

VIRGINIA MEDICAL LAW REPORT

Volume 6, Number 6

LEGAL NEWS FOR THE MEDICAL COMMUNITY

NOVEMBER 2009

Health Care Providers, HIPAA and Social Media

BY MARGARET F. HARDY AND JENN RIGGLE

The news is filled with stories about social media and how it's changing the way organizations are doing business. Many hospitals and health care providers have been reluctant, however, to take advantage of opportunities social media offers.

To date, less than 400 of the country's 5,800 hospitals are engaging in social media. The vast majority of health care providers are keeping a safe distance from social media. Why? Often, it is because the use of social media means that providers must rethink how they communicate with their patients and the community, such as:

- Moving from a top-down approach where the message is controlled and not interactive to one that allows employees, caregivers and patients to talk in an open forum and share information.

- Addressing their fears of violating provisions of the Health Insurance Portability and Accountability Act, more commonly known as the HIPAA Privacy Act, as well as state privacy laws.

So often, providers cite HIPAA as a reason for not embracing new technologies, whether it's having physicians e-mail their patients or establishing a corporate Facebook page.

The irony is that HIPAA standards were created to improve health care's efficiency by encouraging providers to electronically share patient information. By not embracing social media, providers may be missing an opportunity to realize the benefits of consumer-driven health care.

Why is HIPAA so frightening?

The federal government created the HIPAA Privacy Rule to ensure that the private health information of patients is protected from people who might use it for their own purposes. To show everyone they mean business, there are severe civil and criminal penalties for people and organizations that do not comply with HIPAA regulations.

Civil fines can be as high as \$1,500,000 for multiple violations of the same standard in a calendar year. For someone who knowingly misuses patient health information, criminal penalties can include a \$250,000 fine and/or imprisonment for up to 10 years.

HIPAA allows health providers to use and disclose protected health information for treatment, payment and health care operation purposes. With few exceptions, health care providers are required to first obtain the written permission of patients to use or disclose their protected health information for any other purpose. All health care providers are familiar with the need to maintain patient confidentiality. HIPAA, while imposing certain specific duties for protecting patient privacy, did not create the duty. Health care providers have for many years taken precautions to protect patient confidences. In many ways, they just need to take what they've been doing with traditional forms of communication

and apply it to social networking platforms such as Twitter, Facebook, YouTube and blogs. For example, whenever they post a video on YouTube, publish a patient testimonial, tweet or post live surgery webcasts that could potentially reveal the identity of the patient, they need to have written consent from the patient.

The challenge is that providers are not the only people "talking" on hospital and physician social media sites. For instance, employees, caregivers and patients can talk about their experiences at the hospital, the care they received and/or post photos and videos of themselves on a hospital's Facebook page. And without the appropriate training, providers may inadvertently violate HIPAA regulations. For example, if a nurse or other employee posts a video or photo taken at the hospital and has a patient in the background without the written permission of the patient – they are violating HIPAA regulations.

It's clear that hospitals can't afford to have their employees committing HIPAA violations, nor do physicians want to expose themselves to being fired by patients or face malpractice suits or disciplinary complaints for failing to maintain patient confidences because they didn't know how state and federal privacy laws impact social media. But can providers afford not to engage in this conversation and have their competitors dominate this conversation? With proper precautions and training, providers have another option: participate responsibly in social media, broadening the scope and depth of communications with existing and potential patients, while complying with HIPAA and state privacy laws.

Hospital communications departments need to serve as social media evangelists and educators so that employees know what is expected of them if they engage in social media in either an official or unofficial capacity. This is particularly important since many hospital employees do not have Inter-

net access during work hours and have to access the hospital's social networking sites from home.

One way to set the social media ground rules for employees is to create a code of participation that outlines best practices and:

- Sets standards for online communications and behavior to ensure consistency with the hospital's brand and HIPAA compliance.
- Holds employees, physicians and caregivers who participate in social media on behalf of the hospital accountable for their online communications and behavior.
- Legitimizes and encourages participation in social media as a branding, business development and networking tool.

Many of the same principles apply to physicians interested in using social media in their practices. Physician practices should establish social media guidelines upfront that address who will be permitted to participate and the type of information to be posted, keeping in mind the goals of the practice. It's essential to regularly monitor the practice's social media sites, both to control content and ensure that information remains current and relevant.

HIPAA also requires that new employees be trained on HIPAA requirements and that all employees receive regular ongoing in-services on HIPAA. For providers participating in social media, such training and in-services should include a discussion of the roles and responsibilities associated with posting, controlling and monitoring social media sites to ensure they are HIPAA compliant.

Impact of state privacy laws

Almost every state, including Virginia, has privacy laws to protect patient confidentiality. Virginia's law on the privacy of medical information is found in the Virginia Health Records Privacy Act (VHRPA). The standards established by VHRPA are similar to those of HIPAA and also apply to social media.



A checklist

Here's a quick checklist of things to consider when engaging in social media:

- Don't identify patients by name or upload photos or video of them to social sites without a signed consent form that complies with both HIPAA and state law.
- Remember that privacy laws protect more than a patient's name and photo. HIPAA privacy regulations restrict the use and disclosure of all "individually identifiable information." The publication of any information that could be sufficient to identify a particular patient, without the patient's express consent, is a violation of HIPAA.
- All providers are required to designate a HIPAA Compliance Officer, who should participate in your social media planning, training and implementation.
- If you're a health care professional, avoid offering anything that could be interpreted as a diagnosis or treatment plan. When possible, include disclaimer language clearly stating that the purpose of the site is informational and is not intended to provide individual medical advice. In addition, you should recommend that readers consult with their physicians.

Social media has the promise of allowing health care providers to engage with their patients in a new way and provide them with health care information in a way that's relevant and customized to meet their needs. However, it takes more than just establishing a Twitter account and a Facebook page – health care providers need to make sure their health care staff and clinicians have the tools to effectively engage in this new media without breaking HIPAA regulations.

Margaret F. Hardy is an attorney with Sands Anderson Marks & Miller in Richmond. Jenn Riggle is an associate vice president at CRT/tanaka in Norfolk.