Dental Practice **Insights**

Appointment Reminders: Get Cell Phone Consent

Leaving an appointment reminder on a home phone is not always effective these days, because many people no longer check their home phone voicemail regularly or simply don't have a home phone and rely exclusively on cell phone communication. But before you switch to communicating with patients on their cell phones, you must obtain written consent from them.

The MDS urges members to revise your patient intake form to include consent content. Not sure how to word it? Here's some sample text:

Cell Phone Use Policy: (1) I provide consent to the _____ dental practice to use my cell phone number to (choose one or both) call or text regarding appointments. (2) I consent to the _____ dental practice to call me using my cell phone regarding treatment, insurance, and my account. I understand that I can withdraw my consent at any time. My cell phone number is __( ) _____ - _____.
_____(initial)

Practice Management Q&A

Question:

Does My Office Really Need to Prepare for a Random Inspection?

Answer:

Yes. The Massachusetts Board of Registration in Dentistry (BORID) or its designee(s) may visit a dental practice at any time without prior notice and conduct an inspection to determine compliance with state law M.G.L. c. 112, §§ 43 through 53 and § 61 and 234 CMR 2.00 or both, or any state or federal statutes or regulations relating to the practice of dentistry and dental hygiene. The MDS recommends that you conduct a mock audit in your office to be sure your office is in full compliance utilizing the same compliance form that BORID would use. Visit massdental.org/checklists and click "BORID inspection form" to see the actual form BORID uses.

Speaking of random inspections, beginning July 1, 2016, BORID and the Division of Health Professions Licensure Office of Public Protection (DHPL) will begin random continuing education (CE) audits of all licensed dentists. Be sure that your CE documentation is up-to-date and available. A dentist licensed in the Commonwealth must complete a minimum of 40 CEUs per renewal cycle; these must include courses in CPR, infection control for the dental office, and pain management.

BORID and the DHPL have also begun to schedule inspections of dental offices that hold current Permit D-B1 or Permit D-B2 for the administration of moderate sedation and/or minimal sedation. If you received an inspection request, it's important that you respond to determine a mutually agreeable time for inspection.

Protecting Patient Data

Dental practices are becoming the targets of cyber attacks more and more frequently. Why? Your office has a plethora of data that cyber criminals are looking to get their hands on, including patient names, social security numbers, health histories, birthdays, addresses, and in some cases, financial information (e.g., banking and credit card information). According to the U.S. Department of Health and Human Services, nearly 21 million health records have been compromised since September 2009. The Health Insurance Portability and Accountability Act (HIPAA) requires health care providers, including dentists, to maintain the privacy of patient health information and to take security measures to protect this information from abuse by hackers, thieves, and disreputable staff members.

Dentists should put safeguards in place in your offices to protect patient information and ensure that all of your staff members understand the importance of maintaining the privacy of patient information. You also need to have procedures in place to protect your computer data. In fact, HIPAA requires you to have a written security policy in place to protect the integrity of your patient information.

To help members meet this requirement, the MDS recommends the following tips to include in your practice's security policy and implement in your office:

1. Position computer screens so that they are not visible to patients and visitors.
2. Instruct staff never to open an email from an unknown sender. If an email is accidentally opened from an unsolicited email, do not click on any links or attachments.
3. Protect each computer with a different password, which should contain a mix of case-sensitive letters, numbers, and symbols. Passwords should be changed regularly and especially with staff turnovers.
4. Avoid writing passwords down on notepaper and placing them under keyboards or keeping them on desks or surfaces where they could be accessed.
5. Do not allow staff to access personal emails at work or surf on the Internet for non-work-related information.
6. Use only trusted wi-fi hot spots and never use shared computers when accessing office data remotely.
7. Install anti-virus software on every computer, and keep it updated and checked regularly.
8. Use encrypted email to communicate with patients and other health care providers and payers.

The penalties imposed on health care providers for HIPAA violations are great. Monetary penalties can range from a $100 fine to a $50,000 fine per violation, with a $1.5 million maximum annual penalty. In addition to federal penalties, dentists may face penalties imposed at the state level, as well as lawsuits filed by disgruntled patients whose health information has been compromised.