Capture Billing
Medical Billing Services

Capture Billing & Consulting, Inc.
25055 Riding Plaza, Suite 160
South Riding, VA 20152
(703) 327-1800

HIPAA Privacy and Security Changes in the HITECH Act

HIPAA and HITECH Act: What You Need to Know

I was talking to Jonathan Krasner from Business Engineering, Inc (BEI) this past week about HIPAA and the need to make sure data that we are doing everything possible to safeguard our clients' information, especially through data encryption. The following is an article from BEI that Jonathan sent me. I would like to pass it along to all of you because it has a lot of great information.

HITECH Act: Suggested IT Policies & Procedures

Congress passed and President Barack Obama signed the American Recovery & Reinvestment Act (ARRA) in February, 2009. The healthcare IT component of the ARRA is commonly referred to as the HITECH (Health Information Technology for Economic and Clinical Health) Act. The HITECH Act covers a broad range of healthcare IT initiatives including providing over $20 billion in funding towards implementation of healthcare IT. The HITECH Act also includes "Subtitle D" which focuses on privacy and modifies and broadens portions of the HIPAA Privacy and Security laws and regulations.

What You Need to Do

All of our privacy rules and laws (not just in the medical field) need to be updated to reflect the increasingly connected electronic world we live in. The electronic security measures mandated in HITECH are not that much different than what would be recommended for any business that needs to protect proprietary or confidential information.

Technologies that render Electronic Protected Health Information (EPHI) unusable and unreadable to unauthorized individuals are necessary for EPHI to be considered secured. Secured EPHI is not subject to fines under the new HIPAA regulations.

All of the recommendations below can be implemented with no or low additional cost, and with standard IT systems and services.

Encrypt your data:

The new HIPAA regulations frown on unsecured EPHI. EPHI can be unsecured when it is considered "data at rest" (i.e. stored on a hard drive) or "data in motion" (i.e. data moving from one device to another). To solve the "data at rest" issue, all workstations, laptops, servers, flash drives, or any other device that stores data, should utilize data encryption technology.

It is easier to encrypt everything (e.g. entire hard drive) as opposed to encrypting selectively (e.g. just certain files/folders). There is no real harm in encrypting data that is not EPHI.

Encryption is a capability built into most new operating systems (Windows7, Windows Server 2008), so turning on encryption is just a matter of reconfiguring some settings. Devices using older operating systems (e.g. Windows XP, Windows Server 2003, etc.) can be encrypted with any of several off-the-shelf software products.

In the event that an encrypted device is compromised (i.e. a laptop is lost), the data will be inaccessible, and therefore no breech of any HIPAA regulations would have occurred.
The National Institute of Standards (NIST) provides guidance on storage encryption through their Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices.*

Encrypt your network transmissions:

Any time you transmit EPHI between locations (examples: from your PM to a clearinghouse, or from a workstation in an office to a server in another office or datacenter), the transmission should be encrypted. Several technologies are available today and they are commonly used to transmit other secure information such as banking transactions and credit card authorizations over the Internet.

The most common technologies used are Secure Sockets Layer (SSL), IPSecurity (IPSec) and Transport Layer Security (TLS). Most people are familiar with SSL since any website session that is accessed with the prefix "https://" is being managed by a security protocol, which is typically SSL, and the transmission is encrypted to and from the Web server. To implement HTTPS you have to purchase a digital certificate from a trusted authority (such as Verisign) and install it on your secure server(s).

Your IT vendor should be able to configure any of these secure connections that you may require. NIST also provides guidance in three documents:

1. Special Publication 800-113, *Guide to SSL VPNs*
2. Special Publication 800-77, *Guide to IPsec VPNs*
3. Special Publication 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS)*

Utilize encryption on wireless access points:

Transmission on a private local area network within the organizational confines of the covered entity (i.e. which does not traverse the public Internet) and that occurs over standard cabling is generally considered protected, and these links do not have to be encrypted.

However, many medical offices use laptops and tablets that communicate through wireless access points (WAPS). Make sure that all your WAPS use encryption, and that a security key is required to access your network. Do not leave your network open – that will allow anyone to log on and potentially access or intercept your data.

Encrypt your copiers:

It may come as a surprise to some people, but digital copiers have hard drives (just like the ones used on PCs) built-in. If you dispose of a copier, by returning it to a leasing company or selling it, the data on the hard drive (i.e. all the copies that were made on the machine) may be unencrypted and therefore, unprotected. Make sure to contact your copier vendor and ask how you can get the hard drive encrypted. This is a feature that is available for free on newer machines from major manufacturers.

Use secure email or patient portals:

Many providers use email to discuss patient cases between themselves or to converse with patients. Email transmissions are generally unencrypted, especially when dealing with a third party who is not a member of your organization. Secure email is an available alternative, as it encrypts all the information in each message.

Using secure email is not as straightforward as regular email. It may require additional action on the part of the sender or receiver. An alternative to secure email is the use of a patient portal. When using a patient portal, standard email is used between parties to communicate that a message is available for viewing on the portal. The receiving party logs into the portal to receive (and possibly reply) to the message.

Since the EPHI is totally contained within the portal website, and since that information is encrypted, the problem of securing the email is eliminated.

Ensure terminals used for teleworking/remote access are secure:

Many covered entities now allow their employees and contractors to conduct work from locations other than the organization's facilities. This is commonly referred to as teleworking. Most teleworkers use remote access, which is the ability of an organization's users to access its nonpublic computing resources from locations other than the organization's facilities. Organizations have many options for providing teleworkers remote access, including virtual private networks, remote system control, and individual application access (e.g., Web-based email). In addition, teleworkers use various devices, such as desktop and laptop computers, cell

phones, and personal digital assistants (PDAs), to read and send email, access Web sites, review and edit documents, and perform many other tasks.

Teleworkers should ensure that all the devices on their wired and wireless home networks are properly secured and protected, as well as the home networks themselves. This includes properly configuring the account control of the PC, utilizing business-class antivirus/antimalware software and using a broadband router or separate firewall device or software. NIST provides guidance for this in Special Publication 800-114, *User's Guide to Securing External Devices for Telework and Remote Access.*

Check your firewalls:

Any local network that is connected to the Internet should use a device called a firewall to provide external access to the network only to authorized users and processes. Conversely, it should also be configured to guard against and reject unauthorized incoming external traffic (i.e. hackers).

It is best practice to make sure that your firewall is properly configured to allow access and transmission for applications and users that you have approved. Improperly configured firewalls will have open ports that could possibly allow unauthorized access to your network.

Develop and implement a backup/disaster recovery plan:

Although not new to HIPAA under HITECH, the HIPAA security rule does require all EPHI to be subject to a backup/disaster recovery plan.

Think of all the EPHI that was lost when Katrina struck; what would be the effect on your practice if a disaster occurred? How would you recover? In the past, tape backup was often used. However, newer technologies and techniques are now available that are more cost effective and provide better outcomes.

At first glance, all of this would appear to be a tall order to implement for any private practice. In reality, these types of security and privacy measures are commonly implemented for small businesses. Consult your IT support vendor on how to proceed. Also, remember that these

measures do not insure HIPAA compliance for your practice; rather, they are a component of your overall HIPAA plan.

About the Author

Manny Oliverez

Manny Oliverez, CPC, is a 20-year healthcare veteran and the CEO and co-founder of Capture Billing, a medical billing services company located outside of Washington, D.C. He teaches the nation's physicians, administrators, and medical practices how to maximize billing and revenue cycle management processes. Manny also frequently posts articles and videos on his award-winning healthcare blog. For more information on Manny and his company, please visit his website, or call (703)327-1800. And if you're on LinkedIn, please look for him there too. **READ MORE**

Follow Us on Social Media

https://www.facebook.com/CaptureBilling

https://plus.google.com/+CaptureBilling/

https://www.twitter.com/Capture_Billing

https://www.linkedin.com/company/Capture-Billing-&-Consulting-Inc.

Capture Billing & Consulting, Inc.

Capture Billing and Consulting, Inc. is one of the top leaders in the medical billing industry. We help busy medical practices drastically reduce patient and insurance accounts receivable, and increase physician reimbursement. Capture Billing's services provides one of the most cost-effective and proficient billing solutions available to healthcare professionals. Eliminating the need for an on-site medical billing staff can allow physicians to focus on their primary passion of providing quality healthcare to their patients. Physicians can leave the stress of doing their own medical billing to us.

We help you collect more money, faster and easier.

Improve your bottom line and peace of mind with our medical billing services.