Social media hold great promise, danger

COMPLYING WITH HIPAA REQUIRES A STAFF STRATEGY AND PROPERLY DEFINED PATIENT INFORMATION

By **MICHAEL McBRIDE,** *Technology Editor*

While the emergency department (ED) at Martin Memorial Medical Center in Stuart, Florida, struggled to save a shark attack victim's life, two paramedic students who were in the ED as part of their college training took digital photographs of the patient, who later died. When their instructors noticed the picture-taking, they ordered the students to stop, informed them of the hospital patient privacy policy, and advised them to delete the photos from their cell phones. Unfortunately, the students already had emailed the photos to friends.

The medical center's parent organization, Martin Memorial Health Systems (MMHS), launched a full investigation into whether the Health Insurance Portability and Accountability Act (HIPAA) had been violated, which, of course, it had. MMHS interviewed more than 50 people during its 3-week investigation. The health system eventually disciplined all parties involved but fired no one.

How does this case differ from other, higher-profile cases involving HIPAA violations? Hospital personnel did not violate privacy regulations by intentionally entering some famous patient's medical record to take a gander at its contents. Nor were the HIPAA violators doctors who innocently exchanged the patient's protected health information (PHI) on Facebook to consult on a diagnosis. These violators were students, not even ED personnel. They were outsiders who happened to be present in the ED at the time. And yet MMHS was still responsible for the PHI disclosure violation.

POWER POINTS

- **Healthcare providers, physicians, nurses, and other medical staff are obligated not to share patient information.**
- **The largest threat posed by social media usage is the potential to improperly disclose patient information.**

Can such an incident happen on a smaller scale, say, in your private practice? Absolutely. Could your practice survive such an investigation, especially if you ultimately receive stiff fines or lose your privileges at a hospital where you practice medicine? Probably not.

But you can take action to leverage social media in your practice without running afoul of HIPAA and hospital PHI policies:

- **Get to know the sites.**

Daniel Shay, JD, who practices law with Alice G. Gosfield and Associates in Philadelphia, Pennsylvania, says that physicians need to take the time to familiarize themselves with how the various social media Web sites operate to better understand and explain the dangers to their staff. (See "Defining social media" to better understand what social media are.)

"If you don't have a Facebook or Twitter account, sit down with your child and ask him or her, 'What's this all about?' " he advises. "If you're going to be developing a social media strategy, you need to get on a social media site and figure out how it all works."

Shay, who primarily focuses on physician representation, fraud and abuse compliance, Medicare Part B reimbursement, and HIPAA compliance from the physician perspective, notes how easily and quickly PHI can get disseminated on the social media site Twitter. When members receive a message (a "tweet") from someone they follow, they can instantly "re-tweet" it to all of their followers, thus spreading the information exponentially.

"These are things worth taking into account when you're developing a social media strategy," Shay says. "Understanding the nature of social media itself is a good starting point."

- **Remove identifying information.**

"Using social media is like riding a hospital elevator," says Bradley H. Crotty, MD, FACP, a fellow at the Harvard Combined Program in General Medicine at Beth Israel Deaconess Medical Center. "There's no control over who hears the information you might share with another physician, or its context."

CONTINUED ON **PAGE 72**

CONTINUED FROM **PAGE 70**

In addition, information travels rapidly—and largely permanently—once it's been posted to the Web. It's critical, therefore, that you remove as much identifying details as possible when openly discussing cases.

"It's best for patients and doctors not to collaborate on medical advice or treatment over social media platforms," he says. "This is an active area with much potential but also many concerns."

- **Seek patient consent in advance.**

"Healthcare providers, physicians, nurses, and other medical staff are obligated to not share patient information," Crotty says. "While that seems fairly straightforward, it becomes tricky if they want to share how their day's going with their online social networks or blog about an interesting experience they just had in the office."

Blogging about the practice and sharing patient data via the Internet or smartphones with other physicians during consults have become fairly standard procedure, so much so, in fact, that if patients were to find out that their information was being shared with strangers, even other physicians, they might react badly to the news.

"Even if one were to withhold identifying information, most people would not appreciate their medical case being discussed on the Internet," Crotty says. "In fact, small details such as location, time, and narrative may actually expose their identity."

Crotty suggests that, after removing all identifying information from a communication, a best practice when considering writing about a case online would be to ask the patient, 'Is it okay to write about this aspect of your case on my blog?' and obtain the patient's consent.

- **Develop two strategies.**

Research conducted by the Pew Research Center found that 59% of all U.S. adults have used the Internet to research drug or healthcare-related topics. One Pew study, titled "The social life of health information, 2011," by Susannah Fox, associate director of the Pew Internet and American Life Project, states that although patients continue to view health professionals as the first place to turn for answers to their health concerns, they also view online resources and advice from their peers as significant sources of health information.

Today, therefore, in addition to developing a social media strategy to ensure that your practice doesn't violate HIPAA, you should develop another strategy to promote, monitor, and protect your "brand."

Thinking in terms of practice branding, however, might not come naturally for you as a physician because your expertise is in medicine, not marketing.

But from a branding perspective, Crotty says, "social media holds tremendous promise in healthcare. Patients live in homes and communities, not in their doctor's offices."

Social media, he says, offer you new and creative ways to engage with patients. Today's practices can use social media to curate patient resources or tweet announcements about practice closures. Patients can opt in to follow doctors and practices online and even interact directly with their physicians. This ability can be an effective use of social media, but Crotty advises restraint.

"Cultivating a professional social media presence or even a professional home page that contains just your biographic and contact information will meet the needs of most patients who are searching for your information online," he says.

- **Establish "dual citizenship."**

Crotty suggests that doctors cultivate a Web identity/presence for their patients to see and visit, but he advises doctors to develop and maintain online "dual citizenships" containing both a public/professional identity and a restricted/private identity. He further suggests that physicians maximize their privacy settings around their personal information.

"The goal," Crotty says, "is to publically project a professional identity for patients while also being able to par-

"Social media holds tremendous promise.... Patients live their lives in their homes and communities, not in their doctors' offices."

—Bradley H. Crotty, MD, FACP, Fellow, Harvard Combined Program in General Medicine, Beth Israel Deaconess Medical Center

DEFINING SOCIAL MEDIA

If you're going to try to control how staff members use social media, it's important to first understand what social media is and is not, according to Daniel Shay, JD, who practices law with Alice G. Gosfield and Associates in Philadelphia, Pennsylvania.

"Social media isn't just email," Shay says. "If a physician is communicating electronically with another physician on the Web, that is not automatically social media."

The current efforts to bring the U.S. healthcare system into the digital age might blur the lines between health information exchange and social media. You and your staff members receive training and incentives to embrace digital technology and the Internet on the one hand, and you are forewarned of the potential for inappropriate usage of it on the other.

All manner of social media sites exist where healthcare professionals interact in a social capacity and not strictly in a medical treatment capacity. Web forums, Facebook, Google+, Twitter, LinkedIn, various photo-based Web sites such as Instagram, and information-sharing Web sites such as Reddit are just a few.

ticipate in social media with friends and family in a less public way."

It's awkward for physicians to receive friend requests on Facebook, for instance, he adds, so "adjusting privacy settings for personal profiles is a good first step toward 'dual citizenship.' "

- **Have a policy in place.**

Having formal PHI policies in your practice communicate to staff members the importance of their actions in this area, Shay says. PHI policies should include clear guidelines and repercussions for violating them, he adds.

"Hopefully, educating your staff about HIPAA will prevent this from happening," Shay says. "But if and when an improper disclosure does happen, you need to have policy in place that determines how you'll proceed." (For more ideas on policy development, see "5 tips for managing your social media policies.")

- **Manage staff usage.**

Learn if and how your staff members use social media, because knowing that information can help you create effective policy, Shay says.

"You can set your network to block certain popular Web sites, making it impossible for your office computers to access those," he says. "That's not going to stop smartphones, though."

Another point worth examining, therefore, is how smartphones are used in your practice. It's not enough to just have a social media policy for your practice's computers; you need a smartphone policy as well.

"If you don't ban their use altogether, staff should be told that if they use their smartphones to check their email, take pictures, or send chats while at work, they need to keep their HIPAA training in mind," Shay says. He notes that the newest smartphones include cameras with such high resolutions that staff members and caregivers can easily snap photos that inadvertently include highly readable PHI.

5 tips for managing your social media policies

As your practice relies more and more on electronic technologies, you face the dilemma of managing staff members' usage of such technologies. As part of a Health Insurance Portability and Accountability Act (HIPAA) compliance program, you will want to develop policies surrounding social media usage. The following guidelines protect practices and guide employees in avoiding improper disclosures.

FAMILIARIZE YOURSELF WITH HIPAA

Probably the largest threat posed by social media usage is the potential for improper disclosure of patients' protected health information. You may think you have a handle on HIPAA, but you should refresh your understanding and learn how HIPAA applies in a social media setting. To do that, you will need to understand what information is protected and what can and cannot be disclosed—by whom and to whom.

KNOW THE ENVIRONMENT

Next, you must understand how social media themselves are used. You may be familiar with Web forums or Facebook, but do you know how Twitter and Instagram function? If not, familiarize yourself with these types of media. Remember, one purpose of your policies is to provide guidance to your staff members. Familiarity with these sites will help you craft clear policies.

IT'S NOT JUST ABOUT YOUR PRACTICE'S COMPUTERS

Policing your computer network is a critical aspect of your social media policies. Blocking Internet access to social media sites may prevent employees from using them during office hours, but it will not prevent them from using home computers, PDAs, or smartphones to do the same thing, both during business hours and outside of the office. Of course, there's only so much you can directly control. You may have limited access to your employees' social media accounts outside the office, but you can—and should—still educate them on the HIPAA-related risks involved in their use of social media. You will need policies that govern their actions outside of your office.

ONE SIZE DOES NOT FIT ALL

Although good general guidelines to follow may exist with respect to social media usage, beware of "canned" policies. Just as with fraud and abuse or general HIPAA compliance programs, your social media usage policies should be tailored to the specifics of your practice. For example, it doesn't make sense to adopt a canned policy that states the use of Facebook on company computers is forbidden if you already block access to the site. Similarly, a canned policy may miss aspects of social media usage that apply to your practice. If your practice maintains its own social media presence for marketing purposes, for instance, then your policies will need to address how the practice will engage in such marketing activities. A canned policy may not cover this situation. Develop your own policies from the ground up, although you can get help in doing so from a lawyer or consultant.

STICK TO YOUR POLICIES

It's not enough to merely have a policy. You have to "live" by the guidelines you adopt. If the policy states that employee training and education is mandatory, then make certain that all of your employees are trained. If the policy says that violators will be reprimanded or fired for violations, then you must follow through on that threat when you discover one. This statement does not mean, however, that you should implement your policies in a knee-jerk fashion. Part of an effective social media policy involves investigating potential improper uses to determine how bad a problem is and what steps must be taken to resolve it. That investigative process also should be outlined in your policies; you may need legal advice.

—Daniel F. Shay, JD,
Alice G. Gosfield and Associates

"If and when an improper disclosure does happen, you need to have policy in place that determines how you'll proceed."

—Daniel Shay, JD, Alice G. Gosfield and Associates

"It's one thing if they take pictures and delete them a few minutes later," Shay says. "The mere taking of pictures isn't the problem as much as is the pictures' content and where they go."

Some practices take digital photos to include in their patients' electronic record, which, Shay notes, is fine and within the bounds of HIPAA. "But if someone takes one of those photos and posts it on Facebook, [then he or she is] likely violating HIPAA," he adds.

It's futile to try to prevent your office personnel from ever using their computers or other devices for anything other than work-related activities, Shay says. Staff members may check email and visit social media sites, he says, so the question becomes: if they are doing so, how do you ensure that they don't use social media in a way that discloses PHI and violates HIPAA?

The answer is, by educating them on the relationship between HIPAA and social media, Shay says.

"Remind them that any information that identifies patients—whether it's a name, a photograph, a description of unique symptoms perhaps accompanied by other bits of patient information—all of that can be PHI," he adds.

For instance, if a staff member connects with someone outside of the office on Facebook, complains about a patient, and mentions details about that patient, he or she might be violating HIPAA, Shay says.

Or suppose you decide to photograph yourself at work, and the camera happens to catch in the background a clear shot of a patient's electronic health record file on a computer screen. "If that screen is displaying PHI and you upload it to the Internet, that's potentially a HIPAA disclosure as well," he says. "So it's important to stress with your staff how easy it is to inadvertently capture and transfer PHI and to reiterate the importance of preventing PHI from getting onto social media Web sites."

- **Don't forget online forums.**

Practice staff aren't the only medical personnel needing ongoing social media training. You also inadvertently can disclose PHI through social media sites such as LinkedIn, which focuses mainly on professionals and which features online healthcare-related forums and groups in which providers can interact with one another.

These online forums are popular gathering spots for all kinds of professionals who commiserate over the challenges and difficulties of their work. What distinguishes healthcare from other professions, and where medical professionals can get into such trouble, is the sensitivity of the information they discuss and the privacy laws intended to prevent such sharing of PHI in public. It's critical that you and your staff remember to enforce HIPAA and to protect patient privacy in these forums.

"Both online and offline, you need to be careful about this kind of stuff," Shay says. "You could be sitting at a bar discussing your day with another physician and inadvertently identify a patient."

- **Keep it quiet.**

HIPAA allows you to exchange PHI with another doctor for treatment purposes.

"If you're sharing PHI on a patient with another physician who's also treating that patient, you're allowed to disclose that information. That's not a HIPAA violation," Shay says. "The mere fact that you exchanged that information electronically doesn't make that an improper disclosure in a social media setting."

If, however, you're inadvertently overheard by someone who shouldn't be receiving the information, that's almost as bad as posting it online.

"That overheard discussion might not go any further, but it's still a disclosure," Shay says.

- **Monitor disseminated information.**

In 2010, Alexandra Thran, MD, a practicing Rhode Island hospital ED physician, posted PHI on Facebook to consult with other physicians on a case. She got fired, was reprimanded, and was fined. No one claimed she posted the PHI with malicious intent. She simply ran afoul of her hospital's PHI policy and experienced severe repercussions.

"That's what I'm talking about," Shay says. "You think you're being vague, but you're actually giving enough information that people can identify the patient."

Knowing how much or how little information you can safely give out publicly can be a challenge, Shay says. Unless you're prepared to close the doors on any and all sharing of patient information, you have to closely monitor on a case-by-case basis how much and what type of information is being disseminated, he says.

"The only people who have any business knowing patient information are the people providing treatment, the billing staff, maybe a practice administrator (and only then if there's a specific reason for them to know it), and the patients themselves," Shay says. "So, if you've provided enough information in a social media forum for someone who's familiar enough with the symptoms to identify the patient, now you've got a HIPAA disclosure."

In many ways, social media can help you build your practice. Gain a clear understanding of how it operates, and implement clearly defined policies and guidelines, to prevent PHI disclosures.

Send your feedback to medec@advanstar.com. Also engage at www.twitter.com/MedEconomics and www.facebook.com/MedicalEconomics.