You can’t say that: Using social media in the healthcare setting requires sound judgment

It is hard to have tea with a friend or brag about a school soccer victory without involving social media. What was once a private or family matter no longer seems real until it is texted, posted, or even turned into a movie.

Healthcare organizations, including ambulatory surgery centers (ASCs), also are affected by the prevalence of social media, but unlike other businesses, they are bound by patient privacy restrictions that often bump against ever-widening concepts of free speech.

Responsibility for ensuring patient privacy is something ASCs share with hospitals and other healthcare providers, but ASCs often are small and independent organizations, without specialists in human resources, legal liability, or Internet services.

Many ASC administrators believe they should establish policies on social media use; others say current standards, such as the Health Insurance Portability and Accountability Act (HIPAA), apply to social media as well as other forms of communication.

Both positions are correct, according to Marcus Crider, JD, but ASCs should consider other factors in deciding how to handle employee use of social media.

“You’re not required by law to have one; it’s not essential,” Crider says of formal policies.

Crider is a partner at the Waller law firm in Nashville, Tennessee. He specializes in labor and employment litigation on behalf of employers, and he often works with ASCs. He spoke on social media issues at the 2014 conference of the Ambulatory Surgery Center Association (ASCA).

One ASC that has opted not to issue a formal social media policy is Redmond Surgery Center in Redmond, Oregon. “We talked about it at the board level,” recalls Anna Barr, RN, CASC, CNOR, the center’s administrator, “but they decided not to go forward with it at this time.”

About half of the ASCs in the US have made similar decisions, Crider estimates.

The rest have established various policies, often as a result of an incident in which an employee, inadvertently or not, revealed confidential information. To craft an effective policy, one that will be understandable, enforceable, and able to withstand a legal challenge, requires knowledge of both the social media world and the law.

It’s everywhere

According to statistics compiled by Crider, 73% of American adults use social media in its various forms. Users of Instagram total 130 million; LinkedIn, 238 million; Google and Twitter, 500 million each; and Facebook, 1.15 billion.

The ubiquity of social media means that misuse is inevitable. Crider, in his ASCA presentation, recounted the tragic result of a thoughtless Tweet. A young woman on her way to vacation in Africa made a racist comment that circled the world within a few hours. She lost her job, millions of people were insulted, and millions more outraged.

“Do not underestimate the power of social media,” Crider warns. “Use other people’s mistakes as learning opportunities.”
Whether a formal policy exists or not, have a frank talk with employees about best practices, he advises. Remind staff to keep personal and professional matters separate, avoid controversial topics, and guard against the impulse to vent emotions online.

To protect the ASC (or any company) and patients, as well as to spare the poster from embarrassment or discipline, Crider offers more specific best practices in social media use:

• Protect sensitive information such as financial data and trade secrets.
• Don’t reveal private information about colleagues.
• Don’t publish photographs, trademarks, or logos without permission.
• Never use social media to harass someone or make offensive comments or jokes.
• Don’t imply you are speaking on behalf of the company; if necessary, specify that you aren’t.

Why have a policy?
HIPAA spells out requirements for patient privacy, but its provisions may be far from the mind of an employee texting at home or in the break room.

“One of biggest reasons for a social media policy would be to remind everyone of the need for strict compliance with confidentiality,” Crider says.

Additional reasons to develop a policy are to make managers and staff aware of their rights and responsibilities, and to have a written statement to refer to when addressing violations.

A policy, Crider notes, can spell out rules of etiquette for social media. It can address an employee’s expectation of privacy and freedom of expression, which must be honored if the policy is to survive legal challenge. It can inform managers, owners, and governing board members who may not be regular users of social media of its potential to harm or enhance the organization’s reputation.

Such a policy recently came in handy at The Eye Associates Surgery Center in Bradenton, Florida. After an employee posted a seemingly innocent photo that could have revealed a patient’s identity, compliance coordinator Jody Gibbs sent an email to all staff recapping the rule. “Please refrain from posting pictures, descriptions, or experiences regarding patients, patient visits, or exams as it relates to you and The Eye Associates,” she reminded them. “This information, even without patient names, is considered a HIPAA violation,” she added.

“We take it really seriously,” Gibbs says of the surgery center’s social media policy. Employees attend a training program on the topic, and they are encouraged to review the materials when questions arise.

A word about Facebook
The Eye Associates has a website, like most ASCs. It also has a Facebook page, with less detailed information but more chances for interaction with the public and patients. As Gibbs notes, “Any patient on the site has signed a release.”

Facebook can be a public relations tool if used properly. Crider recommends hiring a marketing firm or consultant to design and moderate the website and Facebook page, as it is unlikely any staff member has that expertise. Be sure a system is in place to obtain releases for any personal photos or information, and control online patient feedback to avoid false postings.

What is a good policy?
A good source of guidance for social media regulation is the National Labor Relations Board (NLRB), according to Crider. Over time, through its rulings, the NLRB has made clear which policies it considers justifiable and, equally important, which ones it does not.
The NLRB frowns on policies that are too general. A vague or unexplained statement could be construed as infringing on someone’s rights or subject to being unfairly enforced.

The NLRB considers the following rule to be too general: “Employees must avoid posting anything on social media sites that is disparaging to the company or disrespectful to the company’s employees.”

Other words the NLRB prefers to avoid are “confidential,” “sensitive,” and “unprofessional.”

Since healthcare organizations as a group and individual ASCs have special considerations regarding social media, they will need to develop their own wording. Be as specific as possible, Crider advises. “Provide examples of forbidden behavior to help educate employees, and explain the consequences of violating the social media policy.”

List the specific types of confidential information you do not want disclosed, such as patient names, identifying information, or financial transactions. When discussing harassment or forbidden language, choose descriptive terms like “threatening” and “obscene” and those that have legal definitions, like “hostile work environment” and “defamation.”

It is important to understand and respect employees’ rights, Crider notes. Do not ask for their passwords. Administer discipline consistently. Provide education, and have supervisors monitor compliance. “Develop a thick skin,” Crider adds, “Overreaction can potentially exacerbate negative publicity.”

Finally, ASCs that elect to have either an informal social media policy or none at all are subject to the same regulations mentioned in formal policies, particularly that of protecting the privacy of patients and avoiding disclosure of confidential information. Ensure that employees understand that HIPAA applies to electronic interactions as well as those taking place in person.

“There’s no cyber excuse for violating other policies,” Crider says. ❖

Reference