Privacy Policies for Social Media

Save to myBoK

posted by Chris Dimick

Jan 06, 2010 05:23 pm

The social media site Facebook had become more than just a way for staff at Innovis Health to catch up with friends.

In November 2008, nurses at the Fargo, ND–based healthcare system began using Facebook to provide unauthorized shift change updates to their co-workers. What once would have been a conversation became an update on their personal Facebook pages.

It was a convenient tool, because the nurses had "friended" each other through Facebook and thus could quickly read what each other wrote on their pages. They did not use patient names, but they did post enough specifics about patients so that the incoming nurses could prepare for their shift.

The problem was that everyone else "friended" to their Facebook pages could also read the information.

"I was shocked, after everything-all the reinforcing of HIPAA and privacy-and then for that to happen. It really took me by surprise," says Becky Kirsch, RHIT, CCS, the director of health information management and privacy officer at Innovis Health.

"We needed to remind staff that that was certainly a HIPAA violation. Even if you don't use patient names, [someone else] can still put two and two together.

"Think if the employee has 300 friends, then 300 people could see that."

When Kirsch and other Innovis management learned of the practice, they quickly implemented stricter policies and prohibitions regarding staff use of social media.

Social media platforms like Facebook, MySpace, and Twitter enable people to easily and instantly share information with friends, family, and the world, even. Its use has become mainstream. Facebook alone reported 350 million active users as of December 2009. [Read more about Facebook below.]

But if staff use social media to talk about work-sharing sensitive patient or proprietary business information-that same easy use and powerful reach broadcasts guarded information to large numbers of people. The release of sensitive information over social media can harm an organization's reputation, violate HIPAA, and lead to breach notifications and hefty fines.

Inadvertent Disclosures Most Common

Privacy breaches via social media can be malicious or inadvertent.

Disgruntled employees can use social media sites to broadcast confidential information about the organization. Staff can also release personal health information about patients via social media, disclosing a celebrity's treatment details or leaking the CEO's medical visit to the facility.

But in most cases, such as the nurses at Innovis, employees do not disclose protected information intentionally. Typically they do so when discussing their days or unusual healthcare cases they witnessed-acts they mistakenly feel do not violate patient privacy.

In late 2009, Innovis Health had another social media incident when an Innovis clinic first responder wrote on Facebook about a strange medical situation they had witnessed that day. No patient names were used, the first responder was simply intrigued by the incident and wanted to share the experience with friends after returning home from work, Kirsch says.

Privacy and security expert Chris Apgar, CISSP, is president of Apgar and Associates, based in Portland, OR. He believes that social networking tools and related communication technologies such as texting now represent significant risks to the privacy and security of health information.

Apgar echoes Kirsch's warning that omitting a patient's name does not guarantee that the person cannot be identified. The uniqueness of a situation alone could allow people to reasonability identify a patient. If healthcare employees post any information that can be used to re-identify an individual, they have inappropriately disclosed protected health information, he notes.

"That is a breach, it puts everybody at risk," he says. "And the problem with Facebook and Twitter is once it is out there on the Internet, it is out there, it is not something that [someone] can easily get back."

In addition, information sent via social media technologies is usually unencrypted and therefore unsecured. That represents a risk even in direct communication between two people.

Policies Necessary

The widespread popularity of social media is fairly recent, and many healthcare organizations have yet to address it directly in written policies. For those that have not, now is the time to start, Apgar says.

Although the technologies are new, addressing their use may not require new or unique policies. Organizations typically can extend existing policies to include social media. Many organizations already have an Internet and e-mail usage policy in place, and social media specifics can simply be added to this policy, he suggests.

In April 2009, Kaiser Permanente published an organization-wide social media policy that explains appropriate staff use of social media-both on Kaiser's own social media sites as well as non-Kaiser sites.

The policy, posted publicly on Kaiser's Web site, specifies that Kaiser employees may not post any proprietary information about the organization on social media or "do anything that might reasonably create the impression that they are communicating on behalf of or as a representative of Kaiser Permanente." The policy prohibits employees from discussing any patient information via social media, even if a patient is not identified by name.

"If there is a reasonable basis to believe that the person could still be identified from that information, then its use or disclosure could constitute a violation of HIPAA and Kaiser Permanente policy," the policy states. It applies to staff using social media both at work and during their own personal time.

Marketing and human resource departments typically develop and implement social media policies, and IT departments provide technical assistance in enforcing them, such as blocking banned Web sites from computers. Privacy officers should be involved to ensure policies fully address all privacy concerns.

Beginning with a risk analysis is a good first step, Apgar recommends. Once the risks are evaluated, the organization can begin writing the policies and procedures to address them.

Bad headlines are the least of a facility's worries. Lawsuits for the disclosure of a patient's protected health information can reach the millions of dollars, Apgar says. New changes to the HIPAA privacy and security rule allow the government to issue greater fines and even prosecute individuals for malicious breaches. "There are people sitting in jail right now for criminal violations of HIPAA," Apgar says.

A Complete Ban at Work?

Some organizations choose to completely ban the use of social media on work computers.

St. Vincent's Medical Center's Behavioral Health Services blocks employee access to social media sites, and its Internet policies state that use of such sites is banned, says Elisa Gorton, RHIA, MAHSM, the director of revenue cycle and privacy officer at the Westport, CT–based organization.

Gorton does not feel the ban is extreme, because use of social media is not a requirement of anyone's job description. "Employees should be working at work, they shouldn't be on Facebook," she says.

Apgar recommends that healthcare organizations block staff access to all social media sites including MySpace, Twitter, and Facebook. This is the best way to mitigate the risk involved with the sites, he says.

Banning use of social media at work also sends a clear message that staff should refrain from discussing work on the sites, according to Bonnie Anderson, MBA, CCISM, RHIA, director of information security and network at HealthEast Care System in Saint Paul, MN.

"We know this could be done in off hours at one's home, but if we allow it from HealthEast's network, we are enabling it," Anderson says. "It almost seems like if we are allowing them to do it here it is like unwritten approval or implied consent."

But not all organizations agree. Some do not block access from work computers, and others allow staff to use social networking sites during breaks or in lounges placed away from the hospital floor. Although Innovis Health has now blocked access to social media sites at work stations, staff can still access the sites on computers in the employee break room lounge.

"We consider it their own time," Kirsch says. "It is their break to do as they choose." However, she notes that access could be revoked once Innovis's new social media policy is finalized.

Organizations that allow access to social media sites still should conduct a privacy and security risk analysis and document their assessment, Apgar says. This shows an organization has evaluated and accepted any risk associated with social media use.

Secondly, facilities must put in an enforceable policy that states the terms of appropriate use. Policies should spell out that staff can not disclose protected health information through social media sites. "Say 'it is okay to use it, but here are the prohibitions,'" Apgar recommends.

Taking these steps shows the organization did not "willfully neglect" the risk of a breach associated with social media. New provisions in the HITECH Act state that if an organization willfully neglects a privacy risk, it can be investigated and fined by the federal government, Apgar says. If a privacy incident does occur through social media, an organization can point to its assessment and policies and show it evaluated the risk and demonstrated due diligence.

Addressing All Use, Anywhere

Organizations that ban use of social media at work are under no illusion that their risks are eliminated. That is why policies also must include language that addresses employee use of social media during personal time. Staff can just as easily post information about patients or their organizations from their home computers or mobile phones.

Mobility and social media go hand-in-hand. An estimated 65 million people access Facebook via their phones, and they represent the most active users, according to the company. Twitter thrives on "tweets" sent from mobile phones, and even blogs can be run from a phone. A photo snapped on a phone in a hospital lobby could be on the Internet within seconds.

Social media policies should prohibit employees from discussing work-related information on blogs, social media, and other Internet platforms. Like the Kaiser policy, all social media policies should state that employees must not declare themselves as representatives or spokespeople for their organizations.

HealthEast Care System began developing a policy on social media after an employee reported to management that a Facebook friend and coworker was using Facebook to vent about work and inappropriately discuss patient cases, says LaVonne Wieland, RHIA, CHP, the information privacy director.

The HealthEast policy covers Facebook, Twitter, MySpace, LinkedIn, comments posted to a blog, YouTube, wikis, chat rooms, and any other social networking sites. Those who violate the social media policy can be terminated from employment, Wieland says.

It is impossible for an organization to monitor the social media activities of its employees, making it difficult to enforce social media policies. Instead, organizations must focus on education and awareness and encourage staff to report any breach of policy they may witness on other sites.

"We tell employees that it is their obligation to notify their supervisor or the privacy officer if they come across anything [on social media sites] that is a suspected breach of confidentiality," Kirsch says.

When alerted to inappropriate posts, St. Vincent's Behavioral Health Services staff has contacted current and former staff members and requested they erase the proprietary information or face corrective action.

Education and Awareness Critical

The biggest risk with social media is that many healthcare employees do not realize that posting stories about nameless patients is still a HIPAA violation, Kirsch says. When questioned about their use of Facebook, for example, the Innovis nurses involved in the 2008 incident stated they thought they were doing a good thing-preparing the next shift to provide great care.

As Kirsch began talking with other staff in the organization, she found more who assumed that their posts were harmless because they did not mention patients by name and only their Facebook friends could read what they write.

As Innovis's IT department blocked access to social media sites and the marketing department developed specific social media policies, Kirsch began providing the entire organization with refresher courses on HIPAA, specifically discussing the use of social media.

At HealthEast Care System, Wieland now includes social media when reviewing privacy policies with new employees. "If we are talking about a patient, we are breaching their privacy," Wieland says, "whether we have used their name or not.

"I tell them that it is not appropriate to talk about patients or things at work on social networking or any open, public spot," Wieland says. "What you see and hear at work stays at work."

That core privacy principle is unchanged, regardless of technologies or trends.

"Facebook is very popular right now, so we need to remind each other that we should not be discussing any information about our patients, in any form, outside of work," Kirsch says. "The 'need to know' aspect is huge. Do you truly need to post that information on social media? And the answer is no."

What Is Facebook?

"Social media" describes accessible and inexpensive (often free) Web-based tools used to communicate widely, quickly, and easily. Popular examples include Facebook, MySpace, and Twitter. Blogs are a form of social media that contrast with traditional media such as newspapers and radio. Social media users can post personal information, search for and communicate with other users, send direct or broadcast messages, and e-mail.

Facebook is the fastest-growing social media utility. Created in 2004 by four Harvard college students, the site boasted 350 million active users by December 2009. Half of those users are on the site on any given day, according to the company. The average user spends more than 55 minutes on the site per day.

Facebook is free to use. Members create profiles featuring pictures and personal information. They then "friend" other members, which allows them to view and post comments on their friends' sites and introduces them to their friends' friends.

That online networking is creating what the company calls "the social graph, the digital mapping of people's real-world social connections."

Users choose among three levels of privacy settings, which generally limit who has access to which information on their pages. Users can also form more private “groups.” The service also allows for direct e-mail and instant messaging between friends.

Original source:
Dimick, Chris. "Privacy Policies for Social Media" (Journal of AHIMA website), January 2010.
