C. Scott Litch
Chief Operating Officer and General Counsel

Litch's Law Log

Legal Guidance for Phoning and Texting Parents/ Guardians Plus Sending PHI Via E-mail

As highlighted in the September 16, 2015 issue of AAPD *E-news*, the ADA has released excellent legal guidance related to the very common dental practice action of phoning or texting patients (or in the case of pediatric dentistry, parents/guardians). Unfortunately there is increased legal risk under the Telephone Consumer Protection Act, and dental practices have been sued for violating this law. A dental practice should be aware of the rules, the small carve-out or "safe harbor" under HIPAA, and how to obtain appropriate written consent to send phone or text communications. **The ADA guidance includes a sample consent form.**

Key tips are to:

- Call or text only with health care and collection messages, not marketing or advertising messages.
- Ask parents/guardians to sign a consent form before making a phone call or sending a text.
- Frequently ask for updates from parents/guardians, since cell phone numbers change frequently. Calling the old number more than once can violate the law.
- Stop calling or texting the number immediately if consent is revoked.

If your practice makes calls or sends texts that are marketing or advertising, either directly or through a firm, you must be compliant with the Federal Trade Commission's Telemarketing Sales Rule (TSR). This rule established the national Do-Not-Call Registry to prevent unwanted telemarketing calls. While there are exceptions for an "established business relationship", it does not automatically mean the same thing as being a "patient of record." See more information at *https://www.ftc.gov/tips-advice/business-center/advertising-and-marketing/telemarketing.*

If the dental practice is covered by HIPAA[1], you generally do not need prior written consent before sending a "health care" message to a patient or parent, even if you send automated calls or texts. However, you should limit the message content to health care treatment purposes (such as scheduling), include the name and contact information of the dental practice, stay concise (under one minute for a voice message), and send no more than one message a day and no more than three per week.

Note that ADA membership log-in is required to view the full guidance, available at http://success.ada.org/en/practice/operations/regulatory/follow-the-rules-when-phoning-patients.

HIPAA also comes into play when transmitting protected health information (PHI)[2] via e-mail, for reasons others than electronically submitting a health care transaction (such as to an insurer).

The PHI disclosed should be limited only to that information reasonably necessary to accomplish the purpose of the disclosure. In many cases it may be a better idea to simply convey the information via phone call versus an e-mail message. HIPAA does not require encryption of e-mails containing PHI in all circumstances. However, if you are communicating with a parent/guardian with an unencrypted e-mail, you can protect against legal liability by notifying the parent/guardian of the risks of third party disclosure. If they still prefer to receive PHI via an unencrypted e-mail, they have that right. Disposal of e-mails containing PHI, both in electronic form and those printed out, is also required.

Last but not least, here is a disclaimer that this column is presenting a general informational overview of legal issues rather than providing legal advice. Reading the column is not a substitute for consulting with your own attorney concerning specific circumstances in your dental practice.

For further information contact Chief Operating Officer and General Counsel C. Scott Litch at 312-337-2169 ext. 29 or *slitch@aapd.org*.

[1] *Every health care provider, regardless of size, who electronically transmits health information in connection with certain transactions, is a covered entity under HIPAA, the Health Insurance Portability and Accountability Act.*

[2] *HIPAA protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. This is called "protected health information (PHI)." "Individually identifiable health information" is information, including demographic data, that relates to: the individual's past, present or future physical or mental health or condition, the provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number). Source: http://www.hhs.gov/sites/default/files/privacysummary.pdf*