Published on *The National Law Review* https://natlawreview.com

The “Wild Wild West” Of SMS

Article By:

McBrayer, McGinnis, Leslie & Kirkland, PLLC

SMS text messaging is quickly becoming the preferred method of communication for many people who find it a quick and convenient way to share information with friends, family and, increasingly, with colleagues. This is true in the health care space as well with patients increasingly using text messaging to communicate with providers and to receive health-related reminders and updates, including for health care appointments, medication therapies and health news. For example, anyone can text the word HEALTH to 87000 and begin receiving text messages from the **Center for Disease Control** regarding emergency alerts, new research and reports, as well as health information and tips.

On the provider side, the use of mobile technologies in both public and private sector healthcare has become a part of everyday business. According to SpyGlass consulting group, ninety-four percent of all physicians use a smartphone at work, and there is a growing practice of using text messaging to communicate health and patient case-related information, including in some instances electronic personal health information (ePHI), between doctors and staff. SMS text messaging is fast, simple and convenient, speeding up the delivery of information and theoretically improving patient care.

So what’s the problem with text messaging in health care? Why don’t hospitals, pharmacies and other health care providers simply issue SMS text-enabled devices to physicians, pharmacists and other health care providers to go forth and improve health care with better access to critical information?

The reason is that, generally speaking, text messages sent through commercial data carriers are not encrypted and do not provide the level of security required to prevent unauthorized disclosure of ePHI. Also, for health care providers that do implement and use secure text messaging technologies to encrypt the message itself, there remains a concern regarding the security of the device on the receiving end. Is the receiving device password protected? Is the receiving device lost or stolen? What if the receiving device is an iPhone® and even with password protection, the message displays on the screen for anyone holding (or stealing) the phone to see?

According to the **Healthcare Information and Management Systems Society (HIMSS),** over half of ePHI breaches are the result of theft, loss or misuse of mobile devices. Due to the lack of security typically available for SMS text messaging, providers should avoid using text messages to communicate ePHI, including any individually identifying patient information, even to patients and other providers, unless messaging technology is in place to ensure the security of the message in

transmission, and prevent the unauthorized disclosure of the ePHI from the recipient's mobile device. At the same time, it makes sense that providers should be encouraged to take advantage of the benefits of text messaging for communications involving non-identifying health information, if the organization implements safeguards to protect patient privacy.

In the event an organization determines to permit the use of text messaging for non-identifying patient information, the following is a high-level checklist to help protect the organization and its patients from unauthorized uses of sensitive information:

1) Institute a clear and concise policy that identifies limitations on message content, when the use of text messaging is appropriate and any other limitations.

2) Train providers and staff on the organization's policies regarding the use of text messaging in the workplace, and specifically, with respect to patient care.

3) Passwords and encryption are important ways to prevent misuse and abuse. Even for an organization that does not permit text messaging ePHI, requiring personnel to establish device passwords and to use encrypted transmissions when available will help to reduce authorized use of personnel devices and reduce incidence of losing or disclosing sensitive information.

4) Retention periods and deletion requirements for text messages should be identified. Text messages may represent an important record of what happened and when, but may be subject to the uncertain retention policies of a commercial data carrier, depending on the technology being used.

5) Work with counsel to ensure the organization has appropriate and effective patient-facing policies and procedures in place to communicate to patients how the organization uses text messages to communicate and in some cases offering patients an opportunity to "opt-in" and/or "opt-out" of such communications.

Communicating by text message is woven into the landscape of health care and offers many benefits, and risks, relative to other communication technologies. The pervasiveness of SMS texting makes it impossible to ignore. The balancing act between privacy and convenience can be managed to improve quality of care and patient access. Understanding available technology, maintaining clear policies regarding when and how text messaging may be used in your organization and routine education for personnel are the keys to harnessing this effective and popular communication tool for your organization.

National Law Review, Volume II, Number 278