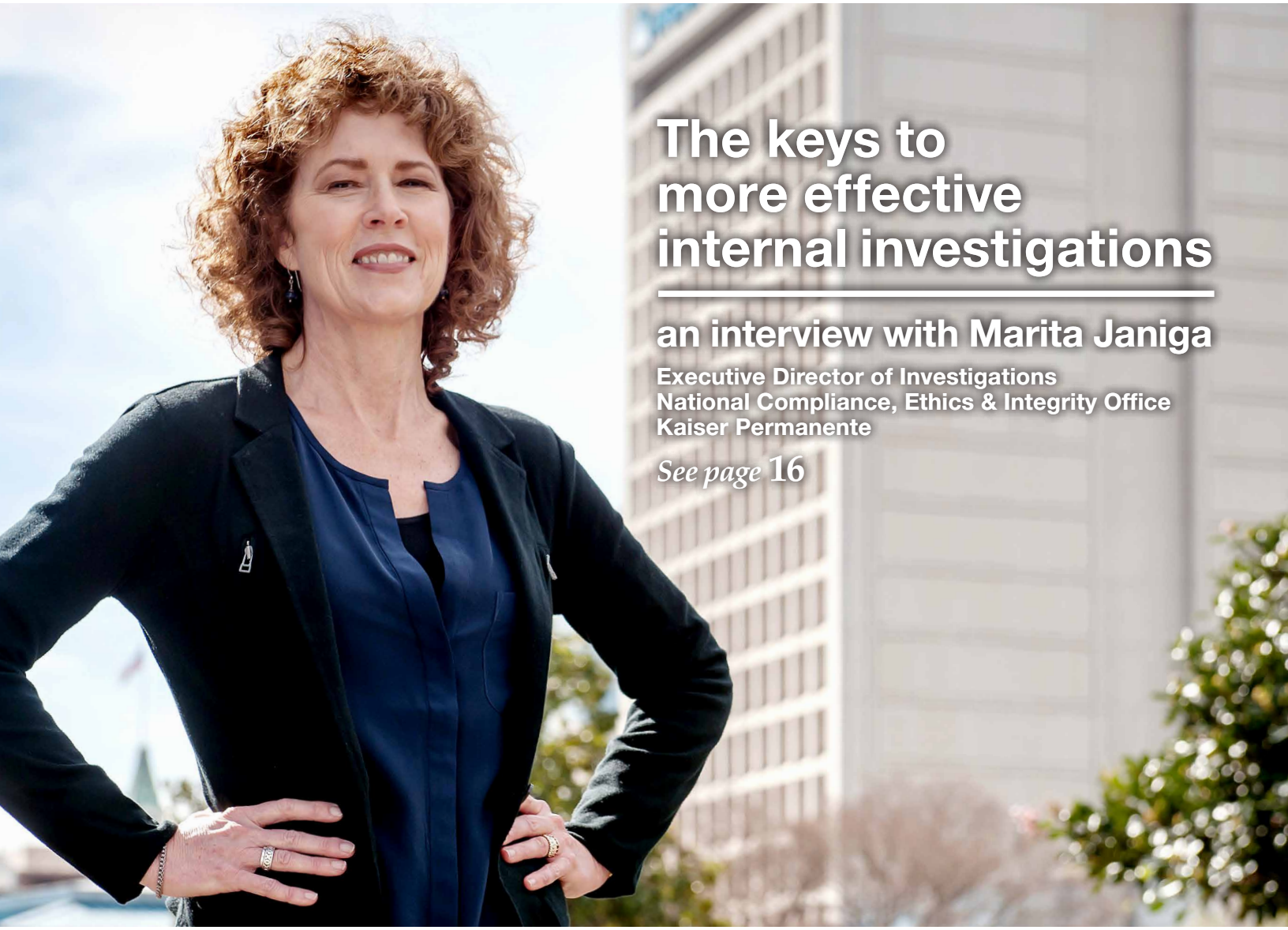
HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

Compliance TODAY

April 2016

A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

WWW.HCCA-INFO.ORG



The keys to more effective internal investigations

an interview with Marita Janiga

Executive Director of Investigations
National Compliance, Ethics & Integrity Office
Kaiser Permanente

See page 16

by Joan Feldman, Esq. and William Roberts, Esq.

Communicating protected health information via text messaging

» Many individuals depend on text messaging to communicate with clinicians.
» Text messaging can improve communication and patient outcomes.
» Providers must assess risk before sending PHI via text message.
» Risks exist with using text messaging in the clinical setting.
» Providers can mitigate risk when text messaging with patients.

Joan Feldman *(jfeldman@goodwin.com) is Partner and Chair of Health Law Practice Group and* ***William Roberts*** *(wroberts@goodwin.com) is Chair of Privacy and Data Protection Group with Shipman & Goodwin LLP in Hartford, CT.*
bit.ly/in-JoanFeldman *bit.ly/in-WilliamRoberts* *@BillRoberts01*

There is no doubt that we are now fully immersed in a world where communications are rapid fire and electronic. Approximately three-quarters of the U.S. population own phones that can receive text messages. Some 83% of American adults own cell phones and three-quarters of them (73%) send and receive text messages. The Pew Research Center's Internet & American Life Project asked those texters in a survey how they prefer to be contacted on their cell phone: 31% said they preferred texts to talking on the phone and 53% said they preferred a voice call to a text message. Another 14% said the contact method they prefer depends on the situation.[1]

In fact, many individuals have abandoned their landlines and rely exclusively on mobile or cellular phone technology. For obvious reasons, communicating with patients at their place of employment is not always possible or welcomed by either the patient or their employer, and mail service is only fine if you have a few days to communicate your message. Although some patients prefer to receive information from their provider via voicemail, many patients prefer to receive healthcare-related information via text messaging as a means to having reciprocal communication in real time.


Feldman


Roberts

According to the United States Department of Health and Human Services, there is a "substantial body" of evidence that demonstrates that text messaging can improve clinical outcomes, improve patient compliance (including medication and appointment reminders), and reduce risky behavior.[2] As a result, more and more providers are eager to embrace text messaging as a means of communicating directly with their patients. Texting may be an extremely effective way to communicate with a patient, but if you are a healthcare provider or acting on behalf of a healthcare provider, communicating with a patient by text is not always advisable, because there are potential privacy and security risks associated with communication via text messaging.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations require healthcare providers to implement reasonable safeguards to protect the privacy and security of patient health information, regardless of the information's form or format. This obligation under HIPAA extends to patient information contained in text messages sent or received by the healthcare provider. Therefore, providers who use text messaging must conduct a risk analysis to determine where the electronic protected health information (ePHI) it is texting is primarily created, received, and maintained on mobile phones (text messages may also reside on workstations or cloud-computing servers or be embedded into patient medical records).

Upon identifying text messages as a location of ePHI, HIPAA directs a healthcare provider to identify reasonably anticipated threats to such ePHI and evaluate the likelihood and potential impact of such threats. Examples of such threats in the context of text messaging include:

- Access of ePHI by an unauthorized or unintended recipient (e.g., text message sent to incorrect patient or third party)
- Theft or loss of the mobile device
- Improper disposal of the device
- Interception of transmission of PHI by an unauthorized person (i.e., hacking).

Recent statistics included in the Department of Health and Human Services' reports to Congress on HIPAA breaches show that misdirecting the transmission of ePHI or the loss or theft of mobile devices are among the most common incidents leading to a HIPAA breach, along with a growing prevalence of hacking and interception of transmission as causes of breaches.

Although the federal privacy rules neither explicitly prohibit text messaging as a means of communicating with patients, nor prescribe how it can be done to remain compliant, there is an overriding expectation under the law that such communications should be sent in a secure and private manner. Even though technology is currently available in the marketplace that allows a more secure format for communicating via text messaging, not all providers, especially providers with limited resources, can afford the current technology. Moreover, even with the secure platform technology, privacy and security risks remain, as they do with all forms of patient communication.

Given the value of real-time text messaging with patients, with or without the security technology, we do not recommend that providers forego communicating via text messaging. However, if text messaging will be used as a form of communication with patients, we do offer the following recommendations and/or guidelines with respect to reducing your privacy and security risks:

- Develop a written policy so staff are aware of who can communicate with patients via text messaging, the indications for text messaging, and the content that is appropriate to communicate via text messaging;
- Contemporaneously record in the patient's medical record the information that was texted to the patient. Specifically, the date, time, content, and person who text messaged the patient should be documented. It is our understanding that cellular carriers do not maintain the text messaging data as long as the retention periods most healthcare providers are required to comply with; therefore, documentation of the text messaging content in the medical record is essential for risk management, auditing, and reimbursement purposes;
- Obtain the patient's written consent prior to communicating through text messaging to confirm that they are willing to receive information via text messaging. Have the written authorization specify the type

of information that the patient is willing to receive by text message. For example, appointment reminders, messages to call the provider, and other content specific information;
- Require that all texting be done on password-protected mobile devices, both on the sending and receiving end;
- Send a confirmatory text message to make sure that the patient is able to receive the text message. To be sure that it is the patient who is texting back, you have the option of asking the patient to text back an agreed upon code;
- Do not send any ePHI that is highly sensitive (e.g., HIV-related confidential information, drug and alcohol information, psychiatric information) through a cellular phone that does not have the secure text messaging platform discussed above. We are also of the opinion that laboratory results and pathology and radiology reports or results should not be sent via text;
- Make sure that before phones are retired, all PHI is deleted;
- Consider requiring mobile devices used for text messaging to be equipped with remote wiping technology in the event the device is lost or stolen; and
- Ensure that data breach policies and privacy and security training programs address the use of mobile devices and text messaging.

Conclusion

We expect, as with most technological advances that, in due time, more secure text-messaging technologies will be more affordable or considered standard technology in all cellular or mobile phones. Until such time, we recommend that you take an inventory of staff that are currently using text messaging to communicate with patients and, if it is a practice that is currently being used, develop a policy that takes into consideration the foregoing recommendations.

1. Aaron Smith: Americans and Text Messaging. Pew Research Center. Available at http://pewrsr.ch/1WX8qUk
2. Department of Health and Human Services: Using Health Text Messages to Improve Consumer Health Knowledge, Behaviors, and Outcomes: An environmental scan. May 2014. Available at http://1.usa.gov/21GN846