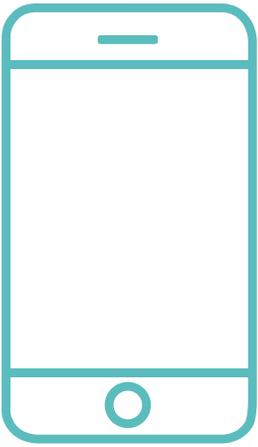


5 TIPS TO HELP LOWER MEDICAL TEXTING RISK

Texting enables physicians to quickly communicate important patient health information. However, texting protected health information can lead to significant healthcare privacy law (HIPAA and HITECH) concerns. In this report, NORCAL's Risk Management experts discuss the pros and cons of physician use of texting, and provide five helpful tips to reduce the risk of inadvertently exposing patients' private information when texting.



THE GOOD

In a recent study,¹ 11% of physicians said their organization offers a secure texting solution. Though not a large number, this statistic is an encouraging sign that practices recognize more physicians are using texting as a method of communication and are working toward creating

solutions to protect the electronic protected health information. Texting facilitates and speeds patient interventions when it:

- » Puts clinical information into physicians' hands more quickly.
- » Provides an easy way to share images and recordings.
- » Shortens response times among physicians².

THE BAD

At its simplest, HIPAA requires physicians to protect the privacy and security of their patients' healthcare information. 53% of physicians said they text with colleagues about work-related matters while not on duty. This means that security needs to apply to all texting about patients, no matter the setting. Between 2009 and 2015, 141 out of 1,148 protected healthcare information breaches involved a portable electronic device.³ Thus, improper releases of patients' information from portable devices already represents 12% of all privacy breaches, and this number will likely only grow as physicians become more accustomed to relying on smartphones to communicate.

- » Texting is inherently unsecure and therefore can jeopardize patient privacy and result in federal healthcare privacy laws (HIPAA and HITECH) violations.
- » Physician texting can also leave gaps in the medical record, as the content of text messages usually isn't entered into a patient's chart. The gaps can complicate the defense of a medical malpractice claim.⁴
- » Texting is done quickly, which can result in unsuitable abbreviations, typos and superficial exchanges.

CASE EXAMPLES

Patient Information Inadvertently Revealed⁵:

A physician received a text about his patient while he was at a restaurant having dinner with a friend. He glanced at the text and then put the phone face up on the table. His friend couldn't help but read the text.

Patient Information Accessed on a Lost Phone:

A physician left her phone in the back seat of a cab. The cab driver, in an attempt to find the phone's owner, inadvertently accessed text messages that contained electronic public health information (ePHI).

Patient Information Sent in a Text Message to the Wrong Person:

A specialist used an out-of-date phone number to text a deceased patient's family physician to let him know the patient had died: "FYI. Mr. Johnston in room 902 died at 0630 today." About two minutes later the specialist got a call back from the current owner of the phone number. The caller told the specialist that he didn't know Mr. Johnston and that he wasn't a doctor. The specialist did not know the family physician had changed his telephone number.

5 TIPS TO HELP LOWER MEDICAL TEXTING RISK

The following risk management tips may help physicians who wish to protect patients' confidentiality while adopting texting as a practice communication tool.

01 Do not electronically transmit highly sensitive ePHI (e.g., information about mental health, HIV, substance abuse or minors).

.....

02 Install password protection, encryption, auto-lock and remote wiping programs to prevent data breaches.

.....

03 Double check your recipient and review content of texts before sending for misleading abbreviations and autocorrect.

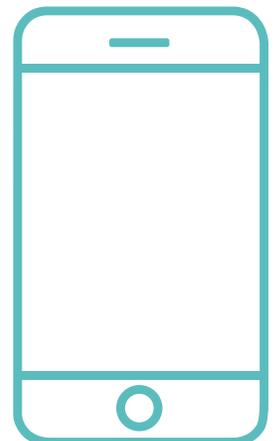
.....

04 Assume any individual nearby can view texts.

.....

05 Ensure that you have cyber-liability insurance coverage for potential exposures.

The risk of violating healthcare privacy laws (HIPAA and HITECH) through texting is a serious concern for all healthcare providers and entities. Every effort should be made to comply with these laws. Setting up a texting protocol may require guidance by business and/or legal advisors, as well as risk management experts.



This report is presented as a courtesy by NORCAL Insurance Company. Our Risk Management Specialists are always ready to help policyholders with risk issues and to support practice changes that lower risk and improve patient safety.

ABOUT NORCAL GROUP

NORCAL Group, now part of ProAssurance, offers a full spectrum of medical professional liability insurance solutions to physicians and other healthcare providers. NORCAL Group includes NORCAL Insurance Company and its affiliated insurance companies. Please visit norcal-group.com/companies for more information.



844.466.7225 norcal-group.com

REFERENCES

1. Gregg, H. (2014, May 13). 10 Statistics on Physicians' At-Work Texting Habits. Available at: <http://www.beckershospitalreview.com/healthcare-information-technology/10-statistics-on-physicians-at-work-texting-habits.html> (accessed 3/2/2015).
2. Ventola CL. Mobile devices and apps for health professionals: uses and benefits. *Pharmacy and Therapeutics*. 2014; 39(5):356-364. Available at: www.ncbi.nlm.nih.gov/pmc/articles/PMC4029126/ (accessed 2/18/2015).
3. Information derived from U.S. Health and Human Services Office of Civil Rights Breach Portal. Breaches Affecting 500 or More Individuals. Report available at: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (accessed 3/2/2015).
4. Greene, AH. HIPAA compliance for clinician texting. *Journal of AHIMA*. 2012; 83(4): 34-36. Available at: http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_049460.hcsp?dDocName=bok1_049460 (accessed 3/24/15).
5. Harris S. Physician texting could violate HIPAA. *The Rheumatologist*. Available at: http://www.the-rheumatologist.org/details/article/2464481/Physician_Texting_Could_Violate_HIPAA.html (accessed 2/18/2015).