DATA BREACHES IN THE DENTAL PRACTICE

by Molly Singer

Imagine this: Your smartphone or laptop that had unencrypted patient ePHI (Electronic Protected Health Information) on it was just stolen. What do you do?

The correct answer is look at your incident response plan. It is extremely important that every practice have an up-to-date incident response plan. The plan should include whom to contact in the event of an incident and outline a procedure for moving forward.

Another question to ask is: What would you do if your computers that held important files were damaged?

Most dental practices have some type of back-up solution in place, but they don't really understand what they have. Do you have just file system backups or do you have full system back-ups? File system backups only back up your data files. The issue with a file system backup is the data might be useless without the application software to run it. Many online solutions like MozyPro and Carbonite are only file system backup solutions.

Working in the dental profession for more than 25 years, I have seen a lot of changes. I recall the earlier days of ledger books, peg boards and DOS Software systems. Then came Windows-based dental practice management software as we evolved into the current digital age of dentistry. Many dental practice owners were initially reluctant converting from a manual system to a digital system. Most practices had greater success after converting over with the proper planning, support and training.

Familiarize yourself with the following acronyms, as you look closer at your standards and protocols to protect your patients' private protected health information:

HITECH Act:
The Health Information Technology for Economic and Clinical Health Act

EHR:
Electronic Health Record

EMR:
Electronic Medical Record

HIPAA:
Health Insurance Portability and Accountability Act

PHI:
Protected Health Information

EPHI:
Electronic Protected Health Information

PCI:
The Payment Card Industry Data Security Standard (PCI DSS) https://www.pcisecuritystandards.org

I often tell my clients "If you are not changing you are not growing" and "failing to plan is planning to fail." As a business owner and CEO of your own company, you should be aware of how vulnerable your practice could be from data breaches.

I have seen obvious issues, which could lead to potential data breaches. These include:

- Routing slips, health history documents and insurance forms with completed information (yes, including Social Security numbers and all) tossed carelessly into garbage cans
- Passwords for the network and practice management on sticky notes right on the monitors or under the keyboard
- Blank or weak passwords
- No HIPAA controls or training
- Practice management software left logged into the network unattended
- Patient credit card numbers and credit card information on a Post-it note or printed out on the schedule as a reminder to process the patient's credit card payment

To start, you should ask yourself the following questions about your current compliances:

- Is your entire staff trained on HIPAA?
- How much of your patient's private information is kept secure?
- When was the last time you performed a self-audit of your securities?
- What would you do if you had a data leak?
- What would the cost be to the office if patients' electronic Protected Health Information (ePHI) were stolen?
- Are you confident your business insurance covers the expense of potential data breaches?
- What steps have you taken to protect your practice?

Your entire staff needs to be trained on HIPAA. It's one thing to sit people down and make them watch a video, but does that really teach them what they need to know? Make the training process fun and interactive. Inform staff members that at the end of training there will be a 25- to 50-question test and the top performer will be rewarded with some form of prize.

All of your patients' private information must be kept secure. This doesn't mean just the electronic information – everything that has private information must be locked up. Physical data should be kept in lock cabinets in a locked room with limited access. Electronic information needs to be encrypted and stored where access is limited to authorized users only.

You should conduct self-audits of your practice at least once a year. If you don't feel comfortable doing this yourself then consider reaching out to a qualified professional. The audit will show you where you're weak, and which areas need to be fixed immediately. When every dollar counts, this ensures you're getting the best value for your money.

The correct answer here is turn to your Incident Response Policy. Every practice needs to have one of these. There are several free templates available online (URLs on page 100) which would be a great place to start.

The cost a practice will be faced with depends on the level of a breach. With that being said, your cost will be far less if you've spent the time to develop a proper plan for information security defense. It usually will cost five-times more for a company to respond to a plan that has no controls in place compared to an entity that has a mature security plan.

Many insurance agencies now offer coverage to safeguard your assets in the event of a data breach. Consider reaching out to them to discuss your needs.

If you're not satisfied with your current information security strategy it's important that you realize that before it's too late. We'll be covering some action items you can do today to help yourself create a plan.

Protecting your patients' data should be a concern of every practice. It's ethically the right thing to do and it will go a long way in showing them that you do care about their private information. If this isn't enough of a reason for you, consider that audits have started to take place. According to an ADA news article titled "Government Auditing to Ensure HIPAA Compliance" written by Kelly Soderlund on December 12, 2011, the federal government is conducting audits to ensure medical professionals and businesses are complying with the privacy, security and breach notification provisions of the HIPAA. This program will complete the pilot phase this year, which means it will soon become a standard practice.

Every week organizations report that they have been attacked by malicious cyber attackers. Dentists and all healthcare professionals who have electronic-protected health information (ePHI) need to ensure they're following HIPAA/HITECH and are doing everything that's within reason to protect their data. According to Ryan Sevey, CISSP, the director of information security solutions with Quanexus, most attacks that occurred in 2012 were due to ease and opportunity. Sevey says one reason for this is smaller companies might think they are not a target, however, in the eyes of an attacker, any business regardless of size is a target. "If anything, a smaller organization presents a better target. The reason for this is that often smaller companies do not have a defined budget for Information Security. To the attacker, a smaller organization presents a smaller risk," says Sevey.

According to the 2012 Verizon Breach Report, companies with 11 to 100 employees reported 570 breaches. This is up from 436 reported breaches by the same company size in

continued on page 100

2011. In comparison, 101 to 1,000 employee companies reported 48 breaches.

Sevey gave the following ideas on how dental practices can better protect themselves. Some of these items can be done today, and others you should work with a qualified professional for assistance.

Risk Assessment

The very first step (and this is required under HIPAA) is to have a risk assessment. Every company, regardless of size, needs to understand its risks. Only once we understand what our potential threats are can we properly defend against them. If you do only one thing this year that's related to information security it should be a risk assessment.

The risk assessment can be done internally or by a qualified professional, and serves as a road map of what you should do. Below is a short list of items a risk assessment might include:

- Business Mission Review
- Critical System Identification
- Asset Map
- Threat Identification
- Expected Controls
- Administrative Review
    - Policy
    - Training
    - Procedure
- Technical Review
    - Design
    - Security Testing
    - Configuration
- Physical
    - Policy
    - Procedure
- Determine Risk
- Risk Mitigation
    - Safeguard Selection
- Recommendations
    - Acceptance
    - Mitigation
    - Assignment

It's important to note that each risk assessment is unique. What one company needs will be different from another. Once the risk assessment is completed, you will know what your most likely risks are and how much money it will cost to mitigate against that risk. In some instances it's a wise choice to accept the risk, as mitigation would cost more.

For example, if the risk assessment shows that once a year you will lose a smartphone, and the cost of the loss would be $40,000. However, to mitigate it would cost $60,000. In this example, it is recommended that you accept the risk, as mitigation would cost more.

For more information about risk assessments, please visit the following links:

NIST 800-30 Risk Management Guide
http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

Quanexus Blog
http://www.quanexus.com/blog

California Technology Agency – Risk Assessment Toolkit
http://www.cio.ca.gov/OIS/Government/risk/toolkit.asp

Create Defense in Depth

Now that you have a risk assessment, you can work on creating defense in depth. Think of security as an onion, and each control you have in place as a layer to that onion. In this example, our onion might look something like this:

1. Firewall
2. Intrusion Prevention
3. Content Filter
4. E-mail Filter
5. Anti-virus
6. Event Management
7. Device Encryption
8. Vulnerability Scanning
9. Disaster Recovery

As we continue down the layers we begin to see that if one control fails, there are still a number of controls in place. It is important to remember that any control can fail, and sometimes even multiple controls can fail at the same time. Your organizations' security posture should not rely on just a firewall or anti-virus only. It needs to have a layered approach to security. The risk assessment will show you which control you need to have in place, and how quickly you should install it. Every organization should have a firewall and anti-virus, and today most firewalls come with Unified Threat Management (UTM). This means they do more than just filter traffic; they can do things like e-mail filtering, intrusion detection, even vulnerability scanning.

Create Strong Policies

Policies are the driving force to ensure data is properly protected. The dental practice owner needs to create the necessary policies, and ensure that enforcement comes from the top. It

is important for employees to understand that policies are mandatory, and that as an employee they do not have the option of not following it. Some policy examples are Acceptable Use, Data Destruction, Business Continuity, System/Network Security Monitoring and Mobile Devices.

All policies are composed of these basic components:

- Purpose – describes the need for the policy
- Scope – identifies what is covered (people, systems, facilities)
- Responsibilities – lays out who is responsible for what
- Compliance – defines what happens if a policy is violated, and how to measure the effectiveness of the policy

Keep in mind that policies are high level, and should not dive into specifics. They should be easy for all to understand and read. Once policies are established, then guidelines and procedures further detail specific processes to ensure compliance of the policies. Appropriate controls should be put in place for management and auditors to observe compliance of policies.

Proper Employee Education

From a security prospective, employees are often the weakest link in the chain. Specific attacks referred to as social engineering actively target employees in an attempt to entice them to disclose information or conduct an action (such as clicking on a link in an e-mail or opening a file).

The policies you have in place are the first line of education; however this needs to be followed up with proper training. Additionally, your other security controls (such as encryption) need to be user-friendly. Telling employees to encrypt e-mails or data will not have the right effect if they're not properly trained on how to carry out that action. There are multiple online training classes employees can attend, as well as general literature, which should be given to employees. Organizations should have a formal training policy. Your employee manuals should include your security control information.

Understand the Risk Management Process

Compliance and business continuity is all about managing risk. Whether large or small, you need to understand your overall IT environment and associate risks. Risk management is an ongoing process, not something you just do once a year.

The basic steps involve:

- List all your business functions
- List all your IT assets
- Determine which assets are required to support each function
- Categorize each function as low, medium or high with respect to the organization being able to function
- List threats than can affect the asset
- Determine the likelihood of each threat actually occurring
- Evaluate alternatives to manage exposure

There are four basic ways to manage risk:

- Avoid risk – don't implement a product or solution that causes undue exposure
- Share risk – purchase insurance to cover your liability in the event of exposure
- Mitigate risk – implement processes to minimize the chance of exposure
- Accept risk – after evaluating alternatives to manage risk, the cost of the solution might outweigh the negative results due to an exposure (cost benefit analysis)

Once you've chosen your risk management strategy, it is important to have a system to manage the implementation of the solutions (controls). These do not have to be elaborate, but they must be in place to assure the owner/manager/board/auditor that the risk management solution is being implemented. An example of a control for document destruction could be a log sheet indicating what was destroyed and who destroyed it. Then, on a monthly or quarterly basis, that log sheet is reviewed and appropriately filed.

"Every company, regardless of size, needs to understand its risks. Only once we understand what our potential threats are can we properly defend against them."

Have Disaster Recovery/Incident Response Plan

Full system backups backup the entire system including the operating system and files, allowing you to fully recover a failed system, including the data and applications. There are many different full system backup solutions on the market offering various options and some of them include off-site remote storage.

Additionally, the time it will take you to recover from a backup is important. Will it take a matter of hours, days, weeks or longer? Regularly testing your backups (both partial and complete) is recommended. This will not only give you an idea of how long it will take to restore, but also if your backups are

continued on page 102

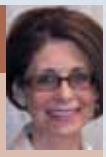
correctly backing up your data. Remember, every day you're spending trying to restore data and get back to an operational status is money you're losing.

Within the last few years, there have been many new technologies brought to market for the small and medium size dental practices that were only affordable to large corporations. If you are still running a tape back-up solution or any solution that is not an imaging back-up solution (full back-up solution), you should contact your IT service provider to look at these technologies.

Conclusion

These topics are a brief introduction to some of the major things an organization can do to help reduce its risk. In the event of a breach that involves personally identifiable information (PII) or protected health information (PHI), it will be important that you're able to demonstrate due care in protecting PHI and PII. You will be in a far better legal position if you're able to show due care and due diligence. For more information or to speak with an information security professional please visit www.quanexus.com. Consider working closely with your practice management consultant to develop a checklist to protect your practice. For more information on dental practice management consulting, please visit www.theparagonprogram.com. ■

Author's Bio



Molly Singer has a detailed background that includes dental IT training and sales, dental practice risk analyst/vender account manager with a dental-specific lender, dental practice management, systems manager and director of marketing and technology for a large multi-location dental practice. She has lectured to dental professionals about embezzlement/theft avoidance in the dental practice, dental practice compliance considerations, start up and practice acquisition transitions, dental practice maintenance and marketing and social media marketing all over the United States. Ms. Singer works with dental professionals as a senior dental practice consultant with Paragon Management Associates, Inc. – www.theparagonprogram.com. Paragon is a national growth and profitability management program based out of Columbus, Ohio.