DataMotion /

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

(and not necessarily in that order)

The Department of Health and Human Services (HHS) Office of Civil Rights indicates that they now have the regulatory teeth needed to perform HIPAA audits, with increased activity starting with the federal fiscal year on October 1, 2013. As a result, you must be prepared to be audited. And, with 46 states now requiring compliance-breach reporting, you must also become your own auditor.

So How Did We Get Here?

About four years after the HITECH Act became law, the Department of Health and Human Services (HHS) published Omnibus Final Rule 45 CFR Parts 160 and 164 to the Federal Register. It specifies that starting September 23, 2013, a wide range of organizations must comply with updated provisions of HITECH including modifications to HIPAA privacy, security, enforcement, and breach notification rules, along with strengthened privacy protections for genetic information.

Compliance is now required by all covered entities and their business associates that touch or handle Protected Health Information (PHI). Organizations such as physician's offices, hospitals, health plans, self insured employers, public health authorities, life insurers, clearinghouses, billing agencies, information systems vendors, service organizations, and universities could all be considered covered entities and/or business associates or their subcontractors.

All affected entities are required to take reasonable steps to ensure the confidentiality of all communications that contain patient or customer information. In addition, mandatory reporting is required for 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, HHS contracted with PricewaterhouseCoopers to conduct surprise audits of hospitals. This round of audits has been completed and reported on. Starting in the 2014 federal fiscal year, HHS will begin a new round of audits – and these may include business associates and their subcontractors, as well as covered entities.

If your organization is a covered entity, or you communicate with one, you could be targeted for an audit this year. This changes the stakes for everyone's need to be ready.

And if that's not enough to get your attention, the states are part of this picture as well. HIPAA allows more restrictive state laws to preempt HIPAA. For example, Texas Health and Safety Code, Chapter 181 is considered more restrictive than HIPAA.

So, to the question "Would my organization know if we lost any patient records?" Your answer should be "Yes."

HIPAA: Patient Privacy Taken Very Seriously

Organizations must fulfill these 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.

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

And satisfies your customers and patients.

And keeps you from paying penalties and/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 to secure your moving data:

1. Do an assessment.

If you do nothing else, at least do an assesment of where your PHI resides, and where it flows to and from. Who touches it? Who processes it? And how does it get there and back? Knowing where the data is that you need to protect, and how it travels, is the first step.

2. Add layers of security, 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 Protected Health Information (PHI) being sent over the Internet as unencrypted text unless content 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 electronic 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 providers are hesitant to apply content filters to their most important communications – email and attachments. For example, if a content filter were to keep every piece of email 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
- Encrypt those messages before they're sent over the public Internet

3. 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 organization's firewall
- People inside and outside your organization's firewall
- Your employees and your business associates (and their subcontractors)
- 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.

4. Make sure your internal communications are secure.

Your employees 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 – whether 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. 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. Equip any employee with access to PHI with email encryption.

5. Make sure your Business Associate and subcontractor communications are secure.

Your people, when working with business associates, and they with their subcontractors, bring up another case of boundary issues.

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

Your associates and subcontractors may use different email systems than you. Often, PII and/or PHI about clients or patients needs to be sent via email. Be sure to secure these emails with encryption that works with many different systems and devices, including mobile devices i.e. smartphones and tablets. Healthcare-related institutions must use solutions that make it possible to communicate with anyone, anytime, anywhere, no matter what email system or device the other party uses.

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

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

6. Make sure your communications with telecommuters are secure.

People who telecommute create another group of boundary issues.

For example, medical professionals, such as radiologists, who often choose to work from home, are moving in this direction.

When they 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. Sometimes, attachments can be extremely large. For example, a single mammogram image can reach 500 megabytes (MB). 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.

So you either must find the time, the budget, and the resources to set up file-transfer sites for these large files or you can use encrypted email with a secure large file attachment capability. Either way,you must make absolutely sure that they comply with encryption guidelines.

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

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

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

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 to track its status? If the request contains sensitive information, is it received from the patient in a secure manner, or did the method of collecting data cause a privacy violation? And if any follow up is needed with the patient, can this be sent securely?

With a messaging system in place that provides secure inbound and outbound service, uses email encryption and secure electronic forms, and provides workflow integration, you can streamline your operations and cost effectively serve patients.

8. 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 employees face a constantly changing list of business associates 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.

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

9. Make sure 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 trackable and 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 enables organizations to dramatically reduce the cost and complexity of delivering electronic information to employees, customers, and partners in a secure and compliant way. The company's core DataMotion Platform solves a broad range of business issues by providing a secure data delivery hub. Easy-to-use solutions are provided for secure email, file transfer, forms processing, and customer contact that leverage the DataMotion Platform for unified data delivery. Millions of users worldwide rely on DataMotion to transparently improve business processes and reduce costs, while mitigating security and compliance risk. DataMotion is privately held and based in Morristown, N.J. For the latest news and updates on DataMotion, visit www.datamotion.com, like DataMotion on Facebook®, or follow us on Twitter® @DataMotion.

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