RM Matters
December 2014

The Dentists Insurance Company
1201 K Street, 17th Floor, Sacramento, CA 95814
800.733.0634 thedentists.com

Email in the Age of Privacy

By TDIC Risk Management Staff

The ongoing discussion about patient privacy leads to numerous questions. The Dentists Insurance Company (TDIC) reports increased inquiries on its Advice Line about patient privacy and email communication from policyholders regarding patients and other providers.

HIPAA and state laws protect patient privacy and require dentists to take precautions to ensure that a patient's private health information is not compromised. Such precautions include:

- Making sure to use reasonable safeguards such as limiting the amount of information sent via email, checking the email address for accuracy before sending and sending an initial email to the patient to confirm the address before transmitting dental records or treatment information.
- Sending email securely, which can be achieved a number of ways, including encryption, secure file transfer software or proprietary information sharing websites.
- Informing the patient that unsecured emails have risks and securing patient authorization in writing before sending email that are not encrypted.
- Training staff on proper email use to meet security standards.
- Performing a written risk assessment to reveal where a practice's protected health information could be at risk. Include email procedures in the assessment.

"When it comes to email security, the focus tends to be on encryption, and whether it is required," said Teresa Pichay, a regulatory policy analyst with the California Dental Association. "HIPAA requires electronic communication of patient information to be secure, and encryption is just one way of doing that. However, it is not specifically required that email be encrypted." Pichay said other security measures such as virtual private networks (VPNs) that are password protected and other "reasonable safeguards" are acceptable for email communications.

According to the U.S. Department of Health and Human Services website, the HIPAA Privacy Rule does not prohibit the use of unencrypted email for treatment-related communications between providers and patients, but states, "Other safeguards should be applied to reasonably protect privacy, such as limiting the amount or type of information disclosed through the unencrypted email."

"Limiting the amount of information is a key point," Pichay said. "Send only the minimum necessary information in email."

Pichay emphasized that dentists must not send information to a patient through unencrypted email unless the patient is advised about the risks associated with unsecured email. Such risks include possible disclosure or interception of "identifiable health information" by unauthorized third parties. Dentists must receive patient consent to receive unencrypted email and retain documentation with the patient record. An authorization form for patient consent to receive unencrypted email must be a standalone document, according to the American Dental Association, which provides a sample form on its website at ada.org.

However, if the use of unencrypted email is unacceptable to a patient who requests confidential communication, other ways of sending dental information, such as by regular mail, should be offered. Also, patient consent to receive unencrypted email is not consent to send patient health information in nonsecured emails with other parties such as specialists and payers. As mentioned previously, electronic communication can be sent securely a number of ways including encryption, secure file transfer software or proprietary information sharing websites.

In addition to HIPAA, state laws also apply to patient privacy. In California, AB 211, passed in 2008, imposes penalties upon individuals and institutions that fail to protect the privacy of patient medical records. The law called for the creation of the enforcement agency known as the Office of Health Information Integrity (CalOHII). Penalties imposed by AB 211 vary depending upon the circumstances of the violation, but can reach a maximum of $250,000 if the patient suffers economic loss or personal injury. Additionally, CalOHII may notify the Dental Board of California for further investigation or discipline of individual providers. Laws vary by state and further information is available on state Department of Health websites.

If a dental practice is scrutinized by a regulatory agency, a risk assessment and policies and procedures pertaining to electronic security can help a dental practice demonstrate compliance with HIPAA. Include email communication as part of a dental practice's risk assessment that takes into account all of the office's electronic patient information including electronic dental records and digital radiographs. HHS recently released a security risk assessment tool to assist with HIPAA compliance for all states. The application is available for download at HealthIT.gov/security-risk-assessment and produces a report that can be provided to auditors.

Dentists must also train their office staff on proper email use. For example, consider giving the patient a heads-up phone call letting him or her know an email is on its way prior to sending protected health information, or communicating a decryption password or code separately from the encrypted email

TDIC's Risk Management Advice Line can be reached at 800.733.0634.