



Featured *Health Business Daily* Story, Nov. 11, 2011

HIPAA Dangers Lurk on Facebook; Ongoing Policy Revisions Are Advised

Reprinted from **REPORT ON PATIENT PRIVACY**, the industry's #1 source of timely news and business strategies for safeguarding patient privacy and data security.

- November 2011 - Volume 11 Issue 11

Only about a third of hospitals have a specific policy governing their employees' use of social media, such as Facebook and Twitter, according to recent estimates. The number is growing but should be far higher, say privacy and security experts, because so many workers who handle protected health information are using the Internet and opportunities are multiplying for them to violate HIPAA, albeit unintentionally.

In April, the Rhode Island Board of Medicine fined an emergency room physician \$500 for "unprofessional conduct" due to patient information she posted, and later removed, from her Facebook page. Although she had not used patient names, it was possible to identify one based on news reports that contained identical details. The board also ordered her to take what would presumably be a refresher course in patient confidentiality; she had already been fired from her hospital job.

While all health care providers are required to have policies governing PHI, experts say the dangers of Facebook, Twitter and other social media require either separate policies or at least revisions of existing ones to ensure that social media outlets are covered.

Attorney David Harlow, a privacy and social media expert in Boston, believes two-thirds of hospitals lack such policies today. Harlow also writes the highly regarded blog HealthBlawg, which can be found at <http://healthblawg.typepad.com> and addresses these and related issues.

Hospitals looking for resources on social media policies and procedures can also turn to a website offered by Ed Bennett, manager of web operations for the University of Maryland Medical Center (<http://ebennett.org>). The social media policies used by Cleveland Clinic, Ohio State University, University of Maryland Medical Center, among others, are posted on the website, along with links to 547 Facebook pages, 85 blogs, 77 Twitter accounts, and 548 YouTube channels for a wide variety of health care providers.

Bennett also writes a blog, Found In Cache, and posts interviews with social media operations officials at health care organizations.

Mayo Clinic is a pioneer in the use of social media, operating the Mayo Clinic Center for Social Media (<http://socialmedia.mayoclinic.org>). It also has a variety of useful information, and offers consulting, coaching and training on the topic, as well as a "social media health network." Both Bennett and Harlow serve on the center's external advisory board.

An estimated 50% of hospitals simply block social media sites, according to Bennett, a ban which both Jeff Drummond, a partner in the law firm of Jackson Walker LLP, based in Dallas, and Harlow say doesn't solve the problem.

Employees "will just use [the Internet] on their phones," says Harlow, "and then you have zero control." Banning all use of phones is just not a practical solution, he says.

According to Drummond, hospitals and other CEs need to strike a balance between safeguarding patients and providing a "happy workplace."

Employees shouldn't be allowed to access Facebook during work hours "if it's because their goat in Farmville is going to die," but if there's a work reason, then it might be OK, within limits, Drummond says.

CEs could allow access for certain employees, and not others, based on their job duties, in the way that role-based-access functions as security controls for protected health information (PHI).

'Agnostic' Policies Are Advised

The University of Minnesota, for example, is updating its policies to reference social media sites and will engage in retraining. Ross Janssen, privacy and security officer at the University of Minnesota, said the university's approach is to ensure that employees have a thorough understanding of what PHI is so they can protect it on all media. Harlow says that's a good strategy.

"You are always fighting the last war," Harlow says. "The goal is not to be platform-specific. You need an online privacy policy that is platform agnostic."

Employees should assume, and policies should as well, that "anything put online will be re-shared as broadly as possible. The way people use Facebook today was completely unimaginable five years ago," he says. Changing policies "is the biggest problem with Facebook," Harlow says.

Harlow recommends that institutions review their policies twice a year, "as the tools available change." For example, the newest kid on the block is Google Plus, and even existing platforms change all the time, as any of the millions of Facebook users know first hand.

Facebook in particular seems to routinely monkey around with privacy controls and it can be difficult to keep up. In late August, Facebook abandoned its default privacy settings that would be in place for all posts, forcing users to establish a level of "sharing" with each post. Posts can now be shared with the general public without the user being aware of it.

Pay Special Attention to Nurses

Nurses, particularly those with fixed workstations, might have more opportunity to post on Facebook than physicians and may require more training about social media than others. A handful of nurses around the country have already been disciplined and fired for posting information and photographs.

The idea that nurses might be more likely to post "fits our view of them" as friendly and caring, says Harlow. Over time, he hopes nurses and physicians will feel less free to engage in such activities because they will move to more of a "patient-centered" model of care, he says.

One Facebook user was recently alarmed when a friend — a pediatric nurse — posted a photo of a child in a hospital bed on her Facebook page, along with a plea for prayers, as he was to undergo brain surgery. The nurse maintained that the child's mother — her co-worker — had given her the photo and asked her to post it. The child, whose first but not last name was mentioned, was not her patient, the nurse said, and the photograph was taken in another hospital.

In reviewing the incident, Harlow says "it sounds like a friendly thing to do; her heart is in the right place." Yet, she should not have posted the photo unless she obtained the mother's authorization in writing, say both Harlow and Drummond.

"It would need to be a HIPAA compliant authorization," Drummond adds, with the authorization stating the time period during which it will be in effect, that the mother has the right to revoke it, etc.

Drummond also argues that, absent an authorization, the nurse was still bound by law to safeguard the child's PHI by virtue of her being a workforce member of a CE, regardless of whether she had a direct treatment relationship with the child.

Identities Can Be Pieced Together

As the examples of the Rhode Island physician and the nurse also show, HIPAA may be violated because of a false belief that just leaving off a name is sufficient when there is no patient consent.

In fact, it's the collection of details that can lead to identification, and under HIPAA, information is really safe to use, and exempt from HIPAA protections, only when it is stripped of 18 identifiers, including names, addresses, "full face photographic images and any comparable images; and any other unique identifying number, characteristic or code, except as permitted for re-identification in the privacy rule."

Drummond says when he has consulted with clients who've experienced a problem with a Facebook post, the offending employees always "think they are doing some sort of outreach or education." The nurse or physician may have treated a patient who was injured after texting and driving, for example, later posting the photo as an example of the consequences.

In one case a nurse has posted on a local blog details about a patient she had treated, including the patient's symptoms and hospital name. "It was a clear violation of [the hospital's] policies and procedures," Drummond says, adding that, when confronted, the nurse "offered no defense" for what she had done.

"There are people who have grown up having everything posted on Facebook, and having no privacy," Drummond says. "They are posting more" with little thought to the potential impact.

Harlow, who is a serial tweeter, says covered entities have less to fear from Twitter, mostly because of its brevity, with posts limited to 140 characters. Although, as former Rep. Anthony Weiner (D-N.Y.) discovered, an objectionable picture sent via Twitter can have career, if not life, altering consequences.

*AIS is celebrating our 25th anniversary with special discounts of 25% off our most popular publications – including **Report on Patient Privacy**. [Click here to see the deals and save!](#)*

Find this article at: <http://aishealth.com/archive/hipaa1111-03>

Atlantic Information Services, Inc.

1100 17th Street NW, Suite 300, Washington, DC 20036 - **800-521-4323**

Copyright © 2011 Atlantic Information Services, Inc. All Rights Reserved.