GDA
ACTION
THE JOURNAL OF THE GEORGIA DENTAL ASSOCIATION OCTOBER 2010

"It's Time"

GDA

Since 1859

Sourcebook and Directory
2010 - 2011

Handling Confusion Regarding Electronic Health Records and HIPAA-Governed Breach of Patient Information

Laney Kay, JD

Here's the good news. After all the propaganda and the worry, we've all seen that HIPAA is really not such a big deal for dentistry. For the most part, common sense policies and procedures are enough to keep our patients' information safe in our offices. However, in the past several months, two HIPAA-related concerns have arisen that need to be addressed. The first is whether or not dentists are among those health care providers who are required to convert to electronic records by 2012. The second concern deals with the new HITECH Breach Notification Rules for Unsecured Protected Health Information.

Are Dentists Required to Convert to Electronic Records?

The answer to the electronic records conversion question is no. There are no federal requirements for dentists to be paperless.

The paperless requirements for records generally do not apply to dentistry. The rules require that those health care practices that deal with Medicare and Medicaid, especially in a hospital setting, convert to paperless records by 2012. There are federal funds available to help affected health care professionals to purchase and implement compliant computer systems and programs, so long as they comply with very strict implementation schedules and standards.

There are very few dental practices that may be affected by these rules. Since the rules are generally geared toward medical offices, there aren't really any computer programs that are dental specific, which would make compliance under the rules very difficult and extremely expensive. However, if you care for a substantial number of Medicaid patients, especially if you provide hospital dental services, it is a good idea to contact your state Medicaid office and make sure there are no specific requirements that you need to follow.

Meeting the HITECH Breach Notification Rule Requirements

There are times when following the HIPAA rules still can't adequately protect our patients' information. Accidental disclosures can happen despite our best intentions. That's where these new rules come in. They detail what procedures must be followed in the event a patient's unsecured information is "acquired, accessed, used or disclosed in an unauthorized way." So, if a patient's bill is accidently sent to another patient, or someone hacks into your computer system, or if one of your office laptops is stolen, these rules tell us what we need to do to minimize any damage done by a breach of information.

If a dentist suspects their patients' information has been compromised, the dentist must perform a "risk analysis" to determine if a breach has actually occurred, and if so, what steps to follow. If a dentist determines that a breach actually has occurred, then interested parties have to be notified or, if no damage has occurred as a result of the breach, the breach still has to be documented.

There are two types of information: secured and unsecured. If information is "secured," that means that it has "been rendered unusable, unreadable, or indecipherable to unauthorized individuals." This can be accomplished by using various forms of encryption for your computer information, or by properly disposing of backup discs and wiping hard drives, and by shredding any papers or x-rays to meet the above definition before disposal.

If secured information is accessed no breach has occurred, because the information isn't usable. So, if someone hacks into your office computer but the information is encrypted, then a breach has not occurred. Or, if someone steals a bag of trash that is full of patient records, but they are all appropriately shredded, no breach has occurred.

"The answer to the electronic records conversion question is no. There are no federal requirements for dentists to be paperless. The paperless requirements for records generally do not apply to dentistry. The rules require that those health care practices that deal with Medicare and Medicaid, especially in a hospital setting, convert to paperless records by 2012."

HIPAA
Continued on page 14

"If a dentist suspects their patients' information has been compromised, the dentist must perform a 'risk analysis' to determine if a breach has actually occurred, and if so, what steps to follow. If a dentist determines that a breach actually has occurred, then interested parties have to be notified or, if no damage has occurred as a result of the breach, the breach still has to be documented."

HIPAA

Continued from page 13

The next thing to consider is whether the breach caused a "significant risk of harm." If the breach exposes the patient to harm, if it could damage the patient's reputation, or if it could harm the patient financially, then actions must be taken to mitigate the harm. For example, if a bill with credit card information is accidently sent to the wrong patient and the wrong patient opens the bill and views another patient's information, a breach has occurred and the original patient must be notified. This notification must take place as soon as possible but absolutely within 60 days and inform the patient that his or her information could have been compromised. This allows the patient the opportunity to cancel the credit card and / or monitor his or her credit information to make sure financial information isn't used improperly.

In the situation above, if the information was retrieved before the wrong patient received the information, or the envelope was returned to the office unopened, then a breach would not have occurred.

These are considered to be exceptions to the breach notification rule. Another exception would be if information is unintentionally disclosed to the wrong person within the same office which results in no harm. For example, if an office has several facilities and an employee sends a patient's financial information to the wrong facility for insurance processing, that's not a breach so long as the individual who receives it is generally allowed to access health information. These exceptions would not require patient notification because no harm resulted, but documentation of the breach would be necessary.

The required documentation is a log of any breaches. These logs must be maintained for a period of at least six years. Here's how it works:

- If a breach occurs during the year, the breach must be documented and then the log must be submitted to the Department of Health and Human Services within 60 days of the end of that calendar year.
- The log must include the date the breach occurred and the date the breach was discovered, a description of the type of information that was disclosed (financial information, medical history, etc.), the number of patients involved,

how and when the patients were notified, and any actions that were taken to prevent further problems.

If a breach occurs and it involves fewer than 500 individuals, you must notify affected patients by first-class mail "without unreasonable delay … but in no event later than 60 calendar days after the date" and then document the breach on your breach log. If you believe that patients would benefit by being notified immediately, you may want to call each affected patient as well as sending a notification in the mail.

If a breach occurs, and it involves 500 or more individuals from the same geographical area, the Department of Health and Human Services must be notified as soon as possible, and definitely no later than 60 days after the breach is discovered. Also, all patients must be notified by first-class mail as soon as possible and a press release must be given to a "prominent media outlet." If there are fewer than 10 patients that are unreachable because their address isn't correct, these individuals can be contacted by phone or e-mail, and / or notice can be posted on the practice's web site. If there are more than 10 unreachable patients, the office must provide a toll-free number for 90 days so that patients can call to ask questions. The practice must also post the breach notice on the office web site, or provide a conspicuous posting in a "major print or broadcast media in geographic areas where the individuals affected by the breach likely reside."

When a HITECH Breach is Caused by a Business Associate

What if it turns out the breach isn't caused by your office, but by one of your business associates? Who is responsible for notifying patients? Is there anything else you need to do with your existing business associates to make sure they are also in compliance with the new breach notification rules? Who is ultimately responsible for making sure the breach notifications are handled properly?

Ultimately, you are responsible for your patients' information. If you choose a business associate, it is your duty to ensure that your business associates agree to handle your patients' information carefully and responsibly. In the event of a breach, you may be the one who reports it to your patients, you will have to document the breach, and you will have to report the breach, if necessary, to the U.S. Department of Health and Human Services. It is your responsibility to make sure that your business associates understand the procedures they must follow in the event of a breach and agree to respond in a timely fashion.

Review your existing business associate agreements to make sure that there is a section dealing with potential breaches and how they should be handled. Make sure that there is a time limit for notification so that patients can be notified within the required timeframes. Make sure there is specific language about who is responsible for actual notification, and who is responsible for notifying the media, if necessary. For example, if there is a breach by an accountant, attorney, software company, or other third-party vendor you use, it may be difficult to determine which patients are affected. Your agreement may specify that you would notify all patients who could be affected, while the business associate would notify the media on behalf of all the dentists who use that third-party vendor.

You may also choose to include a section on indemnification so that you could recoup costs in the event of a breach by a business associate.

Conclusion: Don't Violate HIPAA

Obviously, the best way to handle HIPAA breaches is to avoid them completely. Handling patients' information carefully and conscientiously will prevent most problems from occurring. When it doesn't, following the rules will help lessen your liability and reduce the potential for injury to your patients.

Author Laney Kay, JD, has been writing and speaking on technical and regulatory topics and women's issues since 1989. Her expertise is in taking complex, and / or boring topics and making them fun and informative. She has written numerous articles for state and national journals and has lectured at many dozens of national, state, and local dental meetings. Visit www.laneykay.com for additional information.

"Ultimately, you are responsible for your patients' information. If you choose a business associate, it is your duty to ensure that your business associates agree to handle your patients' information carefully and responsibly. In the event of a breach, you may be the one who reports it to your patients, you will have to document the breach, and you will have to report the breach … It is your responsibility to make sure that your business associates understand the procedures they must follow in the event of a breach and agree to respond in a timely fashion."