ARE YOU PREPARED FOR A DATA BREACH?

It's no longer a matter of if, but more a matter of when.

BY MICHAEL L. BRODY, DPM

© Thelightwriter | Dreamstime.com

Data breaches are a simple reality. Recently highly publicized breaches have been experienced by United Airlines, The U.S. Office of Personnel Management, Anthem Health, Target, Experian, Nieman Marcus, and Ashley Madison. Health First, Anthem Health, Planned Parenthood, and UCLA have experienced high profile medical data breaches. Some of the organizations are already starting to experience lawsuits from individuals who have had their personal information exposed. It is more and more obvious that it is not a matter of if you will have a data breach, but more a matter of when. Many of the breaches listed here happened months or years in the past but were only recently discovered. It is entirely possible that you have already experienced a data breach, but you are not yet aware that it has happened.

Chinese government-sponsored hackers have been implicated in many of the large breaches that have been in the news. In addition, health data breaches have been caused by physical theft of devices such as laptops, improper disposal of retired data storage devices (hard drives), and improperly configured software and websites.

That raises the question "How can I protect myself?" There are a number of steps you can take in your practice to minimize the probability of experiencing a HIPAA breach and then there are other steps you can take to minimize the pain caused to your practice when you do experience a breach.

It is more and more obvious that it is not a matter of if you will have a data breach, but more a matter of when.

Step 1: Keep your technology up-to-date.

- Make sure that each and every computer in your office, including your servers, has up-to-date anti-virus software running.
- Make sure that you keep up with all security patches released by your software vendors, including the software updates provided by the vendor of your operating system.
- If you use wireless networking, make sure that you have the best possible encryption on your wireless network.
- Have a properly configured firewall between the computers in your office and the Internet. This includes changing the default password on your firewall from "PASSWORD" to something that is more secure.

Step 2: Encrypt your devices.

- Meaningful Use Stage 2 requires that all data we store on drives (data at rest) must be encrypted. This includes the hard drives in computers, fax machines, printers, and scanners (yes, these other devices sometimes contain hard drives). Back-up devices must also be encrypted. Backup devices can be:
  - USB Drives
  - Removable Hard Drives
  - Tapes
  - CDs and DVDs

Continued on page 56

Data Breach *(from page 55)*

Step 3: Communicate with your vendors.

• If you use a cloud-based EHR or Practice Management Solution, contact your vendor(s) and ask them for documentation on their current security procedures to protect your data. Get this information in writing.

Step 4: Monitor your devices.

• Know where all of your computers, laptops, back-up devices and all other devices that may contain patient information are at all times. A missing device that has patient information MUST be considered a breach of patient information.

This brings us to the issue of patient information that may be stored on smartphones. Smartphones have direct data connections to the Internet.

• They are not protected by firewalls.

• They do not have anti-virus software.

• They are not encrypted (password protection is NOT encryption).

If your smartphone is encrypted and then lost, the person who finds the phone will not be able to access the data on the phone. But if you have entered your PIN on your phone, the information is effectively decrypted and any rogue software that may be on your phone will be able to expose that information to the Internet. This is why you should not store patient data on a smartphone, even it is encrypted.

As a result, many of the safeguards that we can put into place for our computers and computer networks do not exist to protect the data that may be stored on these convenient personal devices. This leaves smartphones much more vulnerable to attack and for data breaches than other devices where we may store patient info. I strongly recommend that doctors and staff DO NOT use smartphones to store patient data of any type, including clinical images. If you need to take clinical photographs (which are a very good method of documenting patient conditions), use a digital camera that you connect directly to your computer.

Never use the USB port on your computer to charge your smartphone. You may have noticed that if you plug your smartphone into your computer your computer will discover and communicate with the smartphone. Once this has happened, it is possible that there is a direct connection from your computer to the Internet through your smartphone. This direct connection is bypassing all of the security that has been put into place to protect your computer network. This process unlocks and opens the back door to your patient data.

Even with the best precautions data breaches can and do happen. Should your practice experience a data breach you may be responsible for:

• Providing credit monitoring services to the patients involved.

• Fines from the federal government.

• The costs associated with notification of each and every patient involved in the breach.

• Potential lawsuits from patients involved in the breach.

• Negative publicity related to the breach.

There are steps you can take to mitigate some of these potential adverse consequences to a data breach. The first is to have cyber security and HIPAA breach insurance. These policies can help with costs associated with the data breach, except for fines. These costs can add up quickly, and having this insurance policy may just save your practice should you experience a breach. When selecting a policy and your limits of liability, think about how many patients you have in your practice, and how much it would cost to provide credit monitoring to each and every patient for two years. Then think about the potential lawsuits. Have at least one million dollars in coverage for this type of insurance.

While an insurance company cannot protect you from the financial costs associated with a fine, there are steps you can take to protect your practice from fines for HIPAA breaches.

• If you have completed a proper HIPAA Security Risk Analysis and Risk Mitigation Plan,

• And you have followed through on the Risk Mitigation Plan,

• And you have documented the risk analysis and risk mitigation plan and your actions, then should you experience a breach and you properly respond to that breach within 30 days of discovery of the breach—you are exempt from federal fines related to that breach.

If your smartphone is encrypted and then lost, the person who finds the phone will not be able to access the data on the phone.

Discovery is a very important word here. Earlier in this article, we mentioned that there were a number of breaches that were going on for a number of months or years prior to discovery. No matter what day a breach happens, the 30-days clock starts ticking once the breach is discovered. With proper planning and a good faith effort to complete your HIPAA Security Risk Analysis and Risk Mitigation Plan and with proper and prompt follow-up after the discovery of a breach, you can avoid federal fines related to HIPAA breaches.

Now is the time to take all of the necessary steps to protect your data and to properly document those steps. Like many other aspects of our practices and our lives an ounce of prevention is worth a pound of cure. **PM**

Dr. Michael Brody has presented webinars for the e-Health initiative, (www.ehealthinitiative.org/) and is active in the EMR workgroup of the New York E Health Collaborative (www.nyehealth.org/). He has provided consulting services to physicians for the implementation of EHR software and to EHR vendors to assist in making their products more compatible with CCHIT and HIPAA guidelines. Dr. Brody is a member of AAPPM.