromising their patient's health care record and thus open themselves up to pecuniary risk.

There is no tool or one size fits all approach to HIPAA compliance. HIPAA guidelines were designed to be flexible and general enough to work across the whole industry. There are, however, some specific recommendations that we can make to help you understand what it takes to secure your patient records and maintain peace of mind.

1. **Assign a security officer**. For small offices, this can be a part time role to coordinate the various tasks and projects necessary to achieve HIPAA compliance.
2. **Determine your individual risk**. You must establish a process to reduce risks and vulnerabilities to a reasonable level. This consists of identifying risks and then establishing a process to regularly assess your ability to mitigate those risks.
3. **Document your policies and procedures**. How you collect, store, retrieve, backup and delete patient data should be documented in your company's policies and procedures manual.
4. **Define and implement your information access policies**. Data access management and control should be defined and implemented through system logon that match your policies.
5. **Be prepared to handle incidents**. Security breaches, whether they are system outages, virus alerts, spam or other malware intrusions, can happen at any time. You need to have a plan in place to address these breaches when they occur and to mitigate the risk to patient data.
6. **Plan for the worst**. In you don't have a data recovery, disaster recovery or business continuity plan, start on one today.
7. **Control your m**edia. Laptop computers are notorious sources for data leaks. Once stolen or lost, the data on that laptop can be compromised. Thumb drives can be lost or stolen. Even access to your local server, unlocked and unmonitored, can pose a significant risk.
8. **Train your end users**. A policy manual is only as good as its acceptance and use by your end users. Most companies make this part of new hire orientation and then make the policies available online on a local intranet.

© Information By Design, LLC

9. **Audit IT logs**. Devices on your network have the capability to log events. Firewalls, for instance, can log malicious activity. Unless someone monitors these logs on a regular basis, you may never be aware of hacker interest in your data.
10. **Clean up old data**. This is perhaps the most ignored step of all. Because disk storage is so cheap today, it's much easier to tell yourself to leave old patient data on your shared drive rather than remove and archive it. By sending data to archive, you can move it to removable media and store it off-network in a safe, accessible location.

In its most basic terms, HIPPA requires health care providers to both physically and electronically secure patient information from unauthorized retrieval, to securely store the data, and be able to access the data in the event of disaster. These are actions any reasonably run business takes on a day to day basis. Yet, many healthcare providers will not make this investment in time, process, and people. It's time for a change. Time to get hip to HIPAA!

www.informationweekanalytics.com, HIPAA: Time to Get Serious, February 2009.

The authors, ***Gil Laware*** and ***AJ Walters***, are principal consultants for Information By Design, LLC.

© Information By Design, LLC