

Avoiding the pitfalls of social media

BY DANIEL F. SHAY, ESQ.



Every month, Dermatology World covers legal issues in Legally Speaking. This month's author, Daniel F. Shay, Esq., is a health care attorney at Alice G. Gosfield and Associates, P.C.

Social media has become a ubiquitous aspect of American life. Many physicians themselves have personal social media accounts, as do their practice staff members. Social media sites can offer a physician practice the opportunity to advertise new services, improve customer relations with patients, and transmit useful information to the public. However, such communications can bring legal risks as well. Likewise, a physician's personal use of a social media website — as well as personal use by the physician's employees or contractors — can create additional problems. This article provides some guidance for dermatologists looking to manage their social media risks. Note that even if you and your practice have no social media presence of your own, you must contend with social media use by employees and have policies in place to protect patient information.

HIPAA considerations

The Health Insurance Portability and Accountability Act (HIPAA) imposes requirements on covered entities (including physician practices) with respect to patients' protected health information (PHI). These requirements extend to electronic PHI (ePHI), and unsecured PHI (uPHI). All PHI which has not been encrypted is considered uPHI, including posts on social media sites. An improper disclosure of uPHI can therefore raise problems under both the HIPAA Privacy Rule and the Breach Notification Rule.

In general, social media platforms are inappropriate methods for communicating PHI to patients. Depending on the specific privacy controls available on the social media site, and the nature of the message itself (e.g., a private message between two users vs. a public post on a physician practice's main social media page), the communication may be visible to anyone with a web browser. So, it is generally a bad idea to respond to a patient inquiry about, for example,

the results of a biopsy on a social media site. A better approach is to respond by informing the patient that, to protect patient privacy, the practice never responds to such requests on public forums, and instruct the patient to call the office or communicate through a secure medium, such as a patient portal.

Does the patient's inquiry on such a medium act as consent for the physician to respond? If the patient has asked on what is obviously a public social media page, have they not "assumed the risk" of the practice responding with their private information? The simple answer is "No." In fact, HIPAA requires that a patient give their explicit, written authorization to post their PHI publicly. This authorization must be in writing, and in a form that meets specific requirements outlined in the Privacy Rule regulations. It cannot be an "implied," verbal, or even written consent if the written consent does not meet the regulatory requirements.

Practice employees should also be prohibited from posting about patients online to protect against improper disclosures of PHI — and should be trained to consider that their actions on social media platforms might implicate HIPAA.

For example, we had a client whose front desk receptionist posted a photo of a piece of fruit grown by one of the patients, and given to the receptionist. The post was generally positive, discussing how much the receptionist loved where she worked, and how wonderful the patients were. Unfortunately, the fruit sat on top of a daily charge sheet, which included partial views of patient names, telephone numbers, and medical record ID numbers.

Another client discovered that a group of employees had formed their own private social media page on which they gossiped about other employees and administrators, but sometimes also discussed patients, including specifics of the patient's care. While all were

New Practice Management Center



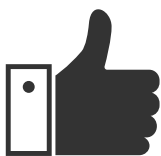
Looking for more help running your practice?

Check out the AADA's new Practice Management Center at

www.aad.org/practicecenter

Likes, Reviews, and You: Social Media Marketing for Your Practice

.....



Learn how to build an effective social media strategy for your practice with this on-demand webinar.

Visit store.aad.org/products/11054.

employees of the practice, the employees were not all involved in the care of the patients discussed, and therefore had no reason to be disclosing the patients' PHI to each other, especially over a social media platform where the information would be stored and could be subject to the platform's own internal data-mining.

Other likely problematic scenarios can include things like employees posting stories about irritating, humorous, strange, or even beloved patients. In the social media context, the employee may not think twice about whether the post contains PHI that could be used to identify a patient. Your job is to make sure that they do.

Online reputation issues

Social media offers businesses convenient methods to communicate directly with customers. However, it also allows customers to post about their own experiences, either on the business's social media accounts, or through online review sites. While some customers may be happy to post about their positive experiences, many will post about negative experiences.

Negative reviews can present several problems for physician practices. A physician may be tempted to respond in several ways. For example, he or she might want to refute the negative review by pointing out the patient's lack of understanding regarding the quality of the actual care received and explain why the care was actually appropriate and proper. Alternatively, the physician might attempt to apologize to the patient and address the specifics of the patient's complaint. While either might be permissible for other businesses such as restaurants or general contractors, within the health care environment such responses may violate HIPAA as well as state confidentiality laws if the responses contain too much information about the patient. As discussed above, a negative (or positive) review also does not waive the need for a specific authorization to reply under HIPAA, if the reply will disclose any PHI.

Moreover, there are good business arguments against such responses. A response refuting the patient's review might come across as hostile, and thereby paint the practice in just as negative a light as the patient's initial review. A response apologizing could become evidence in a malpractice case that the physician acknowledged having erred. A better approach may be to simply adopt a policy that all re-

sponses to patient reviews must state that the practice never responds to specific complaints or comments in a public forum, so as to protect patient privacy, but encourages dissatisfied patients to contact the practice by phone to discuss their concerns. Such a response (1) does not reveal confidential information about the patient (it does not even acknowledge whether the poster is a patient), (2) does not actually acknowledge any wrongdoing, (3) offers the patient a mechanism by which they may be able to resolve their concern, and (4) may appear to the public that the practice is at least attempting to resolve patient complaints.

False reviews present a different problem entirely. A review might claim that the patient had a bad experience when the individual was never a patient in the first place. Likewise, the reviewer might claim to have received services which the practice does not offer (e.g., "The doctor refused to prescribe the drugs I need for my back pain," posted on a dermatologist's page). When a review is entirely false, a physician may want to strike back, such as by flatly denying that the individual is even a patient (e.g., "We don't provide these services!"), or attempting to sue for defamation.

Lawsuits in this arena, however, have proven extremely difficult. Defamation suits generally require (1) that the information posted be false, (2) that the false information be publicly stated, and (3) that the false statement cause actual harm to the plaintiff. Online review sites have generally avoided liability for reviews posted by their users, usually based on federal and state law protections. Suits against individual users have been filed, but are often extremely expensive to pursue. One of the main problems comes in even identifying the defendant in such a case. In many cases, users post under a fictitious name or a user ID. To identify the individual, the practice would likely have to file a defamation lawsuit against an unknown plaintiff, and subpoena the individual's account details from the review or social media site. The practice would also have to demonstrate that its reputation was actually damaged by the false post or review, and to quantify that damage in a dollar amount.

All of these efforts would likely be difficult, expensive, time consuming, and offer no guarantee of success. Moreover, they may not even be necessary. False or negative posts on the practice's own social media



Social media dos and don'ts

Do



Respond to social media inquiries and negative reviews by indicating that the practice does not answer such requests to protect patient privacy but would be happy to respond to a phone call or email.



Warn employees against social media posts containing any form of protected health information.



Consider appointing a staff member to oversee social media in the practice.

Don't



Respond to patient-specific inquiries on social media.



Respond to negative reviews on the review site.



Establish social media relationships between providers and patients.

page can simply be deleted by the page's administrator. Review sites may also offer mechanisms by which the practice may request that a false post be removed. For example, our firm represented a practice that had a false review posted about it, which claimed that the physician who owned the practice had improperly performed a procedure entirely outside the scope of his specialty. The practice submitted a take-down request to the review site, pointing out that the practice did not even offer such services, and the offending review was removed.

Another effective way to counteract the impact of negative or false reviews is to ask satisfied patients to post positive reviews or comments. However, the practice should not offer anything of benefit to the patient in exchange for doing so, since such an offer might run afoul of state or federal laws. Physician practices should also consider whether it is even worth acknowledging a negative review. If the review itself is poorly or unintelligibly written, if the complaint is about an issue of no real consequence (e.g., "I had to wait 10 minutes to see my doctor!"), or if the negative review is heavily outweighed by positive reviews, prospective patients browsing the site may simply ignore it.

Practical tips

Physician practices need effective policies and procedures to address the issues posed by social media. Consider appointing a specific employee as the "social media manager" for the practice. This individual would have responsibility for managing the practice's social media accounts, and would be the only individual authorized by the practice to communicate with the public through social media on the practice's behalf. This approach can help centralize and coordinate the practice's social media messaging, and may help to reduce the risk of employees interacting with patients in an inappropriate manner.

Practice social media policies should also address whether practice employees may connect with patients through their personal social media accounts. In general, it is a good idea to prohibit such activity altogether. This position, however, may prove difficult to actually enforce without access to the employees' personal accounts. Enforcement would rely on self-policing and receiving information from other employees. In addition, practice policies should advise against providing online diagnoses, or offering medical advice. Physician practices should also avoid establishing physician/patient relationships with non-patients through online interactions, as even minimal contacts have used to establish a physician/patient relationship in malpractice lawsuits. For example, a telephone call by on-site staff to an off-site physician has served as the basis for establishing such a relationship, even when the physician never interacted with the patient at all. It is not hard to imagine how a similarly minimal contact over social media could do the same.

Physicians should also review state licensure requirements regarding personal relationships with patients, and professional society ethical rules on such issues. For example, the Federation of State Medical Boards has drafted Model Policy Guidelines for the Appropriate Use of Social Media and Social Networking in Medical Practice. This document advises that physicians should not use their professional position to develop personal relationships with patients, advises physicians to avoid portraying unprofessional depictions of themselves on social media

One More “Do”



Follow the AAD on social media at **@AADMember** on Facebook and Twitter.

websites, and instructs physicians not to use personal social networking sites to interact with patients when discussing the patient’s treatment. Similarly, the American College of Physicians’ Ethics Manual (6th ed.) includes guidance relating to the physician’s duty to maintain effective boundaries with patients. The guidance instructs physicians to be careful of blurring the lines between professional and personal relationships, and to be aware of privacy settings on social media platforms to help ensure patient privacy.

Conclusion

Social media is a fact of modern life. As more and more people use social media — including patients, physicians, and physician practice employees

alike — physicians will need effective policies and procedures to address how their practice and their employees will use social media. The HIPAA regulations require that physician practices establish policies and procedures that address the use of ePHI; such policies should therefore also address ePHI within the social media context. Even if a physician practice intends to maintain no presence on social media platforms, it must still contend with employees’ personal use of social media websites. Developing such policies and procedures may be difficult, without a clear understanding of the legal implications of social media usage within the health care context. Attorneys can help in this regard. *dw*

Discover the power of
True PartnershipSM

LEVERAGE YOUR PRACTICE’S SUCCESS.

QualDerm Partners helps you maximize your practice’s potential. We’re a dermatology practice partnership company that provides the management support, capital and guidance for sustainable growth and profitability. QualDerm’s True Partnership model gives you the benefit of being part of a larger, support-driven organization while preserving your clinical autonomy and practice brand.



Contact QualDerm to learn more about partnership opportunities or to discuss selling your practice.

QualDerm.com
info@qualderm.com
615.250.6723
5203 Maryland Way, Suite 200
Brentwood, TN 37027