FEATURES

The Rise of Mobile Healthcare

Providers look for ways to leverage technology to allow better efficiency

By Richard Stokes

Posted on: December 23, 2013

View Comments (0) Print Article Email Article Share …

What we're seeing in Healthcare in the rise of mobility is similar to what the banking industry went through a decade ago. Today in banking, most people don't give it a second thought to: access their account online, deposit a check using a smartphone app or communicate with their bank without ever having to go in to a branch or pick up a telephone.

Healthcare is headed in the same direction. Today, patients want to communicate with their providers and manage their health in ways other than having to go to the doctors' offices and see their provider. They are also hungry for knowledge and are looking for answers and information about healthcare online.

Similarly, providers are moving toward mobile platforms. They are looking for ways to leverage technology that will allow them to do their jobs more efficiently and communicate in different ways with their patient population. Whether it's using a tablet or an iPad at the point of care or getting an electronic notification that a patient took their medication, the landscape of modern healthcare is changing.

With this evolution towards mobile healthcare comes a significant IT security challenge because of HIPAA regulations and the overall burden of protecting patients' personal health information (PHI).

So what can a practice do to reduce the risk of exposure and take appropriate steps to protect themselves and the data? Here are a few areas that need to be considered:

1. Have a Password Policy and Use It
Make it difficult to crack ('password' or '123456' are not good passwords). Passwords are a pain to remember and can be frustrating when you forget them or accidentally mis-key them. But the benefits of a strong password far outweigh these minor inconveniences should a laptop ever get lost or stolen. Smartphones are also making some advances in this area - the iPhone 5S, for example, now has fingerprint recognition software making them harder to unlock by someone other than the owner.

2. Install and Enable Encryption Software
Encryption software on a mobile device essentially scrambles the data to an unreadable format and can only be unencrypted if you have the key or password to unscramble it. It's an extra step but does add another layer of protection.

And, as long as the proper procedures are followed according to the HIPAA security rule and the Personal Health Information is determined to be rendered unusable, unreadable, or indecipherable then the covered entity is not required to notify the Office of Civil Rights (OCR) of a data breach should a mobile device become lost or stolen.

3. Remote Wipe Capabilities
Have a system in place that, should a device be compromised, can either have the data remotely deleted or completely wiped and rendered useless in its current state. Of all the IT headaches associated with mobile healthcare security this is arguably the most difficult to nail down and the hardest to manage. Ask any IT person in a Hospital system and they'll tell you that Mobile Device Management (MDM) is a moving target and keeps them up at night.

MDM policies can also open a practice up to additional risk. If a device is wiped and the end user had personal information on it then they could pursue litigation against the practice on the grounds of 'wrongful dispossession of a person's personal property'. At a recent healthcare summit I heard about a case where a Hospital system that had a documented and well-communicated MDM policy in place. They adhered to their policy and wiped an employee-owned device that was lost. The owner of the device sued the Hospital because the phone had the only picture of her mother before she had passed. Despite the policy, the courts sided with the employee/phone owner and not the Hospital.

Despite this unfortunate example, having remote wipe safeguards and policies in place is still an important and appropriate step in protecting PHI.

4. Use Up-to-Date and Business-Class Anti-Virus and Malware Protection Software
Internet threats change daily and keeping up with what the bad guys are doing has become an entire industry in itself. There's also a reason why some Anti-Virus software platforms are free! Make sure you stick with a name brand player (McAfee, TrendMicro, Kaspersky, and Symantec to name a few) and keep your subscription current and the software up-to-date at all times.

5. Keep Your Software Up-to-Date
Software developers are constantly updating the code in their programs to make it better and to fix security holes. Microsoft is probably the best known for releasing updates to their software but so do other well-known and widely used application vendors such as Adobe and Java.

Running software on your mobile device that is not updated exposes the practice and increases the risk of that device being compromised.

6. Disable File Sharing Capabilities
Microsoft has some built in file and print sharing capabilities that allow other computers on a network to access resources on your computer. If these are enabled then you can be exposed to allowing others to access your laptop without your knowledge. This can be a problem when you are connected to an unsecured public Wi-Fi network.

Depending on the Operating System you are running the way to disable these features can be different so either get with your IT person or do some research to find out how to disable these options.

7. Connecting When on a Public Wi-Fi
Always use a proper VPN to connect back to your office/server when accessing the Internet over an unsecured public Wi-Fi. This will ensure that if you do transmit PHI it is encrypted even though the public Wi-Fi is not.

Taking the steps as indicated above will go a long way in helping protect you practice but you should also have the right policies, procedures, training and ongoing communication in place to build awareness around the importance of protecting PHI in the mobile world.

Richard Stokes is director of sales of Network 1 Consulting.

POST A COMMENT

Email: *

Email, first name, comment and security code are required fields; all other fields are optional.
With the exception of email, any information you provide will be displayed with your comment.

Name: First * Last

Work: Title Field Facility

Location: City State - Select one -

Comments: *

To prevent comment spam, please type the code you see below into the code field before submitting your comment. If you cannot read the numbers in the below image, reload the page to generate a new one.

Enter the security code below: *

653973

Receive emails when a new comment is posted
Remember me on this computer

POST COMMENT RESET

Fields marked with an * are required.