ELECTRONICALLY REPRINTED FROM JANUARY 2015

DENTAL PRODUCTS REPORT®

DISCOVERY. ADOPTION. SUCCESS.

dentalproductsreport.com

"With the integration of computers and the Internet into daily practice, patient data and dental records have been transferred to electronic platforms, allowing quicker access to information and easier communication between dental professionals."

HIPAA compliance and digital photography with personal mobile devices

Personal mobile devices such as smartphones may not be that smart when it comes to HIPAA compliance.

SHANNON PACE BRINKER, CDA, CDD,
Editor in Chief, CPS

As technology continues to provide unparalleled advances and innovation, dental practices continue to change their methods for performing treatments, maintaining patient records and communication. With the integration of computers and the Internet into daily practice, patient data and dental records have been transferred to electronic platforms, allowing quicker access to information and easier communication between dental professionals. Additional digitization within the dental practice has also occurred, incorporating digital photographs, digital radiographs, emailing, texting, websites and social media.

As our society has become more mobile and

demanding of its technology and information resources, the more personal on-demand devices have also started infiltrating dental practice. Smartphones, tablets, digital cameras, laptops and other digital equipment now enable a variety of functions within dental operatories almost instantaneously. They provide immediate access to and capturing of information, improving efficiency and practice management. However, although these so-called smart devices make it easier than ever to maximize the information within a dental practice that can lead to enhanced and more efficient care, sometimes their use might not be so smart.

Photographic and information sharing with mobile devices

Smartphones and tablets have permeated our society and our workplace. A survey completed by the Pew Research Center in 2013 determined that 91% of American adults own a cell phone and 56% own a smartphone.[1] In addition to at least half of dental team members owning smartphones, many dental offices have integrated the use of mobile devices into their practices. Mobile devices (i.e., iPads, iPhones, Androids, etc.) are now used for capturing images, chart documentation and interoffice communication.

This can be very beneficial for practices to improve efficiency and communication, as mobile devices are portable, easy-to-use, and convenient. Unlike mobile devices of the past, cell phones and tablets can now take quality images acceptable for diagnostic and treatment planning.[2] Information can be stored on the device or in "the cloud" for network access. These devices also have email and message capabilities to easily share information. Because of the prevalence of popular brands of mobile phones, limited training is required for using this equipment.

In addition to the use of dedicated "practice-owned" portable electronic devices, the use of personal mobile devices for practice-related functions has also increased. Clinicians may use their devices to share information and photographs about cases with colleagues, talk with patients or communicate with office staff. With access to the dental office network remotely, some team members can work from home charting or accessing billing information, while using their personal devices to check in and ask questions of staff members in the office. Additionally, some social media marketing encourages staff members to take photographs on their personal devices around the office and post them on the Internet. The convenience of this technology may be too good to pass up, but the seriousness of patient privacy, along with new regulations and guidelines that have been developed, may give you reason to pause to ensure proper patient information protection.

***Dental digital cameras** such as Shofu's EyeSpecial C-II provide practitioners with the ability to take variety of diagnostic images. These cameras can be securely locked away to protect patient privacy.*

Digital data standardization

With the introduction of the Health Insurance Portability and Accountability Act (HIPAA) in 1996, dental practices became a covered entity responsible for creating and implementing policies to protect personal health information (PHI).[3] By establishing national standards, these policies required dental practices and team members examine the way they treated PHI within their practice. The HIPAA guidelines include two major components: The privacy rule and the security rule.

Under the privacy rule, the law requires that HIPAA-covered entities must implement safeguards to protect PHI. Another component to HIPAA, the security rule, is far more comprehensive, and sets standards for access, management and storage of electronic patient health information (ePHI). This rule requires that ePHI be maintained with confidentiality, integrity and accessibility, and that practices utilize security risk assessment to demonstrate their ability to protect ePHI.[4]

Introduced in 2009, the Health Information Technology for Economic and Clinical Health (HITECH) Act widens the scope of the privacy and security protections of HIPAA and provides more enforcement.[5] This law further expands upon the principles of protecting ePHI and places liability on the

practice to prove compliance on all HIPAA/HITECH rules. This spans threat monitoring to documentation of ongoing security measures, even if third-party applications are used for encryption. It also requires that the sender and receiver of an ePHI file or email utilize secure locations, as well as a secure pathway through which the material is sent.

In addition to HIPAA and HITECH, systems are required to be Digital Imaging and Communications in Medicine (DICOM) conformant, with all images taken in the practice meeting these standards.[5] DICOM images include not only digital images, but also any pertinent patient data or notes regarding the images.[6] Thus, any ePHI images stored on personal mobile devices or even mobile devices within the practice must be secured and shared over a secured network. With the increased scope of requirements for maintaining the privacy and security of ePHI, dental practices must assess the risks present in their current policies and equipment.

Avoiding risk with mobile devices

Although mobile devices provide a convenient and easy-to-use option for taking photographs and sharing information, according to the Department of Health and Human Resources, theft and loss of unencrypted devices and media storage have been the leading culprits of major HIPAA health data breaches.[7] Another study of health care workers determined that theft accounted for 66% of the reported breaches over the past two years.[8] These data breaches occur generally because the mobile device did not have users enter a password or provide biometric identification to access the information stored on the device.[9] Additionally, these devices were typically not encrypted, meaning ePHI could be shared with anyone with access to the mobile device, and the devices used public Wi-Fi connections or unsecure cellular networks to send and receive ePHI.[9]

To avoid some risk while continuing the use of mobile devices in the dental practice, a variety of safeguards are available. These include setting strong passwords, encryption, automatic log off, requiring a user ID, enabling remote wipe, locking the device, registering the mobile device, installing a firewall and using a secure Wi-Fi connection.[10] However, when using personal mobile devices, these safeguards may not be enough to be categorized as HIPAA and HITECH compliant.

Dental-specific equipment may be the best approach to ensure full HIPAA, HITECH and DICOM compliancy. Dedicated dental digital cameras provide dental practices with the ability to take a variety of photographs, ideal for diagnostic purposes and treatment planning. These devices can be securely locked away, and can either utilize a secure Wi-Fi network for transfers or connect directly to the practice computer. Once on the computer, these images can then be shared through secured access to other necessary parties. Although some convenience may be sacrificed, these cameras are typically lightweight, intuitive and ideal for dentistry, capturing precise and accurate photographs of the face and intraoral cavity.

Using Apple devices and mobile apps

For practices that choose to utilize mobile devices for patient care, especially Apple products (e.g., iPhones and iPads), there are several ways to make your devices more HIPAA and HITECH compliant.[11]

1. Set longer passcodes. The automatic 4-digit pin does not provide adequate security, and users of Apple devices are recommended to create a longer passcode of between 7-10 characters.

2. Activate remote features. Apple products include three options for lost or stolen iPhones and iPads. The erase data feature erases all data on the device if the wrong passcode is entered 10 times. Remote tracking utilizes the iCloud to locate the device as long as the device is connected to Wi-Fi or has a cellular signal. Remote wipe can be initiated as long as the device is connected to Wi-Fi or has a cellular signal, but once wiped it can no longer be tracked. By activating these features, the data can still be removed from the device and protected in the event of a lost or stolen device.

3. Disable Siri. By disabling Siri when the phone is locked, the voice-activated feature is unable to access information when the phone or tablet is locked.

> **"The convenience of this technology may be too good to pass up, but the seriousness of patient privacy, along with new regulations and guidelines that have been developed, may give you reason to pause to ensure proper patient information protection."**

4. Avoid auto-login apps. Although most dental professionals utilize mobile devices for convenience, auto-login apps are a major threat to ePHI confidentiality and security. This includes the native Mail application on Apple devices. In order to remain HIPAA-complaint while using mobile devices, users should access mail by using the Internet browser that requires a username and password, and users should always logout after each session.

In addition to the native apps found on Apple devices, additional application development has led to a variety of dental specific apps. The purposes of these apps are mixed, as some focus on providing convenience and instant access to information, while others claim to provide better security and HIPAA-compliancy. Before utilizing any applications on your mobile device, users must determine whether the app will have access to ePHI, and if it does, if the information will remain HIPAA compliant. This includes requiring a username and passcode upon opening the app, ensuring that the material on the app is encrypted, and safeguarding that the information is stored in a secure cloud network, not on the mobile

device itself.

Some applications (e.g., Dropbox and Google Drive) are not secure and can put your data at risk because they have not signed HIPAA-compliant Business Associate Agreements, and they allow, in some cases, unauthorized users to access your information without your knowledge.[11] Users must research any applications they download to their phone that could potentially be a threat to ePHI data, in order to remain HIPAA and HITECH compliant, and to avoid any breaches of patient information.

Conclusion

Due to the high demands and technological advances within dental practices, many offices have found that utilizing personal and office specific mobile devices improves efficiency and convenience. However, with strict regulations for storing and sharing patient information by HIPAA and HITECH, dental practices must consider the risks in utilizing mobile devices in every day practice. The law comprehensively protects any type of patient information stored by a dental practice, and with more enforcement, dental practices must implement strict policies regarding personal mobile devices and secured sharing. By utilizing equipment designed for dentistry (i.e, dental digital cameras), dental practices reduce their risk for HIPAA and HITECH violations and yet continue to capture and share essential information compliantly. ●

ABOUT THE AUTHOR

Shannon Pace Brinker, CDA, CDD is a national and international speaker and published author. Shannon serves as the editor in chief of Contemporary Product Solutions, which she owns with her husband Erik. Contemporary Product Solutions provides product reviews for the complete dental team, and is the only dental editorial that combines product reviews for the whole team. Shannon is a past faculty member at the Dawson Academy and Spear Education. She is an active member of the AACD and the first auxiliary to sit on its board of directors. Shannon was selected as one of Dental Product Report's 25 most influential women in dentistry, and Dr. Bicuspid's dental assistant educator of the year in 2012. For more information, Shannon can be contacted at shannon@cpsmagazine.com.

REFERENCES

1. Smith A. Pew Smartphone Ownership—2013 Update. 5 June 2013. Pew Internet. Retrieved from www.pewinternet.org/Reports/2013/Smartphone-Ownership-2013/Findings.aspx.

2. Helvey GA, Culp L, McLaren EA. Developing a digital dental team. Compend Contin Educ Dent. 2012;33(12):654-5.

3. Summary of the HIPAA Privacy Rule. 1996. United States Department of Health and Human Services. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf.

4. DiMatteo A, Latanyshyn KA. The case for digital radiography. Inside Dent. 2014;10(10):110-9.

5. HITECH Act Enforcement Interim Final Rule. 2009. United States Department of Health and Human Services. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html.

6. Farman A. DICOM for digital imaging and communication in dentistry. Inside Dent. 2009;5(8):80-3.

7. McLaughlin J. The great BYOD challenge: 5 tips for implementing a HIPAA-compliant "Bring Your Own Device" policy. The Profitable Dentist. 2014;249:10-1.

8. HIPAA Security Rule Compliance When Communicating with Patients Using Mobile Devices. Jan 2011. Center for Democracy and Technology. Retrieved from http://www.projecthealthdesign.org/media/file/Mobile-Device-Privacy-and-Security-Webinar-Slides-012511.pdf.

9. Lewis Dolan P. Doctors driving IT development with their mobile technology choices. 23 May 2011. American Medical News. Retrieved from http://www.ama-assn.org/amednews/2011/05/23/bisb0523.htm.

10. Your Mobile Device and Health Information Privacy and Security. 21 March 2014. HealthIT.gov. Retrieved from http://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security.

11. Rios J. HIPAA Security for iPhones. 10 Oct. 2013. HITECH Answers. Retrieved from http://www.hitechanswers.net/hipaa-security-iphones/.