Meaningful Use and Encryption
By Angela Short, MHA, CPCO, CPC-D, The Dermatology Group, PC

Concerta Healthcare agreed to pay $2 million over data breaches steaming from an unencrypted stolen laptop. Hospice of North Idaho agreed to pay $50,000 for an unencrypted stolen laptop that contained less than five hundred patients. These two cases only scratch the surface of the number of cases settled or under investigation by the Office of Civil Rights. To illustrate the risk that health care organizations face in terms of cyber crimes, on April 8, 2014, the FBI issued a notice indicating that "cyber activity is likely to increase in healthcare due to the large number of providers making the transition to EHRs, the laxed data security, and the potential value of the medical records on the black market." This should be a wake-up call to health care providers.

To comply with Stage 1 of Meaningful Use, healthcare providers must attest that they have complied with measures regarding the use of electronic health information. As part of this attestation, a provider must conduct a security risk analysis in accordance to requirements under 45 CFR 164.308(a)(1). A security risk analysis is a comprehensive evaluation of the medical practice's electronic resources (e.g., EMR) and identifying, if appropriate, that measures are in place to protect this information when at rest, in motion (e.g., emailing information), in transit, (e.g. on a laptop) and when information is being destroyed.

Though, healthcare providers are required to identify vulnerabilities in the way they secure health information and put measures in place to reduce or mitigate the risk of the information being compromised, probably the greatest risk that most practices overlook are measures to protect information in motion. Ask yourself the question, how often does a provider within your practice email communication regarding a patient, or send information about a patient to an outside vendor by email, or to their home email address? Even at a more basic level, how often is health information transported via a laptop or tablet? What measures are you taking to make this information unreadable while in motion? Is email even allowed under the statue and if so must a provider encrypt the communication?

While the statue does not prohibit email communication, the statue does require providers to determine the level of risk that the information being emailed could be inappropriately accessed. Based on the risk, a provider may elect a number of different options including:

- Accept the risk due to the fact that the office rarely emails information pertaining to a patient, and the likelihood that the information could be compromised is so low that the practice is willing to accept the risk. (Hint, this is probably not the option that you want to elect regardless of the amount of information being emailed.)
- Adopt a practice wide policy prohibiting an email that contains patient information. While this may sound like a simple solution, it probably is not realistic in most practices because staff needs a way to communicate with vendors and others regarding a patient.
- Put measures in place to ensure the information being sent is encrypted. Regardless of the email system that you are using, there are simple, cost effective options to ensure the messages that you are sending/receiving are encrypted.

Ask yourself another question, how many times have you received emails from friends and/or family where the message was obviously not sent by the person you know? You often open the email to find a link that hopefully no one clicks on. This email should be an immediate red-flag that this person's email has been compromised and someone has their password. This is just an example of how easy it is for your email account to be compromised. If someone compromises your email, then the emails stored on the email account can be comprised. By encrypting these messages, even if the account is compromised the messages are not readable.

Depending on the email service that you are using, encryption is likely available to protect emails stored on the email server. For example, if your practice uses an exchange email account, the practice should be able to set up encryption to protect emails stored on the server. Check your email service provider regarding the availability of encrypting emails on the server and how to set this up correctly.

Additionally, you should encrypt messages being transmitted that contain protected health information. Encrypting the message generally involves a two step process that requires an action from the sender and receiver. Again, many email services have this capability built into the system, for example at my practice, we can type secure message into the subject line and the system recognizes that the message needs to be sent securely. The receiver will receive a message that they have a secure message, and the receiver must go through an exercise to verify that they are the intended receiver and then they will be able to view the message. Yes, it takes an extra step on both sides but this extra step could avoid a fine and/or penalty should your email face a cyber-attack.

The practice must also evaluate laptops and mobile devices to determine if encryption is needed to protect the information stored on the hard drive. While a preferred method for providers and staff to access confidential information is through a secure Virtual Private Network (VPN), let's face it that if an employee needs to access a report out of the office and has been issued a laptop, then it is likely that they may not be in a location where accessing the VPN is possible, for example while traveling by airplane, although some airlines now offer wi-fi service. It only takes a minute looking away that someone can walk away with the laptop. To ensure mobile devices are protected, practices should, at a minimum, do the following:

- Take an inventory of all mobile devices, whether it be a laptop, tablet or smart phone. Keep in mind that you also need to inventory staffs use of personal mobile devices and the information being stored on them. It is highly suggested that your practice have a policy that prohibits storage of protected health information on non-company owned devices. While this may result in your practice buying additional devices, this is a small amount of money in comparison to the cost associated with cleaning up after your data has been stolen.
- Take an inventory of who should have access by position. Does the front desk really need to access information from home or on a laptop? Does your physician on call need to access information from home? The front desk probably does not need to access information outside the office where the provider would clearly need access. As part of the security risk analysis, your practice should go through every job description and clearly outline the level of access this position/employee should have.
- Establish clear policies and procedures for use of laptops and other mobile device as it relates to protected health information. Train staff on the policies and procedures and have them sign off that they have received and agree to follow the policy.
- Take the extra step to encrypt the laptop. There are a number of software programs on the market that can help protect the device, but it is highly suggested that you use an individual/vendor that has experience setting the software up on a device as you can easily lock yourself out of the computer.

Again, while HIPAA does not require encryption, having encryption in place can help prevent a lot of headaches if a laptop is stolen. On a side note, I have personally been the subject of my information being compromised. A company that I worked with previously had a laptop stolen and all employees' information was stored on the computer including social security numbers, address, and annual salaries. The company was required to offer a monitoring service to help with any potential threats. This was ten years ago when cyber attacks were not as common and I can tell you first hand that as the person having my information compromised it was scary. It has increased my awareness of ensuring my credit report is accurate. I do not think any organization wants their customers to worry about the personal/demographics information that they are providing. While HIPAA does require every organization to take the initiative to conduct a security risk analysis, healthcare organizations should not stop at the analysis. Healthcare organizations should exercise preventive measures to reduce the risk of information being compromised.

References:

http://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf
http://www.pcworld.com/article/254338/how_to_encrypt_your_email.html
http://www.pcworld.com/article/2025462/how-to-encrypt-almost-anything.html

About the Author

Angela Short joined The Dermatology Group in 2007 as the Vice President of Operations. Prior to joining The Dermatology Group, Angela served as the Chief Operations Officer for a hospital owned multi-specialty group in Northeast Tennessee and Southwest Virginia. In this role, Angela facilitated numerous practice acquisitions. Additionally, Angela served as the Chief Compliance Officer with a large multi-specialty group in Virginia, where she managed a government mandated compliance program. Angela earned a Bachelors Degree in Business Administration with a concentration in Accounting from East Tennessee State University, and a Masters in Healthcare Administration from Seton Hall University. Angela is a Certified Medical Practice Executive, Certified Professional Coder, and Certified in Healthcare Compliance.

Originally in May/June 2014
Tags: Meaningful Use