Vet practices need to protect medical records, client information and employee files.

Hacked!

Don't let your practice become the victim of a cyberattack. Use these tips to protect against a data breach.

By Katie Navarra

You've undoubtedly heard about the cyberattacks on Equifax, Yahoo and other global companies, where computer systems were held for ransom or data stolen or destroyed. Maybe you've received a letter from your bank that said your account number had been compromised and that a new card had been issued.

Banks, retailers and Fortune 500 companies seem like obvious targets for cyber thieves, but what you might not realize is that small businesses have the potential to be more susceptible to cyberattacks than large ones. Hackers know that small business owners often don't invest in sophisticated security technology and tend to be more lax about security protocols.

Today, all companies, including equine veterinary practices, are increasingly the targets of cybersecurity threats. These can range from the theft

ISTOCKPHOTOS.COM

of data to the unauthorized release of confidential information, or even a cyberattack. The resulting data breach can interrupt your daily business and damage your reputation.

"Veterinarians should be particularly concerned with these threats. Veterinarians have statutory and regulatory duties to keep certain information confidential," said Melissa Subjeck, a partner in Hodgson Russ's Business Litigation Practice. The Buffalo-based attorney is also a horse owner.

The consequences vary depending on your geographic location and the type of data breach. When a breach occurs, your business might be subject to negligence claims, state privacy liability and breach-notification liability.

"Every veterinarian, regardless of size, is obligated to have robust security systems in place to protect against cyberattacks," said attorney Avery S. Chapman of the Chapman Law Group, PLC, and the Equine Law Group, PLC.

Thinking about your responsibilities to protect data can be overwhelming. In the article that follows, attorney Gary Schober, a partner and cybersecurity expert at Hodgson Russ, Subjeck and Chapman, offers insight into the type of data a veterinarian must protect. He'll also provided practical advice for increased security practices.

Equine Medical Records

The Health Insurance Portability and Accountability Act (HIPPA) does not cover horses (or any animals). But that doesn't mean that veterinarians aren't required to ensure that medical records are protected and properly transferred.

"Pre-purchase exams and other records relating the condition of the horse can affect the marketability and salability of the horse," Chapman said. "Those are considered confidential and owned by the owner."

Unless a veterinarian is legally required to release medical records or receives written authorization from an owner to share such records, they must be kept confidential. In today's digital world, the vast majority of a horse's medical records are maintained and shared electronically. The notes documenting an emergency visit, MRI or radiographic images taken to assess an injury or facilitate a pre-purchase exam are recorded, stored and shared over the internet.

ISTOCKPHOTOS.COM

"Veterinarians have statutory and regulatory duties to keep certain information confidential," said attorney Melissa Subjeck.

When transmitting such data, it's even more critical to establish a procedure that protects such records. Chapman recommended a two-step verification process and the use of an encrypted link for sharing files such as MRIs or radiographs. To achieve this, he advised clients to send one email that contains the link to records—then a second, separate email containing the password to access those files.

Client Information

In addition to protecting a horse's medical records, a veterinary practice should take steps to maintain the confidentiality of client information. Credit card numbers are the first piece of data most people think of when they think of data theft.

"No one wants to store information that can be stolen, but veterinarians don't want to chase recurring payments, either," Chapman said.

A physical swipe of the card is always the most secure method of accepting a credit card payment, but isn't always practical.

Veterinarians aren't the only business owners who maintain credit card information for regular or slow-to-pay clients. However, you do have an obligation to use secure software to protect the data that is on file.

In addition to the obvious confidentiality requirements associated with accepting credit cards, businesses are also required to take steps to protect a person's identifying information. That includes a person's full name, social security number, bank account number, email address and driver's license number.

Employee Data

Often the focus of data protection is centered on medical records and client information. But any business is required to protect personnel and employment records. This can include social security numbers, performance reviews and medical information related to employees, Schober said.

One way to limit risk is to keep software, firewalls, virus protection systems and operating systems up to date. Desktops and mobile devices can be programmed to update at the close of every business day. Hiring an outside technology professional for an audit can provide insight into security threats for your business.

Once recommendations are made, implement those protocols as soon as possible. Be prepared with an explanation if those guidelines are not followed and a security breach occurs.

Don't forget about paper files. Many practices still rely on paper client records and employee applications and files. Make sure filing cabinets are locked and access is limited to those who absolutely need it.

Technology Best Practices

Because most breaches are technology related, utilizing best practices as they relate to technology is key. Chapman, Schober and Subjeck offer several best practices that any veterinarian can implement regardless of the operating system used.

Dual-factor or two-factor authorization is a process for confirming a user's identity. As implied by the name, two different types of verification are required to confirm a person's identity. Chapman's earlier recommendation for sending separate emails with a password and link to medical records is one type of dual-factor authorization method.

For practices that use remote login and/or VPN servers, a dual-factor verification method could include a combination of a password and a biometric marker such as a fingerprint (similar to those that can be enabled on equipped laptops and new smartphones).

Enabling auto-lock on computers and mobile devices can prevent someone from walking away and the work computer staying "open" to prying eyes. Auto-lock causes the computer to shut down behind a log-in wall when no activity is detected for a specified amount of time.

Password protocols are a top priority for Subjeck. At a minimum, all passwords should be reset from their de-

fault, administrative settings. It's also advantageous to change passwords at least quarterly.

Assigning unique user names and individual passwords comprised of a combination of letters, numbers or characters can help thwart hackers.

"In the public domain, it's considered negligence not to change passwords from the default ones assigned," Chapman said.

Employee training is a critical component for practices that hire employees. First and foremost, employees must understand the importance of protecting the data the practice owns. That includes knowing and following established procedures for sharing data.

Employees should know what information can and can't be shared, or whom they should ask if the occasion arises.

It's also important to train employees to identify and delete questionable emails and attachments without opening them, Schober said. Sometimes the simple act of opening a fake email can alert cyber criminals or put unprotected computers as risk.

Establish record retention protocols. Extraneous data increases a practice's risk for exposure if a hacker is successful in breaching a security system. "It is important that all businesses purge information that is not needed from a regulatory or business standpoint," Subjeck said.

Data breach and cyber liability insurance can provide coverage for legal and forensic services, public relations and crisis management, notification expenses, and defense and liability expenses.

The American Veterinary Medical Association (AVMA) website notes that according to a study from the Ponemon Institute, the average data breach cost per compromised record is $214. Take that amount and multiply it by the number of clients you serve and each record you house, and the cost of settling data breach damages can be staggering.

The AVMA PLIT-sponsored Program through The Hartford Group is one way to obtain data breach coverage to protect your practice.

Schober recommended reviewing the insurance policies you currently have to detect any gaps in coverage that might exist.

Hiring an attorney familiar with cybersecurity can be well worth your time and expense. An attorney or other consultants specializing in cybersecurity can help you develop a comprehensive cyber protection plan for your business.

Take-Home Message

Staying one step ahead of cyber criminals can be challenging. Part of what complicates the process is that there currently are no federal laws that specifically address cybersecurity and a veterinarian's responsibility. The board of veterinary medicine in each state provides the governance, which means requirements and consequences will vary from state to state.

"The ethical rules and privacy laws governing larger practices apply equally to smaller practices," Subjeck said. "Smaller practices can also be subject to allegations of negligence by individuals affected by a security breach."

Taking a proactive approach to protecting the data your practice maintains is your best defense. Work with an attorney or other consultant who specializes in equine and cybersecurity. The American Veterinary Medical Association (AVMA) also offers resources that can help you get started. EM

Ad Index