Social media: Helping staff manage personal, professional boundaries

A 20-year-old nursing student, Emily, was excited to be on her pediatrics rotation and taking care of Tommy, a 3-year-old leukemia patient. One day, when Tommy’s mom was out of the room, Emily asked Tommy if she could take his picture. He readily agreed. When she got home, Emily excitedly posted the photo on her Facebook page. His room number was easily visible in the background.

Three days later, Emily was called to the dean’s office. Her Facebook post had been reported. Emily was expelled from the program, and the hospital banned the nursing program from its pediatrics program. Emily didn’t intend to breach the patient’s confidentiality, but it didn’t matter. Not only was the patient’s privacy compromised, but the hospital faced a HIPAA violation.

Emily’s heartbreaking story is just one example of how social media, with its urge to connect, can also challenge professional boundaries. The case is cited in a new white paper and nurse’s guide to social media by the National Council of State Boards of Nursing (NCSBN).

Social media holds many benefits for health care—it can create closer bonds between caregivers and their communities—but it also carries risks.

What’s a manager’s role in guiding the staff in managing the risks?

Guidance comes from NCSBN, ECRI Institute, and sample policies of hospitals and health systems.

“We were shocked when we did a survey and found how many state boards were having complaints [involving social media] and had had to discipline nurses,” Nancy Spector, PhD, RN, NCSBN’s director of regulatory innovation, told OR Manager.

The 2010 survey found 33 of 46 state nursing boards had received complaints about such violations, and 26 boards had taken disciplinary action.

Risks of social media

In its paper, ECRI Institute outlines the growth of social media, how health care organizations are using it to their advantage, and how they can take steps to limit its risks. ECRI Institute is a nonprofit organization that researches health care technology and services.

Some obvious risks are privacy and the risk to reputation, notes the paper’s author, Paul Anderson, the institute’s director of risk management publications.

Privacy

“It’s so easy on social media to violate patient privacy,” Anderson observes. “It almost invites you to violate privacy because it wants you to tell stories.”

Privacy violation is not just about disclosing patients’ names.

In one case, two nurses independently photographed a patient’s x-ray, and at least one posted it on her personal Facebook page. An anonymous caller alerted police. Though the photo was deleted before authorities could verify it was there, the nurses were fired immediately. They also faced discipline by the state nursing board.

Even when sharing patients’ success stories or good outcomes, the staff must tread carefully, Anderson advises. He suggests that risk managers may want to consider a policy stipulating that all descriptions of patients be reviewed before being released.
One organization’s social media policy

Sutter Health, a northern California-based health system, cleverly uses social media to communicate its own social media policy. Employees can watch a short animated video on the policy and review a tip sheet summarizing the official policy (www.sutterhealth.org/employees/social-media-policy.html).

Examples of guidelines for employees

The policy outlines acceptable use of social media, both through sites hosted by Sutter Health and other sites. A few examples of guidelines for employees’ personal use of social media are:

- **Limit participation on social media during work time unless required by their position; incidental use during break times or in a manner consistent with other general internet use is not prohibited.**
- **Not to disclose any patient-identifiable information of any kind without the express written authorization of the patient, even if the person is not identified by name, if the person could still be identified by the information.**
- **Not to disclose any confidential information about the organization, its vendors, suppliers, or patients.**

Responsibilities for managers

Some responsibilities of managers outlined in Sutter’s policy are:

- **Not to access a restricted website or social networking site without authorization (such as insisting that an employee provide a password).**
- **To consult the human resources department before taking any action against an employee for social networking, such as requesting that an employee remove a post or coaching/counseling for social networking use.**
- **To be cautious about establishing an online relationship with employees on personal social networking sites.**

Employee rights

Regarding employees’ rights, Sutter’s policy includes a statement that “nothing in the policy will be interpreted to limit or interfere with an individual’s rights to discuss the terms and conditions of their employment or other rights under Section 7 of the National Labor Relations Act.”

Addressing consequences, the policy states: “Any individual who violates this social media policy will be subject to appropriate remedial action; in the case of employees, this may include discipline, up to and including termination.”

Risk to reputation

What employees say online can harm an organization’s reputation. Yet employers walk a fine line in managing what employees post on social media about their workplace on their own time.

That was highlighted in a case settled with the National Labor Relations Board (NLRB) in 2010. The board administers the National Labor Relations Act, which protects workers, both union and nonunion, in exercising certain rights, including the right to discuss their wages or working conditions without being disciplined by their employer.

The case involved an ambulance company that fired an employee at least partly for her derogatory comments about her supervisor on Facebook. In the settlement, the ambulance company agreed to revise what the NLRB termed as its “overly broad rules” that prohibited employees from disparaging the company or its supervisors. The NLRB said it considered this an improper restriction on the employee’s right to discuss her “wages, hours, and working conditions with coworkers while not at work.” The NLRB’s counsel, quoted in The New York Times, said the employee’s posting was similar to employees standing around a water cooler talking about their working conditions, adding, “They have a right to do that.”
What types of limitations can employers impose?
Though they can’t infringe on employees’ rights to discuss working conditions, Anderson says, they can have a policy that, for example, prohibits staff from speaking or writing negatively about an employer’s services. Thus, a statement by a nurse such as, “I would never have surgery here,” could be prohibited. But a statement related to working conditions, such as, “I have the worst manager. She gives me the lousiest shifts,” could not be restricted.

Managing social media
To harness the benefits of social media while helping to manage its risk, the ECRI Institute paper advises that each organization have a social media plan. Having a plan helps to avoid a haphazard approach that can waste resources and leave the organization open to a potentially damaging mistake.

Regarding employees’ use of social media, the best course is to have a social media policy and educate the staff. By having a policy, an organization makes clear what is acceptable and what is not, Anderson points out.

Some resources include:
- The American Medical Association’s policy, Professionalism in the Use of Social Media (www.ama-assn.org/ama/pub/meeting/professionalism-social-media.shtml). Though written for physicians, it outlines key points that could apply to staff as well.
- Sample hospital policies are available on Ed Bennett’s Found in Cache blog, which covers use of social media in health care (http://ebennett.org).
- NCSBN offers educational resources for nurses.

Once a policy is in place, make sure the staff receive education, and for documentation purposes, have signed that they have read the policy. “Make sure you’re not in a situation where the staff can come back and say, ‘I didn’t know,’” Anderson cautions.

A policy serves to protect the organization. If an employee violates a patient’s privacy, for instance, the organization could be liable for a violation of the Health Insurance Portability and Accountability Act (HIPAA). But if the organization can demonstrate that it has a social media policy and has educated the staff about it, that can help to insulate the organization.

Says Anderson, “My experience is that if guidelines are reasonable, the staff will try to comply. But if there are no boundaries, it’s the Wild West.”

References