Dentist's Advantage
PROFESSIONAL LIABILITY & PRACTICE PROTECTION

The National Society of Dental Practitioners and the Dentist's Advantage Insurance Program for Dentists

RISK MANAGEMENT ARTICLE

Managing Electronic Communication with Patients

Electronic communication via email, fax, or telephone can be an effective strategy for both you and your patients by promoting more timely and efficient communication. For example, patients have more time to craft questions before sending them by email so their questions may be clearer and more succinct. You can quickly answer simple questions by phone and send email reminders to patients to discourage missed appointments.

However, it is easy to fall into the trap of not treating electronic communication with the same care as print communication. Failure to do so can result in legal action against dentists who, for instance, fail to follow privacy regulations, leading to disclosure of protected health information to an unauthorized person. By taking a few precautions, you can enjoy the benefits of electronic communication while minimizing the risk of litigation.

Privacy protection

The HIPAA Privacy Rule (modifications to the rule effective 2002) and Security Rule (effective 2003) guide how protected health information is handled. The **Privacy Rule** applies to health information in any form (electronic, oral, or written) and permits communication electronically such as through email as long as "reasonable safeguards" are taken to protect privacy.

The **Security Rule** covers electronic protected health information that is created, received, maintained, or transmitted (for example, information transmitted via the Internet). The Security Rule requires safeguards to protect confidentiality (so information is not disclosed to unauthorized persons), integrity (data is not changed without authorization and there is a record of any change), and availability (data are accessible to authorized persons) of electronic patient information that covered entities create receive, maintain, or transmit.

The 2013 HIPAA Privacy and Security Omnibus Rule strengthens these rules and, most importantly, extends most of them to dental practices' business associates (e.g., a billing service) and their contractors. This means that you should ensure that your business partners are also taking care to follow regulations related to protected health information. Interestingly, patients now have the right to request health information be sent by unencrypted email; the covered entity should first advise the patient of the risk of privacy violation.

Criminal penalties from mishandling protected information can be as high as $1.5 million annually for all violations of an identical provision. To avoid penalties, conduct a security risk assessment to help identify potential security risks (see *Assessing risk*).

Communicating information

One of the primary means of communicating patient information is through the patient's health record. When choosing a software program, make sure it has security safeguards in place and includes a feature that ensures records cannot be altered. In addition, regular backup is essential.

When releasing electronic information to other covered entities such as billing services, include only the information that is essential for the entity to complete the service.

Of course you should not indiscriminately share information, but when seeking consultation, it is important to provide enough information. Take note that according to HIPAA, you can share protected health information

with other providers for treatment purposes as long as "reasonable safeguards" are taken, such as verifying a new fax number before sending a transmission.

According to HIPAA, patients who initiate email conversations are, unless otherwise stated, giving providers permission to correspond with them through email. However, it is wise for you to ensure that patients understand potential risks such as the possibility for emails to be hacked or forwarded to someone else.

Mobile devices
You should take special care when protected health information is accessible through mobile devices. HealthIT.gov recommends that if a practice decides to use mobile devices, clinicians should follow these precautions:
- Use a password or other user authentication
- Install and enable encryption
- Install and activate remote wiping and/or remote disabling
- Disable and do not install or use file-sharing applications
- Install and enable a firewall
- Install and enable security software
- Keep your security software up to date
- Research mobile apps before downloading
- Maintain physical control
- Use adequate security to send or receive health information over public Wi-Fi networks
- Delete all stored health information before discarding or reusing the mobile device

You should have a policy that outlines the appropriate use of mobile devices. Teach staff about the policies and document that staff received the information. HealthIT.gov provides a variety of resources such as posters to encourage staff to appropriately use mobile devices. You can access these resources at www.healthit.gov/providers-professionals/downloadable-materials.

If a breach occurs
Despite safeguards, disclosure of protected health information may inadvertently occur. The Breach Notification Rule of the 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act, as well as the Omnibus act, provide guidance on how to respond if a breach occurs. Dentists are required to notify affected patients, the secretary of Health and Human Service, and, if the event affects 500 or more individuals, the media of the breach.

The Omnibus act extended breach notification responsibilities to business associates; they are also required to notify the covered entity, such as a dentist, when a breach occurs.

Shielding from litigation
Ensure that your staff members receive education regarding electronic communication and protected health information (see *Strategies for appropriate electronic communications*), conduct regular risk assessments, and follow state and federal rules and regulations. You should also consult your professional liability insurer to determine if you have adequate protection for risks related to electronic communication. These simple steps will help shield you from litigation.

RISK MANAGEMENT ARTICLE

Assessing risk

The HIPAA Security Rule requires covered entities such as dentists to conduct periodic security risk assessment (SRA) and develop safeguards to protect electronic patient information. Safeguards are divided into three categories:

• **Administrative:** Administrative functions to meet security standards such as assignment of responsibility to a specific person and training requirements.

• **Technical:** Automated processes used to protect data and control access to data such as authentication control for access.

• **Physical:** Means to protect electronic systems and the data they hold from environmental hazards and unauthorized intrusion. This includes restricting access and using off-site computer backup.

You can download a print version of the SRA Tool, a Windows application, or an iPad version, as well as a guide on how to use the tool, at www.healthit.gov/providers-professionals/security-risk-assessment-tool. The SRA Tool takes the user through each HIPAA requirement by presenting a question about the organization's activities. The user's "yes" or "no" answer will show where corrective action is needed for that particular item.

At 156 questions, the SRA tool requires a considerable time investment. This might be something you can delegate to the office coordinator. Risk assessment should also be repeated on a regular basis.

Source: Security 101 for covered entities. *HIPAA Security Series.* 2007;2(1):1-11.

Strategies for appropriate electronic communications

Use these suggestions to ensure electronic communication remains safe and secure.

• Ask patients to sign a release form (consult with an attorney first) that acknowledges potential problems with electronic communication.

• Change passwords at least quarterly and avoid simplistic passwords. HealthIT.gov states that passwords "should be at least six characters in length, and should include a combination of upper and lower case letters, at least one number and at least one keyboard character, such as a punctuation mark."

• Keep fax machines in a secure location, verify a fax number before starting a transmission, and use a cover sheet with nonprotected health information. Make telephone calls to patients in private.

• Take special care with mobile devices and encourage patients to do the same.

Resources

American Dental Association. Dental records. 2010.
American Dental Association. Principles of Ethics and Code of Professional Conduct. 2012.
American Dental Association. HIPAA Privacy and Security. http://www.ada.org/en/member-center/member-benefits/practice-resources/dental-informatics/electronic-healthrecords/health-system-reform-resources/hipaa-privacy-security.
Department of Health and Human Services. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; other modifications to the HIPAA rules. Federal Register. 45 CFR Parts 160 and 164. January 25, 2013, Vol. 78, No. 17.
HealthIT.gov. Security risk assessment tool. n.d. http://www.healthit.gov/providers-professionals/security-risk-assessment-tool.
HealthIT.gov. Your mobile device and health information privacy and security. n.d. http://www.healthit.gov/providers-professionals/your-mobile-device-and-health-informationprivacy-and-security.
HIPAA. Frequently asked questions: Does the HIPAA Privacy Rule permit health care providers to use e-mail to discuss health issues and treatment with their patients? 2008. Can a physician's office FAX patient medical information to another physician's office? 2006. Does the HIPAA Privacy Rule permit a doctor, laboratory, or other health care provider to share patient health information for treatment purposes by fax, e-mail, or over the phone? 2005. http://www.hhs.gov/ocr/privacy/hipaa/faq/health_information_technology/570.html.

Dentist's Advantage
PROFESSIONAL LIABILITY & PRACTICE PROTECTION

The National Society of Dental Practitioners and the Dentist's Advantage Insurance Program for Dentists

RISK MANAGEMENT ARTICLE

Kaweckyj N, Frye W, Hilling L, Lovering L, Schmitt L, Leeuw W. The business of dentistry: Patient records and records management. November 21, 2011. http://www.dentalcare.com/media/en-US/education/ce390/ce390.pdf.

Article reviewed by Dr. Kenneth W.M. Judy, DDS, FACD, FICD, PhD

Article by: Cynthia Saver, MS, RN, President, CLS Development, Columbia, Maryland