Maintaining Patient Privacy

Is Your Email HIPAA-compliant?

BY M.H. JIM PUN, MENG, DDS

Computers are an integral part of our daily lives. They increase productivity, enhance understanding, and simplify even the most difficult tasks. Arguably, life would be much more difficult, less productive, and maybe even harder to understand without computers. It should come as no surprise that, according to a 2006 American Dental Association study, 96 percent of dentists used computers at home and 93 percent used them at work. Furthermore, 91 percent of dentists used email for personal communication and 75 percent used it for professional communication.

Of course, this dependency on computers can have a downside. Digital patient records are often quicker and easier to access than traditional hard copy files, but the same technology that makes these patient records easier for you to access also can make them—and you—susceptible to privacy and legal concerns.

Our patients' privacy, even in electronic form, is valuable and needs to be protected, and the Department of Health and Human Services (HHS) formally recognized these privacy concerns through the Health Insurance Portability and Accountability Act (HIPAA) of 1996. Using HIPAA's Privacy and Security Rules and the 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act, the HHS maintains standards for electronic health care transactions and patient information, and you must maintain these standards, too.

The HIPAA Privacy Rule

The HIPAA Privacy Rule sets national standards for the protection of certain health information. According to the U.S. Code of Federal Regulations (CFR), protected health information (PHI) is "any oral or recorded information that is created or received by a health care provider (and other affected entities) about an individual that relates to his or her physical or mental condition, the provision of health care, or the payment of the health services." PHI includes any information that is collected about the past, current, or future conditions of a patient's care and medical services. Some very common pieces of PHI that your dental office collects daily include patients' names, social security numbers, addresses, and even birthdays.

The HIPAA Security Rule

Complementing the Privacy Rule, the HIPAA Security Rule sets national standards for the protection of certain health information that is stored or transmitted in an electronic format, known as e-PHI. The Security Rule requires all health care providers and covered entities, including dentists, to maintain reasonable policies and procedures to protect e-PHI. According to the CFR, this rule requires that providers:

- Ensure the confidentiality, integrity, and availability of all e-PHI created, received, maintained, or transmitted.
- Protect against any reasonably anticipated threats or dangers to the safety or integrity of e-PHI.
- Protect against reasonably anticipated forbidden uses or disclosures.
- Ensure compliance by their workforce.

Essentially, this rule means that your dental practice must always take the necessary steps to protect identifiable patient information that is transmitted in any electronic format.

The HITECH Act of 2009

Included in the American Recovery and Reinvestment Act of 2009, the HITECH Act sets national standards for the notification of unauthorized acquisition, access, use, or disclosure of

To make all PHI-E compliant with HIPAA's technology standards, your dental office will likely need to incorporate various electronic security controls. Combining two or more security models can help you to ensure that your PHI-Es are safe no matter when they were created, how they are transmitted, and who has access to them.

e-PHI. In addition to including health care providers, this act requires business associates, vendors, and related entities to comply with HIPAA's Privacy and Security Rules. Under this act, a provider who willfully neglects to comply can be subject to penalties of up to $1.5 million.

HIPAA and your email

No matter how many emails your office sends out each day, it's important to remember that these forms of communication can be considered e-PHI. When your emails contain important patient information, they are classified as PHI emails (PHI-E). This classification requires you, as a health care provider, to comply with HIPAA security standards when sending out emails.

According to the CFR, PHI-E must have the following technical safeguards:

- *Access controls.* These controls allow only approved users or software programs to have access to e-PHI.
- *Audit controls.* These controls must use hardware, software, or procedures to record and examine all electronic activity using or containing e-PHI.
- *Integrity.* Covered entities are required to implement policies and procedures that protect e-PHI from improper destruction or alterations.
- *Person or entity authentication.* Health care providers are required to implement procedures and systems verifying that a person or entity seeking access to e-PHI is approved to receive this information.
- *Transmission security.* Health care providers and covered entities must use technical security measures to prevent unauthorized access to any e-PHI transmitted over an electronic network.

Ensuring HIPAA compliance

When using PHI-E, compliance with access controls, audit controls, entity authentication, and transmission security can be accomplished through the use of computer programs, procedures, or protocols that address each standard independently.

Alternately, your office can subscribe to or establish a secure website to handle and transmit your PHI-E. These secure websites work similarly to those that are used for online banking. Using such a website model will safeguard against most, if not all, HIPAA concerns. Additionally, these sites often require the person requesting the e-PHI to authenticate his or her identity using unique information. This unique identity also will allow your website to maintain adequate audit control.

PHI-Es also can be securely transmitted using electronic networks, such as the Internet, with methods like Transport Layer Security (TLS) or Internet Protocol security (IPsec). Both TLS and IPsec work to encrypt transmitted information, keeping it safe from tampering and theft. Though these methods help to protect e-PHI passed via PHI-E, it still remains difficult to maintain the integrity of all PHI-E, as it needs to be protected during its entire digital life.

However, Digital Rights Management (DRM) is one way to ensure the integrity of PHI-E, because it uses various technologies to limit access to and use of digital content by owners, publishers, and manufacturers. Typically, these technologies are used to control unauthorized (and usually unpaid) access to online music or videos, but they also can be used to protect electronic documents, such as email. Though there are many ways to apply DRM to electronic documents, the most comprehensive solutions use proprietary viewing software on recipients' computers and a separate server for administering access rights.

To make all PHI-E compliant with HIPAA's technology standards, your dental office will likely need to incorporate various electronic security controls. Combining two or more security models can help you to ensure that your PHI-Es are safe no matter when they were created, how they are transmitted, and who has access to them.

When transmitting PHI-E, it is important that your dental team members take great care to ensure that your office complies with HIPAA regulations. For small dental offices with limited resources, PHI can be printed onto paper or film and delivered via traditional mailing methods that are not subject to the HIPAA Security Rule or the HITECH Act. However, as we become more and more dependent on technology, most of our offices must transmit this PHI electronically.

Remember, when you send PHI-E, not only are you sending email communications, but you also are sending information that must be protected. This information must be safeguarded for the protection of not only your patients, but your dental practice, too. ◆

M.H. Jim Pun, MEng, DDS, graduated from the University of Western Ontario School of Dentistry in 2000 and completed a General Practice Residency (GPR) at the Ohio State University College of Dentistry. Dr. Pun has a keen interest in the practical application of technology in dentistry and how this technology can improve patient care. He currently operates a private practice in Marion, Ohio. Dr. Pun can be reached at *pun@neatsmile.com.*