Technology

# Physician use of social media: Navigating the risks

## Establish social media guidelines to protect health information, and reputation of practice and physicians



by **DANIEL F. SHAY, JD** *Contributing author*

### HIGHLIGHTS

**01** By understanding how information can be transmitted on social media sites, practices can tailor their social media policies to respond to the risks.

**02** With inquiries to a practice's social media account, it may be easier to state that the practice does not publicly discuss patient care, but suggest that the user contact the practice by phone to resolve any issues.

As social media use in the United States continues to grow, Physicians are realizing how valuable a tool it can be for marketing and patient interaction. But the use of social media within a healthcare context introduces additional risks that physicians and practices must learn to navigate.

**SOCIAL MEDIA** can represent a useful tool by which physician practices may advertise their services, disseminate general health information, and interact with patients. However, there are also risks involved in using social media that practices must understand and avoid.

Some physicians have faced serious consequences from poor use of social media. For example, a physician was terminated from his position at a Chicago hospital after posting pictures of an intoxicated patient on his personal social media account. In other cases, practice employees have posted pictures taken at work which included patient protected health information in the background of the photo.

These types of behavior present risks to physician practices, including potential breach of the Health Insurance Portability

and Accountability Act (HIPAA). While there is no way to completely prevent inappropriate uses of social media, practices should develop and enforce social media policies to protect themselves. This article offers practical advice on how to evaluate and respond to risky social media behavior, and how to craft policies to address such behavior.

## HIPAA RISKS

By understanding how information can be transmitted on social media sites, practices can tailor their social media policies to respond to the risks presented by social media HIPAA disclosures.

These risks are not insignificant. Posts on social media sites are usually not "encrypted" for HIPAA purposes, and therefore are considered "unsecured protected health information (PHI)." Improper disclosures on social media therefore implicate not only the HIPAA Privacy Rule, but also the Security Rule and Breach Notification Rule.

Improper PHI disclosures via social media typically result from two types of communications:

- direct communications with patients; and
- employee posts on personal social media accounts.

Social media policies designed to respond to HIPAA must address each vector by which PHI may be improperly disclosed.

With respect to communications from patients, consider the differences between responding to a patient inquiry about the results of a diagnostic study on a site like Facebook as opposed to a site like Twitter. A response on the practice's Twitter account will be visible to at least all of the practice's Twitter followers, and potentially to any individual with a web browser. Therefore, practice policies should state that Twitter may not be used to communicate directly with patients, particularly in response to inquiries about their own health.

On Facebook, the question is more complicated. What privacy controls does the practice have enabled on its Facebook account? Did the patient communication appear on the practice account's timeline —visible to all—or was it sent as a private message? A response on the practice's public page is almost as visible as a Twitter post. But a response by private message is not visible to anyone but the user of the account receiving the message.

Improper HIPAA disclosures are also likely to happen on personal employee accounts. For example, an employee may think nothing of posting about an irritating patient with sufficient detail as to identify the patient. Even well-meaning employees can make such a disclosure without realizing it. If a practice employee takes a picture with their favorite patient and posts it to their social media account, the post is a PHI disclosure. Likewise, employees may post photos of seemingly innocuous content, such as a picture of their lunch…which happens to be sitting on top of a patient chart or order sheet.

These types of disclosures will require a careful analysis to determine if they rise to the level of a "breach" under HIPAA, including attempting to determine how many people may have seen the post (which can vary based on the time of day it was posted, how many friends the account has, any privacy settings on the post, etc.).

## DEFAMATION AND REPUTATION MANAGEMENT STRUGGLES

In contrast to scenarios where a practice employee discloses PHI on a social media site, defamation involves patients posting negative comments about the practice on their own social media accounts or to public review sites like Yelp or Google Pages. When this happens, physician practices must understand their available options.

While the first inclination may be to sue the "deep pockets" of an online review site, such lawsuits have proven unsuccessful due to federal and state law protections. Lawsuits against individual users may represent a better chance at responding to defamatory comments, but can be expensive and time consuming, even if they ultimately prove successful.

If the suit is not successful, some states have laws that require businesses who lose defamation lawsuits to pay for the individual's legal expenses. These laws are designed to prevent lawsuits known as "strategic lawsuits against public participation" (or "SLAPPs") where businesses attempt to stifle otherwise legitimate negative public comment. Practices must therefore carefully consider whether it is worthwhile to file a lawsuit at all, particularly in "anti-SLAPP" jurisdictions.

By understanding how information can be transmitted on social media sites, practices can tailor their social media policies to respond to the risks presented by social media HIPAA disclosures.

It is also worth considering the actual impact of negative reviews and statements. Readers are more likely to ignore a negative review if it is poorly written or illegible, or if it is the lone negative review in a sea of otherwise positive reviews. Such negative reviews may even be dismissed by readers as obvious fakes. Many review sites also include built-in mechanisms by which businesses can challenge individual user reviews.

Rather than sue, it may therefore be wiser to use built-in mechanisms on review sites to ask that such posts be removed. The results may not be speedy, but it is likely less expensive than trying to sue the review site or the patient.

## GENERAL POLICY GUIDELINES

Effective social media policies will address the types of risks practices face in social media usage.

These can include general rules, such as prohibiting excessive use of personal social media by employees during work hours, or prohibiting disclosures of PHI. Effective employee training will also be essential, such as providing employees examples of PHI in the social media context.

For example, practices can create a fictional patient and post information about that patient to a social media account, then demonstrate how quickly that information can spread. Alternatively, the practice could play "Find the PHI" with practice employees by using a photograph containing mock PHI. If employees understand how their social media behavior can impact the practice, and how their posts could violate the law, they can develop the instinct to think twice before posting.

Practices may also want to limit employee interaction with patients via social media. Just as the practice might prohibit socializing with patients outside the office, a similar approach can be taken in the social media setting. Doing so can further limit the potential for inadvertent HIPAA disclosures.

For the practice's own social media accounts, only a handful of people should be posting on the practice's behalf. This could be a single person, or a small but coordinated group. These individuals should be educated on the use of the different platforms. They should also be provided with guidance such as how to respond to patient inquiries about matters such as appointment times or test results. A simple statement that, for example, the practice never responds on public forums to such inquiries, but which directs the individual to call the practice or use the practice's patient portal, may be sufficient.

With respect to reputation management, practices should consider encouraging their patients to post positive comments if they had a good experience. When a practice responds to negative comments, it should only do so with several points in mind. First, any public response should be courteous. As with any other public communications, a response to negative comments is part of the practice's public face, and should remain professional. Second, the response should not include any PHI.

For this reason, as with inquiries to a practice's social media account, it may be easier to state that the practice does not publicly discuss patient care, but suggest that the user contact the practice by phone to resolve any issues. Even if the user never calls, it will at least appear that the practice is not being dismissive of a dissatisfied patient. Moreover, such a response neither confirms nor denies that the user is even a patient, and avoids any potential disclosure of PHI.

As with the practice's social media accounts, only approved individuals should respond on the practice's behalf. ◘



### MORE ONLINE

**Three social media offenses to avoid:**
http://bit.ly/1zv6gRe

**ACP issues social media guidelines:**
http://bit.ly/1IWuaN6

**The big problem with most social media policies for physicians:**
http://bit.ly/1tsVquu

*Daniel F. Shay, JD, is a healthcare attorney with Alice G. Gosfield and Associates, P.C., in Philadelphia, Pennsylvania.*