OFF THE CUSP
Dental industry news, trends and information from Patterson Dental.

KEEPING PATIENT AND BUSINESS DATA SAFE: INFORMATION SECURITY BEST PRACTICES

By Patterson Dental
Dec. 23, 2020

With the recent news of a hack involving U.S. government agencies and tech companies purportedly by Russia state actors, the prospect of falling victim of a data breach is once again on the minds of many business owners and consumers. Russia's alleged hack was large in scale, involving numerous U.S. government networks and private companies' systems around the globe. But not all cyberattacks involve sophisticated techniques and affect large-scale networks. Even small and midsized businesses can fall victim to cyberattacks – and dental practices are no exception.

In July of 2019, a dental practice in Florida fell victim to a ransomware attack targeting a computer running the practice's QuickBooks accounting software. The hackers demanded a ransom of $10,000 to unlock the encrypted data. Fortunately for the practice, no patient or employee information was compromised, and the practice was able to restore most of the lost data without paying the ransom.

And in the fall of 2020, a dental practice in Virginia was contacted by assumed hackers who claimed it had infected its computer server with a virus. The hackers also posted several files from its server to the dark web and demanded a ransom to retrieve the data. Fortunately, the practice said it did not pay a ransom nor did it experience data loss or a significant service disruption.

Each of these examples highlight the importance of making sure your practice is protected from potential cyberattacks. Even if your office does experience a data breach but is able to recover the data without paying a ransom, the occurrence can still be a financial burden due to associated costs of dealing with the matter, such as retrieving the lost data, restoring computer software and securing computer servers. Communicating that personal data may have been compromised due to a cyberattack may even have a negative impact toward your reputation and relationship with patients.

Information security best practices

Methods for protecting your computers, business data and patient data are increasingly complex and ever changing. No checklist can guarantee total security; however, there are some best

practices that can minimize many risks to your systems and data. The following list of information security best practices are recommended for businesses of any size. For a more comprehensive, printable version of the following list, download the free PDF. If you are uncertain about any of these suggestions, please contact your IT support provider for assistance.

1. Regularly update software

Software vendors regularly provide updates to fix security problems and add or fix functionality. Ensure all software products capable of getting these updates are configured to do so automatically. For those who do not have this functionality, set a calendar reminder to check with the vendor periodically for any new updates.

2. Use only maintained software

Using software that is maintained means that the vendor ensures that, as any security flaw or other problem is discovered, a patch is developed and applied. Each revision of software has a useful life, and once that useful life ends, the vendor no longer maintains that software revision, and your systems can be left vulnerable as new weaknesses are exposed and remain unpatched.

3. Change default passwords before using a device or system for normal "production" activities

Vendor-supplied default usernames and passwords are freely and easily available on the Internet. These are the keys to your systems and data; failing to change these passwords leaves your systems vulnerable to easily being reconfigured or accessed without your knowledge.

4. Do not reuse passwords

Efforts should be made to use different passwords for each system you access. If your computer login is the same as your customer database, email, bank account and Facebook account, an attacker needs only a single password to access everything.

5. Use passphrases to assist with choosing strong passwords

Password complexity typically means having a combination of upper case, lower case, numbers, symbols or special characters and a minimum length. While "Passw0rd!" will typically pass most complexity rules, it is relatively common and easy to guess. As an alternative, consider using passphrases to build a stronger password. A passphrase is generally stronger due to its length, but can be structured to be memorable, which can eliminate the need to write it down. A passphrase is essentially a sentence with some substitution of numbers and symbols for some letters. A "3" for an "e" or an "@" for an "a" as an example, and it might look like IL0v3pysicalTher@py or P@ssphrases4Life!

6. Be diligent to recognize phishing email attempts

A phishing email is sent by a cybercriminal impersonating an individual or reputable company, in hopes of getting someone to reveal personal information such as passwords or credit card information through links or attachments included in the email. It can be difficult to spot phishing emails, but here are some common red flags:

- Misspelled words in the email address or the email domain
- Links or buttons urging you to click within the email have an unknown website address
- Spelling and/or grammatical errors within the email
- Requests to send your sensitive data via email or through an attachment or link in the email

7. Protect your network and computers with a firewall

While a firewall is typically a physical device that sits between the internet and your computers to prevent outsiders from getting to your computers and data, it can also be software on your computer – either included with the operating system or purchased from an alternative vendor. If you have computers that you take home or use at public locations to perform business functions, ensure that the computer has firewall software installed, enabled and configured.

8. Protect all computers and servers with antivirus and anti-malware software

Install and regularly update antivirus and anti-malware software on every computer and server used by your business.

9. Secure your wireless (Wi-Fi) network

If you use a wireless network in your business or at home, make sure it is encrypted using the strongest encryption settings available to you and your systems. Currently this is WPA-2/WPA-3 but check with your IT support and/or wireless vendors for suggested settings.

10. Do not allow patients to use the same wireless network as your business computers

Be sure guests using your Wi-Fi network are provided an SSID (the name of the wireless network you see when you try to connect), which is different and separate from your business computers and data.

11. Physically protect business computers and network devices from unauthorized individuals

Ensure your network devices are behind locked doors and only authorized people have access to the room. Further, do not allow computers in public spaces to be left unattended where someone could attempt to install malicious software and/or hardware.

12. Encrypt your data and computing devices

Data that are stored and transmitted should be encrypted. Many software vendors provide encryption capabilities within their products, and a combination of these can provide layers of protection. Configure disk encryption for your computers and servers and configure encryption options for any databases or other key software packages where available.

13. Implement basic security policies

Policies help reinforce the importance of information security – and, depending on the types of data your business handle, may be required. Here are a few policies to help reduce risks that could lead to a security breach:

- **Removable media policy**: Restrict the use of USB drives, external hard disks, thumb drives and any other writeable media
- **Password policy**: Require unique, strong passwords that must be changed periodically
- **Appropriate use policy**: Define appropriate computer and internet use, including that only authorized software may be installed on business computers
- **Data handling and retention policy**: Define how to handle and protect patient information and other vital data; when the data are no longer needed, define appropriate methods for securely disposing of the data

Patterson Dental prioritizes compliance

Patterson recognizes the importance of security and compliance and continues to deliver new security features in our practice management software version releases. For our Eaglesoft customers, the new Eaglesoft 21.00 Update 1 is now available which includes a security enhancement to bolster security related to dental practices and patient data. The update also includes the new ADA 2019 Insurance Forms.

To ensure continued HIPAA compliance and mitigate potential data breach attempts impacting your practice, it is strongly recommended that Eaglesoft customers install this update. As mentioned above, it is important to regularly update any computer software used at your office.

Training office staff in the information security best practices listed above will help reduce the risk of your practice becoming victim of a cyberattack. Taking information security seriously is the first step to keeping both patient and business data safe.

- - -

From Patterson Dental's blog, Off the Cusp. View and share the original blog post: https://www.offthecusp.com/keeping-patient-and-business-data-safe-information-security-best-practices/