OFF THE CUSP

Dental industry news, trends and
information from Patterson Dental.

3 CLOUD-BASED SECURITY CONSIDERATIONS

By Linda Harvey

Jan. 18, 2021

Have you switched to cloud-based practice management software (PMS)? Or are you just beginning to think about ditching your server for the freedom cloud-based services offer? Don't fire your managed services IT provider just yet. As you evaluate different options, keep the following three considerations in mind.

1. Data security

If you plan to eliminate your server, have you thought about where and how miscellaneous patient and/or business data will be stored? Examples of electronic protected health information (ePHI) include referral letters, copies of treatment plans, patient voicemail messages from your VoIP phone system or emails. Storing patient data on individual workstations is not secure even if the device is password protected. Sections 45 CFR 164.312(a)(1) and 164.312(b) of the Security Rule require that you implement secure access as well as audit controls to protect ePHI from unauthorized access—whether it's an unauthorized team member or a hacker. How will you protect your network in general?

Storing ePHI even temporarily on a workstation, then deleting it and emptying the trash bin, is not HIPAA compliant. Sections 45 CFR 164.310(d)(2)(i) and (ii) of the Security Rule require that "PHI on electronic media, clearing (using software or hardware products to overwrite media with non-sensitive data), purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains), or destroying the media (disintegration, pulverization, melting, incinerating or shredding)."

2. Remote login policy

Given all the changes and uncertainty 2020 brought, it is much more common to have team members working exclusively from home and logging in to your PMS remotely. This is certainly the advantage of using a cloud-based PMS. However, don't forget to implement access controls, such as limiting the IP addresses that can log into the PMS, and/or using two-factor authentication. This prevents staff from logging in from locations lacking proper security such as a cell phone, public location with open Wi-Fi, or a friend's tablet.

Section 45 CFR 164.308(a)(1)(ii)(D) requires that you implement procedures to regularly review records of information security activity such as audit logs, access reports and security incident tracking. This includes auditing log ins to your PMS.

3. Password protection

A third consideration includes protecting your passwords. One Michigan dental practice had a close call because they saved their PMS password in the browser. Unfortunately, a team member clicked a link in an email thinking she was renewing their antivirus program, proceeded to pay with the office credit card and suddenly found she had involved the office in a scam. The practice became concerned that their PMS could be in jeopardy because the password had been saved in the browser. Fortunately, their PMS provider was able to verify the ePHI was not accessed by unauthorized individuals. Thankfully, there was no breach.

The most secure option is to not allow any browser to save passwords—and definitely not allow passwords to be posted on a sticky note on your monitor. Use two-factor authentication (2FA) wherever possible. 2FA is a method of establishing access to an online account or computer system that requires the user to provide two different types of information. For example, using a username and password to log into a site, then receiving a numeric code via a text message or email that must also be used to complete the login process.

While you enjoy the business flexibility of cloud-based PMS, remember to have frequent and candid conversations with your managed services IT partner about maintaining optimum—and HIPAA compliant—security of your valued data.

About the author

A nationally-recognized healthcare risk management and compliance expert, Linda Harvey, MS, RDH, HRM, assists dentists and teams in navigating regulatory requirements. She is the founder and president of two compliance-related companies. And is passionate about helping dental professionals become compliance experts for their practice.

During her programs, Linda draws from real-world experience, having worked with offices that have undergone HIPAA, OSHA and Infection Control audits. Linda's programs will challenge you to look at your compliance programs from a different perspective, particularly amid the COVID-19 crisis.

References

Office of Civil Rights. Frequently Asked Questions About the Disposal of Protected Health Information. Accessed 12/26/2020.

- - -

From Patterson Dental's blog, Off the Cusp. View and share the original blog post: https://www.offthecusp.com/3-cloud-based-security-considerations/