



Healthcare Risk Management™



Facebook firings show privacy concerns with social networking sites

Remind staff about slippery slope with online postings

IN THIS ISSUE

■ Nurses fired for posting X-ray on Facebook cover

When it seems as though nearly everyone is on Facebook, MySpace, or other social networking sites, you can be assured that many of your employees are online chatting about everything under the sun — including what happened at work that day. For health care employees, that can lead to a serious breach of privacy if they pass on protected health information.

That's what happened in Lake Geneva, WI, according to authorities there. Walworth County Undersheriff **Kurt Picknell** reports that his office began investigating when an anonymous caller claimed that a nurse at Mercy Walworth Medical Center had photographed a patient with her cell phone and posted the picture on her Facebook page. Picknell's investigation determined that two nurses had independently photographed an X-ray image of a patient and at least one posted the image.

The nurses took photos of an X-ray showing a sexual device lodged in the patient's rectum. Picknell reports that the police investigation confirmed the incident was discussed on one of the nurse's Facebook page,

Financial Disclosure: Author Greg Freeman, Managing Editor Karen Young, Associate Publisher Russ Underwood, Nurse Planner Maureen Archambault, and *Legal Review & Commentary's* co-author Radha Bachman report no consultant, stockholder, speaker's bureau, research, or other financial relationships with companies having ties to this field of study. *Legal Review & Commentary* co-author Leilani Kicklighter is a consultant for Kendall Endoscopy Surgery Center, Presidential Surgicenter Center, and Visual Health Eye Surgical Center. She also is a principal in The Kicklighter Group.

EXECUTIVE SUMMARY

A recent case in which nurses were fired for posting private patient information on Facebook has raised concern about the danger of online postings. Risk managers must ensure that staff not give in to the temptation to chat online about their patients.

- Good privacy training and sanctions can protect the hospital.
- Young employees and new hires may be more likely to breach patient privacy.
- Specifically caution employees about posting patient information online.

SPECIAL REPRINT

Reprinted with permission of AHC Media LLC.

P.O. Box 740056, Atlanta, GA 30374. For subscription information: (800) 688-2421.

MAY 2009

VOL. 31, NO. 5 • (pages 49-51)

but she has since removed her page. Authorities did not see the image posted on Facebook, but the anonymous caller claimed to have seen it on the web site.

Picknell says the nurses' conduct does not violate state laws, but he referred the case on to the FBI for possible federal violations. Mercy vice president Barb Bortner issued a statement saying the nurses were fired for violating company policy. She said Mercy employees undergo regular education about company policies and federal regulations such as HIPAA.

The threat from social networking sites builds on the problems posed by the ubiquitous cell phone

camera. Risk managers previously have raised concerns about threats posed by staff and visitors having cell phone cameras in the hospital, making it simple to take photos that could compromise patient privacy or even facilitate sexual abuse. Publishing the photos on social networking sites takes the danger to a new level, experts say. **(For more on the risks from cell phone cameras in health facilities, see *Healthcare Risk Management*, September 2007, pp. 97-101.)**

Also, snooping in medical records and gossiping about patients is nothing new in health care. Celebrity patients always have been at risk. In one notable situation, the UCLA Medical Center in Los Angeles reported last year that more than 120 workers had looked at celebrities' medical records and other personal information without permission between January 2004 and June 2006. The popularity of social networking sites makes it easier to spread private information that, in years past, might have been shared only with a small circle of friends and family, says **Dwight Scott, JD**, an attorney with the Houston law firm of McGlinchey Stafford and previously in-house counsel for a major hospital organization.

The nurses' actions definitely violated HIPAA, Scott says, and, when there is a HIPAA violation, there usually is a violation of state and federal privacy laws, he says.

"This is an egregious violation, and termination is exactly what should have happened," Scott says. "If I were one of those nurses, I wouldn't only be worried about where my next job is coming from, but also whether the board of nurse examiners in Wisconsin is looking into them, which I bet they are."

In most states, this type of conduct would trigger a mandatory reporting requirement to the nursing board, Scott notes.

A. Kevin Troutman, JD, an attorney with the law firm of Fisher & Phillips in Houston, points out that the hospital apparently did nothing wrong. In fact, what it did right — explicitly prohibiting such behavior and firing staff who violated that rule — will probably safeguard it from a HIPAA violation or anything other than a frivolous lawsuit, he says.

The employer is subject to criminal prosecution for the action of employees unless it can prove that it provided adequate training on patient privacy, Troutman says. If the employer properly trained employees, and they committed HIPAA violations anyway, then the employer is unlikely to be held responsible, he says. That is why it is so important

Healthcare Risk Management® (ISSN 1081-6534), including **HRM Legal Review & Commentary**™, is published monthly by AHC Media, LLC, 3525 Piedmont Road, Building Six, Suite 400, Atlanta, GA 30305. Telephone: (404) 262-7436. Periodicals Postage Paid at Atlanta, GA 30304.

POSTMASTER: Send address changes to **Healthcare Risk Management**®, P.O. Box 740059, Atlanta, GA 30374.

Subscriber Information

Customer Service: (800) 688-2421 or fax (800) 284-3291, (customerservice@ahcmedia.com). **Hours of operation:** 8:30 a.m.-6 p.m. Monday-Thursday; 8:30 a.m.-4:30 p.m. Friday.

Subscription rates: U.S.A., one year (12 issues), \$499. Add \$17.95 for shipping & handling. Outside U.S., add \$30 per year, total prepaid in U.S. funds. For approximately 15 CE nursing contact hours, \$545. Discounts are available for group subscriptions, multiple copies, site-licenses or electronic distribution. For pricing information, call Tria Kreutzer at 404-262-5482. Missing issues will be fulfilled by customer service free of charge when contacted within one month of the missing issue date. **Back issues**, when available, are \$87 each. (GST registration number R128870672.)

Photocopying: No part of this newsletter may be reproduced in any form or incorporated into any information retrieval system without the written permission of the copyright owner. For reprint permission, please contact AHC Media, LLC. Address: P.O. Box 740056, Atlanta, GA 30374. Telephone: (800) 688-2421. World Wide Web: www.ahcpub.com.

AHC Media LLC is accredited as a provider of continuing nursing education by the American Nurses Credentialing Center's Commission on Accreditation.

This activity has been approved for 15 nursing contact hours using a 60-minute contact hour.

Provider approved by the California Board of Registered Nursing, Provider #14749, for 15 Contact Hours.

This activity is valid 24 months from the date of publication.

Healthcare Risk Management® is intended for risk managers, health system administrators, and health care legal counsel.

Opinions expressed are not necessarily those of this publication.

Mention of products or services does not constitute endorsement. Clinical, legal, tax, and other comments are offered for general guidance only; professional counsel should be sought for specific situations.

Editor: **Greg Freeman**, (770) 998-8455.

Director of Marketing: **Schandale Kornegay**.

Managing Editor: **Karen Young** (404) 262-5423
(karen.young@ahcmedia.com).

Associate Publisher **Russ Underwood** (404) 262-5521
(russ.underwood@ahcmedia.com).

Senior Production Editor: **Nancy McCreary**.

Copyright © 2009 by AHC Media, LLC. **Healthcare Risk Management**® and **HRM Legal Review & Commentary**™ are trademarks of AHC Media, LLC. The trademarks **Healthcare Risk Management**® and **HRM Legal Review & Commentary**™ are used herein under license. All rights reserved.



Editorial Questions

For questions or comments, call **Greg Freeman**, (770) 998-8455.

to keep up-to-date records showing patient privacy education was provided for new employees and refresher courses on a regular basis.

"I expect that most hospitals will be able to show that they have appropriate training and policies, including sanction policies, in place. Unfortunately, some individual nurses made very bad decisions regarding patient privacy, and the hospital is having to deal with the aftermath," Troutman says. "The really interesting point is that to protect themselves, hospitals and other health care providers must recognize how changes in the uses of social networking and other web technology present new threats to patient privacy. Considering both the rapid changes in technology and the number of new people entering the workplace, this is going to be a moving target."

Although Troutman says the hospital is not likely to face sanctions and may have a good defense against a lawsuit by the patient, he points out that the organization is taking a hit in public relations.

"No hospital wants people in the community to think that its employees are laughing at patients behind their backs and making light of their situations," he says. "That alone is good enough reason to try to get ahead of this kind of activity, even if you know you can distance yourself from legal repercussions."

Scott says the Wisconsin case is an important reminder to risk managers of the need to factor in employees' social lives when considering risk and formulating policies.

"Everybody likes to go home and talk to their spouse or loved one about an interesting thing that happened at work that day. It's just human nature," he says. "Now that forum has been opened up with the prevalence of the social networking sites. Instead of talking with your spouse in the living room about this strange case, you're talking with all your friends in a public forum."

The nurses in Wisconsin may have become so inured to the casual chatting on Facebook and the frequent posting of pictures on the site, that they did not realize they were crossing a line until it was too late, Scott speculates. In their minds, they may not have viewed their actions as much different than just telling a friend about the day's events at work.

Talking to your friends about work isn't necessarily an invasion of privacy. It's when you include patient-identifying information that it becomes a violation, he points out.

"Some of the fine print in HIPAA clearly states that an X-ray is protected health information, but

SOURCES

For more information on patient privacy and social networking sites, contact:

- **Dwight Scott**, JD, McGlinchey Stafford PLLC, Houston. Telephone: (713) 335-2127. E-mail: dwscott@mcglinchey.com.
- **A. Kevin Troutman**, JD, Fisher & Phillips LLP, Houston. Telephone: (713) 292-5602. E-mail: kttroutman@laborlawyers.com.

there is an argument for the nurses that the pictures of the X-ray they took did not identify the patient if they didn't show the nameplate," Scott says. "It's not a good argument and doesn't excuse the behavior."

Troutman agrees, saying problems stemming from blogging and posting on social networking sites are similar to what happened when e-mail first became popular. E-mail encouraged a false sense of casualness that could lead to improper behavior, and now the same problem is seen as more people are starting to use social networking sites.

"You've got to get them to realize that this is not an informal communication when it comes to your privacy policy," he says. "They really shouldn't even be talking to people in the break room about patients, but sending it on the Internet makes it a very serious violation."

Scott advises risk managers to specifically warn employees about the dangers of posting information on social networking sites or blogging about their work. When he was in-house counsel, his organization provided regular inservices on patient confidentiality, including an online test that employees had to complete annually to remind them of patient confidentiality issues.

Troutman says risk managers — who aren't necessarily going to be Gen X or Gen Y youngsters who are into online blogging and networking — must consider how their employees look at online activity and how important it can be to them. Privacy education regarding online activity is particularly important for new hires, the younger generation who may be most heavily involved in online activity and the least familiar with privacy concerns, Troutman says.

"I see employers dealing with a lot of new hires who don't understand basic business etiquette and the most basic concerns about privacy," he says. "Unfortunately, it's the employer's responsibility to teach them, to eliminate this idea that the rules

don't count when you're talking online."

While you cannot prohibit employees from posting or blogging on their free time, Scott says you should underscore how easy it is to breach patient confidentiality online. In particular, he says, emphasize that simply avoiding obvious patient identifiers such as names is not enough.

"If you're talking about a 74-year-old gentleman who lives in a small town in Wisconsin and how he came in with an unusual medical condition, it might be pretty easy to figure out who he is," Scott says. "Remind them what a slippery slope this can be — that they can find themselves in violation of their confidentiality agreement without even realizing they did anything so egregious. By then, it's too late. Their careers are in jeopardy." ■