SEMEL CONSULTING HIPAA Brief www.semelconsulting.com

Don’t Use Webmail or Text Messages for Patient Info

Definition:

Webmail includes the free mail services available on the Internet, like Gmail, Yahoo! Mail, Hotmail, etc. plus free e-mail accounts you may receive with an Internet service from Verizon, Time-Warner, Cox Cable, Comcast, Century-Link, and others. Text messages include the services from cell carriers like Verizon, AT&T, T-Mobile, Sprint, and others.

These services are free and so easy. Why can’t we use them?

Free webmail services are not secure methods of communication. While they may be fine for personal messages, they do not include the security required to communicate protected information, including medical records and lab and test results. Even e-mail messages you send to someone else in your office goes outside to the free webmail service and then back. Text messages are never deleted by the cell phone carriers. The recent scandals involving the media prove that text messages can be hacked. The companies that offer these services typically will not sign Business Associate Agreements, required for any organization that stores patient information, including any messages or attachments containing Protected Health Information (PHI.)

What happens if we use webmail or text messages to communicate patient information?

In 2012 a small medical practice was using webmail to communicate patient information. They were also using an online calendar to schedule patient appointments. The practice was fined $ 100,000 and had to pay for notification costs for patients whose data was breached. It also had to implement secure communications and undergo a Corrective Action Plan to address their underlying lack of HIPAA compliance.

So what should we do?

You have several choices. First you should immediately stop sending patient information by webmail or text messages.

1. You can use **faxing** or other methods to communicate patient data. You should not use a system that converts faxes to e-mail messages sent through a webmail account.
2. It is less expensive and easier now than ever to implement **a Cloud-based secure e-mail system** for communicating within your practice. Communicating patient information to anyone outside of your practice should be done using e-mail encryption. Cloud-based solutions like Microsoft Office 365 provide secure e-mail, including shared contacts and calendars, for a low monthly fee per user. An added benefit is you don’t have to purchase servers or Microsoft Office licenses. Best of all, Microsoft will sign a Business Associate Agreement.
3. If you use an **Electronic Health Records** (EHR) system it probably includes a **portal** through which you can securely communicate with patients.
4. You can subscribe to an **e-mail encryption** service that secures sensitive data. Instead of receiving an e-mail containing protected information, your recipient receives an e-mail inviting them to log into a secure site to retrieve the protected information. All they get is a message to log-in; no protected information is ever sent.
5. Text messages should be replaced by voice calls as long as any voice message you leave is not converted to an e-mail or text message through an unsecure service.

Where can I get more information?

HIPAA Compliant E-mail: Myths & Facts

Healthcare Texting in a HIPAA-Compliant Environment

Email is Not HIPAA Secure

SEMEL CONSULTING
www.semelconsulting.com

http://www.emrandhipaa.com/emr-and-hipaa/2010/12/23/email-is-not-hipaa-secure/

Email is Not HIPAA Secure

Posted on December 23, 2010 I Written By **John Lynn**

John Lynn is the Founder of the HealthcareScene.com blog network which currently consists of 10 blogs containing over 8000 articles with John having written over 4000 of the articles himself. These EMR and Healthcare IT related articles have been viewed over 16 million times. John also manages Healthcare IT Central and Healthcare IT Today, the leading career Health IT job board and blog. John is co-founder of InfluentialNetworks.com and Physia.com. John is highly involved in social media, and in addition to his blogs can also be found on Twitter: @techguy and @ehrandhit and LinkedIn.

An interesting discussion happened in the comments about HIPAA secure fax services in regards to the security of email. Being a tech person who formerly managed a few different corporate email systems, sometimes I forget that many people don’t understand some of the details about the security (or lack of security) that’s provided by email.

The short story is: **Email is NOT HIPAA Secure (at least in 99% of cases)**

There is a way to encrypt email sent between 2 email systems, but so far a standard and mechanism for encryption between all the vast number of email providers has not been established. I won’t go into the details of why this is the case (cost of encryption, standards for encryption, etc), but suffice it to say that almost none of the email systems send encrypted email that would satisfy the HIPAA requirements.

In fact, most times when an EMR, PHR or other patient portal wants to send a secure email/message to someone they send an email which contains a link to an encrypted website that has a unique login. The reason they do this is because there’s no recognized and adopted standard for encryption of email. However, presenting Protected Health Information (PHI) through an encrypted webpage where someone has a unique login is HIPAA compliant and doesn’t require the receiving email system to understand the encryption. It’s a pain, but it’s the reality of privacy of health information right now.

One of the major reasons that many people think that email is secured is that a number of email providers (Gmail being the most famous for this) turned on encryption for all of their users. The misunderstanding is that this encryption is just for users logging in to check, read and send their email. It does not encrypt the email as it it sent from Gmail to the destination email system. Aleks, from Sfax described it similar to a postcard. It’s open where anyone listening can see what’s in the email with no traces left behind.

The only security email partially offers in this manner is the volume of emails that are sent. There’s such a huge volume of useless emails that there’s some security by obscurity benefits. Although, that security doesn’t meet well with the HIPAA requirements. Plus, remember that one thing that computers are great at doing is crunching large amounts of data.

One minor exception that I might make is that if you’re sending email in an internal email system, then it’s possible to set up email encryption. This is possible because you control the email system for the sender and the receiver and so there are ways to do this. However, I know very few people that have actually set this arrangement up. Probably because if they are on your internal email system they usually have access to your EMR and all the PHI can remain in the EMR instead of your email system.

Now many have said that you shouldn’t use the free email providers like Gmail. After reading this it should be clear. You shouldn’t use ANY email provider for sending PHI. So, whether you use Gmail or some other free email provider it shouldn’t matter since I’m sure you won’t be sending any PHI through email any more.

http://www.emrandhipaa.com/emr-and-hipaa/2012/04/17/texting-is-not-hipaa-secure/

Texting is Not HIPAA Secure

Posted on April 17, 2012 | Written By **John Lynn**

John Lynn is the Founder of the HealthcareScene.com blog network which currently consists of 10 blogs containing over 8000 articles with John having written over 4000 of the articles himself. These EMR and Healthcare IT related articles have been viewed over 16 million times. John also manages Healthcare IT Central and Healthcare IT Today, the leading career Health IT job board and blog. John is co-founder of InfluentialNetworks.com and Physia.com. John is highly involved in social media, and in addition to his blogs can also be found on Twitter: @techguy and @ehrandhit and LinkedIn.

I previously posted the somewhat controversial post: Email is Not HIPAA Secure. It was an extremely important post and included 54 incredible comments discussing email security and email in how it relates to HIPAA. Today I want to discuss the security issues related to text (SMS) messages.

The short story is: **Texting (SMS) is NOT HIPAA Secure**

I recently did a focus group to discuss physician communication. At one point I asked how many of them use text messages to communicate with other doctors. All of them acknowledged that they used it and that they were using it more and more. I then asked how many sent PHI (protected health information) in the text messages that they sent. While the response wasn't as strong likely because they knew it was a loaded question, they all acknowledged that PHI was sent by text message all of the time.

One doctor even commented, "They're not going to put us all in jail."

There is some validity to this comment. They're not going to go around like an old school lynch mob putting physicians in jail because they sent some patient information in a text message. Although, that doesn't mean that they couldn't go around handing out hefty fines for HIPAA violations.

Let me be clear that there are secure text message platforms out there. I've actually been thinking about this quite a bit lately since I've been advising a local Vegas Tech iPhone app called docBeat that offers this secure text message functionality for free. In fact, there are quite a few companies that are trying to provide this functionality. Although, I like docBeat because it offers a whole suite of Physician Communication Tools and not just secure text messaging. I think there's value in a doctor only to have to go to one place for all their communication needs. In a future post, I'll do a full write up on what docBeat's offering physicians.

At some point, I think doctors are going to turn the corner and realize that the standard SMS text messaging service that every cell phone has these days is not the right way to communicate. Besides the fact that standard text messaging isn't secured, it's also stored forever on the server of your cell phone service provider. Most doctors likely haven't thought that everything they've sent over text could be brought back to haunt them forever.

Other problems with standard text messaging is that you don't really know what happens with the text message once its sent. Did the text message actually send? Did the person you sent the text message actually receive it? If they received the text message have they read it?

The great thing is that we all finally have realized the value of simple communication with a text message. Now we just need to move to these new secure text messaging platforms that solve the security, reliability and tracking issues with standard text messaging.

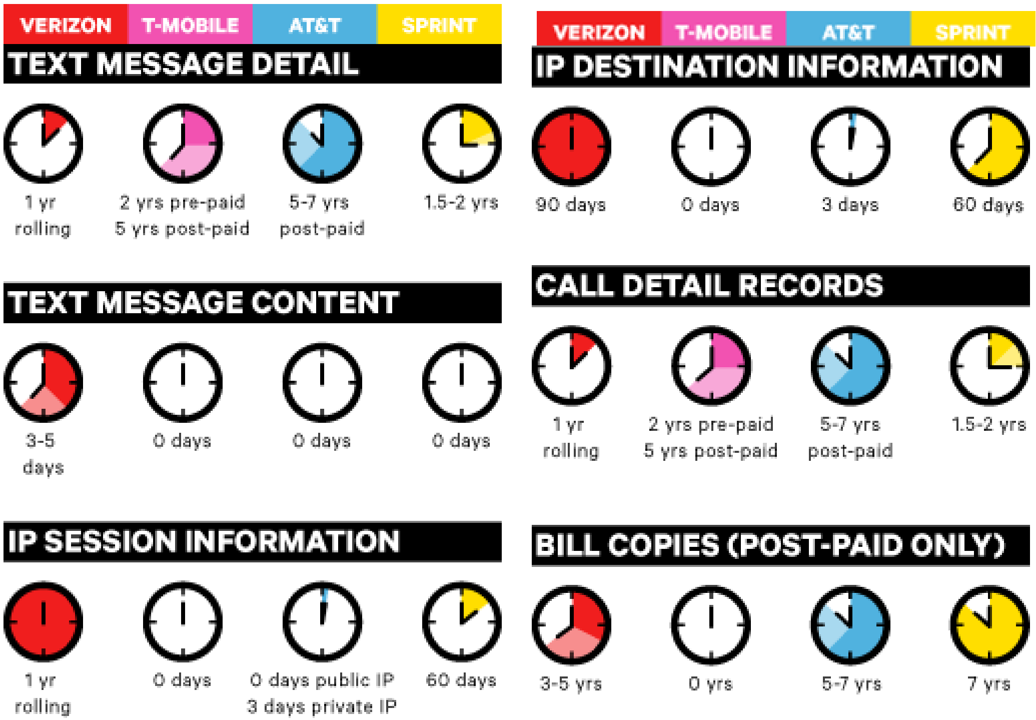
http://www.emrandhipaa.com/emr-and-hipaa/2012/06/27/telcoms-store-sms-text-message-details-not-hipaa-compliant/?trendmd-shared=0

Telcoms Store SMS Text Message Details – Not HIPAA Compliant

Posted on June 27, 2012 I Written By **John Lynn**

As an extension to my previous post called “Texting is Not HIPAA Secure” I wanted to point out some data that Wired posted about Telcom’s SMS message retention policies.

The information was found in a Department of Justice document and I believe is a good illustration for why PHI should not be sent through traditional SMS text messaging. Here’s the chart that wired created showing the major Telcom providers record retention policies:



The top 2 sections are the most important when it comes to secure text messaging. Last I checked, the telcom servers weren’t HIPAA secure. Not to mention, I can’t say I’ve seen a Telcom provider sign a business associate agreement with a healthcare provider. Neither of things are likely to ever happen.

The challenge is that text message is so valuable in healthcare. It’s such a simple and flexible way to communicate between doctors, nurses, staff, HIM, etc etc etc. This is why I predict over the next year we’re going to see a huge uptick in adoption of secure text messaging by third parties. The technology is there. We just need wider spread adoption of it in healthcare.