DataMotion™ /

Healthcare: How to Disappoint Your HIPAA Auditors and Gain the Respect of Your Board of Directors

(and not necessarily in that order)

With HIPAA audits now randomized, you must be prepared for them every day. And with state regulations requiring compliance-breach reporting, you must become your own auditor.

HIPAA is the Health Insurance Portability and Accountability Act, the 1996 federal regulation that mandated health-data privacy.

This regulation requires compliance by all insurers and health care providers, including physician's offices, hospitals, health plans, employers, public health authorities, life insurers, clearinghouses, billing agencies, information systems vendors, service organizations, and universities.

But that's not all.

The Act's Privacy Rule also regulates medical payment history privacy. Simply put, it requires that all health entities take reasonable steps to ensure the confidentiality of all communications that contain patient or customer information.

And things could get even more serious very quickly. The passage of the HITECH Act creates mandatory reporting requirements of HIPAA violations, even when the data is lost by a third party. This increases the need for subcontractors to implement the same level of security typically found in larger organizations.

The guidelines governing audits have changed. Prior to 2008, an organization was only put through an intense investigation when a routine audit found an egregious problem—and such routine audits were usually scheduled.

But in February 2008, the U.S. Department of Health and Human Services, which oversees HIPAA compliance, contracted with the firm PricewaterhouseCoopers to conduct surprise audits of hospitals.

If you work at a hospital, or communicate with one, you could be targeted for a surprise audit this year. This changes the stakes for everyone's need to be ready.

And if that's not enough to worry you, the states are getting into the picture as well. In New York State, the loss or compromise of 10 or more patient records must now be reported to the New York State Department of Health.

So, ask yourself, "Would my company know if we lost 10 patient records?" If you're in the state of New York, your answer must be "Yes."

HIPAA: Healthcare made difficult.

One of the consequences of HIPAA is that it makes all kinds of medical research more difficult. That's because people are more reluctant to participate as subjects, and it is more difficult to reach the right people to request their participation in research projects.

Another noticeable consequence of HIPAA is that doctors are reporting less communicable diseases to state authorities.

What's worse is that even the public HIPAA was designed to protect doesn't really like it. In a nationwide survey of 2,392 adults quoted in the Oct, 2007 Government Health IT Newsletter, nearly 3 out of 5 Americans agree that privacy of their health information is not well protected by federal and state laws and organizations.

Any health provider who has struggled to help someone who needs information but doesn't have the right

identification on the phone, will tell you it gets in the way more than it helps.

So what's the answer?

The only thing an organization can do is to fulfill the requirements in a way that allows everyone to get their jobs done in an efficient, cost-effective manner.

And satisfies the auditors.

And relieves your board of directors.

And satisfies your customers and patients.

And keeps you from paying penalties or risking prison time.

And the way to do that is to outfit your organization with the technologies it needs to secure information when it travels, as well as when it is used, stored, and communicated both inside and outside your organization.

To avoid auditors, and penalties, you have a lot of planning to do.

The penalties for failure to conform to HIPAA regulations go far beyond the hundreds of thousands of dollars in fines. They include public humiliation, loss of reputation, brand damage, class-action lawsuits, and yes, even prison.

But there are practical ways to avoid these penalties. The goal is to keep private information private, to keep prying eyes out, and to be able to prove both to auditors.

Here are some methods:

1. Take secure measures, in case people make mistakes.

One of the most common causes of any kind of security breach is human error. Whether conscious, accidental, or simply due to laziness, human error can result in Personally Identifiable Information (PII) or Personal Health Information (PHI) being sent over the internet as unencoded text unless filters are put in place to detect these messages and encode or reroute them safely.

At the same time, you can't afford to stop communications. Likewise, you can't afford to handle hundreds of false positive alerts – alarms signaling that a breach has occurred when one hasn't. No one has time for that.

Many companies are hesitant to apply filters to their most important communications – email and attachments. For example, if a filter were to keep every piece of mail from leaving your company that included the word "diabetes" and a person's name, you couldn't send out an email message with an attachment that says, "Watch for these symptoms, they may indicate you have diabetes."

On the other hand, you must be sure that the attachments that include a patient's name, id number, and blood-test results can never be intercepted accidentally, or be sent outside your company unencrypted.

To accomplish this, you need to:

- Install smart filters that analyze both the email and its attachments,

- Correlate fields in both documents and attempt to match them to known patient databases,
- And quarantine or redirect those messages.

2. Make sure the boundaries between systems are secure.

Communication security breaches commonly occur where data is transferred between two or more systems.

It can happen any time and any place where data is transferred between:

- People inside your company's firewall
- People inside and outside your company's firewall
- Your people and your partners
- Your people and your customers (or patients)
- Two different systems

Whenever information passes between systems and people, the data needs to be secured at all times, even when in transit. You must also ensure the data that is sent to people outside your firewall is always sent in encrypted format, so that no one but its intended recipients can read it.

For example, should you need to transmit patient data from a doctor's office to a central database, if it is encrypted, it could be sent automatically as an email attachment.

3. Make sure your INTERNAL communications are secure.

Your people who work from home provide a specific example of HIPAA boundary issues. It is critical that any data that they transfer to their home computers from work is sent securely, one copy of a database file, one spreadsheet, one PDF attachment, or one presentation that someone works on over the weekend.

Your business information must pass across the Internet securely, even though it will remain inside your company and your firewall. It must never be compromised – or vulnerable.

But one mistake is all it takes.

How do you ensure that this never happens? Despite your most well intended policies, there is always a chance that someone somewhere will let your guard down.

Today you hope it never happens, or if it does, that it won't cause a problem.

But hoping isn't acting. You must act.

You must put a comprehensive filter in place, so that you can implement and enforce business rules to prevent these occurrences.

You could either encrypt the file and send it, and email a warning to the sender, or you could quarantine the suspicious file and report the sender to his or her manager, the legal department, or whomever else you chose.

4. Make sure your PARTNER communications are secure.

Your people, when working with business partners, bring up another case of boundary issues.

It's likely that they must regularly transfer information back and forth with external partners. In some cases this can contain very sensitive information.

Your partners may use different email systems. They often need to send personally identifiable information (PII) and or personal health information (PHI) about clients or patients via email or attachments.

Sometimes, attachments can be extremely large. For example, a single mammogram image can reach 500 megabytes. So not only would you need to exchange this file securely, you would need to send it in a way that does not overburden – or stop – your email system.

Healthcare-related institutions must use solutions that make it possible to communicate with anyone, anytime, anywhere, no matter what email system the other party uses.

Likewise, you must demand the ability to securely transfer extremely large files with all these same people.

5. Make sure your communications with telecommuters are secure.

People who telecommute create another group of boundary issues.

Medical professionals, such as radiologists, who choose to work from home, are moving in this direction.

When people must transfer large, important, time-sensitive files such x-rays or mammograms as email attachments through your company's email system, they have the potential to bring your email system to a standstill.

So you must find the time, the budget, and the resources to set up file-transfer sites for these large files. And you must make absolutely sure that they offer unbreakable security.

With a sophisticated system in place, you could manage and track the secure transfer of confidential, large files so you'd know they were delivered to, and opened by your intended recipient.

6. Make absolutely sure your communications with CUSTOMERS – or patients – are absolutely secure.

When communicating with customers (or patients), your people most likely have no knowledge of the recipient's email system.

Which means that although your company might have created a secure email portal, extensive research shows that customers do not want to use a browser to visit a portal to communicate with – or get information from – you.

They want to use email. And they want you to send important information quickly, via email. And if you do, they want it, of course, to be secure.

Not just because it's the law. Because it's common sense that people don't want anyone to have access to their private medical information, any more than anyone should have access to their private banking information.

Healthcare-related institutions can now adopt solutions that allow them to communicate securely with anyone – regardless of whether the other party has the same email system or not – without the trouble of using a portal. All they need to do is establish a password.

The customer or patient can receive their email replies securely in their inbox without visiting a portal.

7. Make sure when your customers – or patients – communicate with you, everything they do is secure.

Your customers and patients must often submit forms, ask questions of specific people and departments, or submit follow up information about an ongoing illness or other matter.

For a long time, these needs were served by paper-based processes, but can now be handled through secure electronic forms on your web site.

But the question is how does this data reach the right department or employee to process it? And can this data be integrated into existing knowledge worker software such as the company's customer relationship management system to track its status? If the request contains sensitive information, is it received from the customer in a secure manner, or did the company's method of collecting data cause a privacy violation? And if any follow up is needed with the customer, can this be sent securely?

With a messaging system in place that provides secure inbound and outbound service, uses email and ad hoc forms for message composition, and provides web service and XML workflow integration, you can streamline your operations and cost effectively serve customers.

Such a system eliminates the need to retype data from paper-based forms – an error prone, time-consuming and costly way of doing business.

8. Make sure your customer workflow is automated, so there are fewer mistakes.

When you enter information into your system, you should only enter patient information once. Multiple entries of the same information are big bright red flags for auditors.

To avoid this, you need to make very sure that any time information is entered securely, it is routed to its destinations in your CRM system or case handling systems without the need for humans to unencrypt, read, retype, fax, or otherwise invite errors. Or auditors.

9. Make it easy to transfer files securely – even very large ones.

FTP, or file transfer protocol, is the standard way to transfer files across the Internet. However, it requires big investments of time and effort to make it work, and even when it does work, it transmits user login credentials and the contents of files in an unencrypted manner.

So while your people face a constantly changing list of partners with whom they must exchange sensitive

files, how can you offer them a secure, easy, reliable method of doing so?

You need a secure messaging system that automatically routes large files, alerts the recipient that they are available, and that tells you when they've been opened and by whom.

10. Make sure that you can demonstrate that your system is compliant and auditable.

After an email message is sent, how do you know what happened to it? Did its intended recipient open it? Were its attachments opened? Is there proof that the message was received and was read?

Should a question arise about who viewed a message or its attachments, can you prove who read them to an auditor?

It's increasingly obvious that a secure messaging system must be auditable. To make this possible, messages and their attachments, their metadata and the fingerprinting data must be both viewable and traceable.

The fingerprint data must record – permanently – the IP addresses of the recipient's computers, and the system's time must be synchronized with an atomic clock so that message times are never a point of dispute.

Such a system would allow your administrators – and, if necessary, auditors – to easily review and sort through volumes of message information, and quickly retrieve a particular message, as well as all the tracking and fingerprint information associated with it.

ABOUT DATAMOTION

DataMotion is the first Intelligent Information Transport service that automates key business processes, so you can easily and quickly exchange information with your partners, customers, and colleagues.

The DataMotion solution automates key business processes, such as automated billing, credit application processing, or customer outreach, to help you send critical information over the Internet.

CONTACT US WITH QUESTIONS:
Toll-Free: 1.800.672.7233 Tel: 1.973.455.1245 Fax: 1.973.455.0750
Email: info@datamotion.com www.datamotion.com
DataMotion, Inc. 35 Airport Road Morristown New Jersey 07960