The rapid emergence of social media in the past five years has been accompanied by a flood of individuals and businesses in every industry seeking to use new tools to communicate with peers, family, friends, colleagues, and potential customers. Although the healthcare industry has been slow in adopting social media, the rate of adoption has increased in the past two to three years.

Healthcare's reluctance to adopt social media has been driven largely by concerns about the risks it poses to organizations. Social media can, for example, make it easy to violate patient privacy, potentially exposing individuals and practices to sanctions for violations of the Health Insurance Portability and Accountability Act (HIPAA) privacy rules and state laws. Similarly, the very attributes that make social media attractive—its immediacy and interactivity—can lead to users saying things either in their own names or on behalf of practices they represent that cause serious reputational damage.

Accompanying those risks, however, are significant potential benefits. As consumers increasingly flock to social media for guidance about their health, healthcare providers can take advantage of new tools to reach consumers who they may not otherwise have been able to communicate with. Whether their goal is to promote community health or to increase market share, healthcare organizations of all types are increasingly adding social media to their communications arsenals. As their colleagues move into this arena, competitive pressures will likely lead to more and more providers following suit, lest they be left out.

This Guidance Article provides basic definitions for social media and social networking, an overview of current usage among healthcare consumers and providers, and guidance on creating a social media plan, policies, and procedures to manage specific risks inherent in social media use by healthcare organizations.
With all this social media use, there is a clear demand from consumers for healthcare-themed social media content. Health-related information has long been the number-one category of Internet searches and use, according to a February 2011 report from the Pew Internet Project, which called the Internet “the de facto second opinion.” (Szokan)

Social media is a significant factor in how patients use the Internet for healthcare. A February 2011 study from the National Research Corporation found that 41% of nearly 23,000 respondents said that they use social media to research healthcare decisions, with nearly all those respondents—94%—saying that Facebook was their primary source, followed distantly by YouTube at 32%. Respondents to the survey also indicated that they trust social media, with nearly a third of respondents saying that their trust is “high” or “very high”; one-quarter of respondents said that the information they find via social media is “very likely” or “likely” to influence their decisions. (Cohen)

Healthcare Providers’ Use of Social Media

Nurses, physicians, and other healthcare providers are frequent users of social media, both personally and professionally; likewise, healthcare organizations of all sizes use social media as a significant part of their marketing and public relations plans.

In a 2011 survey of 1,100 nurses, for example, only 16% reported that they did not use any social media, while more than 68% reported that they use Facebook, with high percentages also using YouTube (44%) and LinkedIn (37%). A smaller, but still significant, number reported using Twitter (11%). (Springer)

Like the nurses, an August 2011 survey of physicians found that 87% use at least one social media site personally and that 67% do so professionally. As with nurses, Facebook was most likely to be used by doctors on a personal basis and Twitter the least likely. (Dolan)

Although reliable data on how many healthcare organizations use social media is generally unavailable, data for hospitals is compiled by Ed Bennett, the manager of web operations at the University of Maryland Medical Center in Baltimore. On his private website (see Web Resources), Bennett has maintained a list of hospital social media use since at least 2008; the most recent data shows that more than 4,000 social media sites were owned by 1,229 U.S. hospitals as of October 2011 (Bennett). Since, for the most part, Bennett relies on hospitals to self-report their activity, this likely underestimates the total presence in a field that changes daily. His website includes more detailed information by state and breakdowns by types of hospitals (e.g., children’s hospitals).

Physician Social Media Use

Most hospitals use social media as an extension of their existing marketing and public relations plans. Posts and updates tend to revolve around themes such as sharing news about the organization and its services, sharing general medical news, highlighting the organization’s community events, sharing “success stories,” and doing basic customer outreach and engagement. Unlike hospitals, which use social media as corporate entities, physicians who use social media often do so on their own behalf as individuals, possibly blurring the lines between their personal and professional lives. Nonetheless, a 2011 research letter suggests that physicians use Twitter to promote similar information to that of hospitals, despite their differences. The researchers looked at the 20 most recent English-language tweets from 260 physicians who had at least 500 followers, reviewing 5,156 tweets in total. (Chretien et al.)

Nearly half the studied tweets focused on health or medical information, such as linking to studies and essays on healthcare and the practice of medicine. More than 20% were personal communications. Roughly one in seven—14%—were retweets, or forwarding of another user’s message, and a similar number were purely self-promotional. Only 1% of the tweets were about medical education. (Chretien et al.)

In 2010, the American Medical Association (AMA) issued a policy statement to help guide physicians in their use of social media; a similar statement was issued in 2011 by the National Council of State Boards of Nursing (see “Web Resources”). For more information about AMA’s policy statement, as well as findings from the research indicating how physicians often failed to meet the policy statement’s standards, see AMA’s Social Media Policy.

Creating a Social Media Plan

Although the presented data indicates that social media use in healthcare is growing rapidly, many hospitals fail to take full advantage of such tools. These hospitals may end up wasting already-scarce time, energy, and financial resources, ultimately making a mistake more damaging than any of the legal pitfalls discussed later in this Guidance Article.

To ensure that they do not end up falling into the trap of wasting time, practices and individuals using social media must develop a plan. Although practices can start slowly with social media use—creating a Twitter account, for example, as a way to experiment with and understand social media—they must not do so haphazardly. A disorganized approach to social media will be obvious to other users and will damage the organization’s credibility and reputation.

Practices can start by identifying goals. Will the practice limit itself to passively monitoring social media, or will it be an active participant in the social conversation? Is the audience likely to understand social media? Will the practice’s social media presence be obvious to other users and will it damage the organization’s credibility and reputation?

Based on the answers to these questions, the practice will be able to identify the right tools to use and identify the resources and personnel who will be in charge of monitoring them and updating content, as appropriate.

Finally, the practice will set policies—ground rules for how staff will use these tools to achieve the organization’s goals and manage privacy, reputational, and other risks discussed later in this Guidance Article.

Define Level of Engagement

A key initial decision for any organization beginning to use social media is to define its level of engagement. In most cases, this is not actually a choice between two or more levels of engagement; rather, it likely begins with a passive approach and builds toward fuller application.

An early passive approach includes activities such as setting up profiles and looking for mentions of the facility, particularly on networks like Twitter. The facility may already be doing this with the general media, monitoring local newspapers and TV and radio for stories—good or bad—about the organization, and early social media engagement can simply be an example of this approach.
extension of that activity. Most tools, including Facebook and Twitter, actively facilitate this kind of brand awareness. If users see that the organization has a profile, they are likely to go to that profile or “tag” it in a way that the organization is notified. Monitoring other sites, such as blogs, requires more work, such as setting up alerts in Google so that the organization will be notified when a search term—a physician’s name, for example—is used.

This kind of passive monitoring can be an effective way to learn about social media tools as well. Before committing to a more active engagement, the practice can get a chance to see how the tools are used by thought leaders in the community, local media, and industry. Having developed a basic understanding of the various social media, the organization can plan to become a more active contributor. This usually begins with sharing other peoples’ content as described above, including general healthcare news or local media stories about the hospital, its staff, and its patients.

Beyond sharing others’ work, providers and practices willing to invest greater resources may consider creating original content. This could include hosting a blog or creating a YouTube channel where videos can be posted. This content can be an extension of an existing marketing plan, but it does require additional resources and a commitment to follow through. New content will have to be created regularly, and sporadic posting will be seen as a half-hearted commitment to participation and will damage the provider’s or practice’s credibility.

**Define the Audience**

A key part of determining the level of engagement is defining the audience that the practice will use social media to communicate with. Defining the audience will also help the practice choose which tools to use, as discussed below.

Part of the audience could be internal—staff and current patients, for example. In this case, the practice could make announcements about weather delays or emergency disaster response, such as in the case of a hurricane or blizzard; promotions, awards, and other staffing events that might also be announced in a staff newsletter; and any news, activities, and events of interest primarily to internal staff.

Part of the audience could be external—the community, potential patients, and future staff. In this case, practices would still likely discuss activities and events that they would share with internal staff, but they may also share general healthcare news. In using social media to talk to external audiences, practices can think of all the things that they might engage in as part of existing community outreach and then talk about them in a new place, in a new way, to more people. The message a practice shares via social media is not different; only the specific tool to share it changes.

**Identify Resources**

The organization has decided on the nature of its social media engagement and its audience, the organization must choose which social media tools to use to achieve those goals. Table 1. Choosing the Right Medium displays a simple matrix for identifying which common tools will work for various goals.

Making this decision is not as simple as finding a line in a table, of course. Those responsible for social media will need to try several tools, learn what others in their communities are using, and find a comfort level. The practice will likely need to use several of these tools—maybe even all of them—to achieve a comprehensive social media plan.

**Define Authorized Users**

The social media plan should identify who is authorized to use social media on behalf of the practice. An individual should be made accountable for social media and have responsibility for posting content, monitoring usage, ensuring overall execution of the social media plan, and monitoring for policy violations. Although the responsible person will want to bring others into the process to establish a diverse voice for the public—and any person is ultimately responsible for the content that they post—the accountable individual retains overall responsibility for the plan.

Before others are asked to participate in the organization’s social media plan, the practice should define who is authorized to participate. Will authorized use be limited to senior staff? a subset of clinical staff? What, if any, training will be required before people can participate? When is permission required to participate or review required before an individual post can be published? Answers to these questions will be important for those who have accountability and important as well for other staff who may be eager to participate, even if the organization does not want them to. Most important, staff should not be left guessing whether they are permitted to participate in social media on the practice’s behalf.

Finally, all staff, including those who are explicitly permitted to participate in social media, should be educated about the social media plan and policies. Because individuals are likely using social media personally at home, they could be inclined to try to participate in the official social media, even if they are not supposed to. By educating them about the overall policy, staff will not be in a position to claim that they do not know of the policy or that there is no policy in place.

Social media training is also an opportunity to remind staff of any existing general Internet usage policy, which should help to alleviate concerns about staff members wasting time on social media or spending too much work time on personal pursuits. Personal social media use during work hours can be treated like all other personal Internet use, consistent with existing policy and culture.

**Privacy Concerns**

An attractive feature of social media, particularly in marketing and regardless of the industry, is its promotion of storytelling, which can be a powerful technique for conveying complex information and for driving change. But because it promotes information sharing, social media presents significant privacy concerns, specifically violations of the HIPAA privacy rule. Social media may make privacy violations more concerning than they might otherwise be because they distribute information instantaneously to a wide audience and because, unlike verbal conversations, the use of social media creates a permanent electronic record that is likely discoverable in litigation. Numerous examples demonstrate how nurses, physicians, and other providers have violated patients’ privacy rights and how risk managers can take steps to help lower the likelihood of violations.

In one case, two nurses from a Wisconsin hospital independently photographed a patient’s x-ray; at least one of the nurses posted it on her personal Facebook profile. An anonymous caller alerted local police to the photo’s presence and an accompanying discussion among the two nurses. Although the photo was deleted before the authorities could verify that it was there, the two nurses were fired immediately. The nurses’ actions apparently did not violate state law at the time, but their actions clearly violated federal privacy protections under HIPAA. Although the nurses faced action from the state licensing board in addition to termination from their jobs, the hospital likely saved itself from sanctions and liability because of its swift action in terminating the nurses and its thorough, well-documented HIPAA privacy training for employees. (“Facebook Firing“)

Other more recent cases include an Oregon nurse aide who was jailed for eight days following a series of Facebook posts that included identifiable photos of patients (Duara) and an agency nurse at a California hospital who was disciplined after he posted photos and disparaging comments regarding a patient who came to the emergency department seeking treatment for a sexually transmitted disease (Thielst).

These cases emphasize the importance of not only conducting HIPAA training but also documenting that it took place. Risk managers should ensure that HIPAA training includes a specific discussion of social media pitfalls, emphasizing that all workers have a duty to protect patient privacy, even when using their own personal social media profiles.

Policies should clearly address whether and how photos of patients can be taken and used. No photos of patients should be taken or used without specific authorization by the patient. The authorization should specify how the photo will be used (e.g., in a brochure, on a website, for clinical purposes), and staff who might seek to use existing photos for any purpose should check to ensure that the authorization covers a second use.

In another, less overt case, a Rhode Island physician was reprimanded and had her clinical privileges curtailed after she inadvertently compromised a patient’s identity on Facebook. The physician had written about the patient without using the patient’s name or intentionally identifying him or her. However, according to the state medical board, the doctor’s description of the patient’s injuries was specific enough that an anonymous third party was able to identify the patient. According to news reports, the physician was directed to pay $500 in administrative fees to the medical board and attend a continuing education course; in addition, the hospital where the physician treated the patient in question terminated the physician’s privileges. (Associated Press)

Although the physician in this case, unlike the nurses in the previous cases, did not do so intentionally, the state board determined that she violated the patient’s privacy. Risk managers can use this case to emphasize to their staff that even when telling success stories or emphasizing good outcomes, they must tread carefully when describing patients. Risk managers may want to consider a policy that would require review of all descriptions of patients by the risk manager or someone familiar with the HIPAA privacy rules to help
ensure that patients have been sufficiently deidentified. All training should address the consequences of violating patient privacy. Staff should be aware of the penalties that the facility faces for HIPAA violations and know that they face individual discipline for using social media in a way that violates patients’ privacy.

Reputation Management

After privacy, one of the most significant risks that any practice or provider must manage when using social media is that to its reputation. In healthcare, as in any other industry, this encompasses two distinct elements: first, ensuring that the content published or posted via social media accurately reflects the organization’s message and does not harm its reputation; and second, being aware of and responding to criticism and complaints that originate outside the organization. The two are closely tied and can typically be managed by ensuring that policies and procedures follow four main practices: staff engaging in social media should be aware of what is being said about them and their organization, be timely in their response, be honest in both responding to outsiders and in creating new content, and be respectful in all communications.

Self-Generated Social Media Harm

Just as they can in real life, providers using social media can say any number of things (e.g., knowingly false or misleading statements, medically inaccurate statements, profanity, racial slurs, sexist statements, direct insults) that will damage their reputations. When providers or their staff forego anonymity and comment using either their own names or the organization’s name, what they say reflects on the organization directly.

There are numerous examples of people—sometimes celebrities, sometimes simply individuals working on behalf of an organization—doing lasting harm by posting crude, inappropriate, or otherwise unprofessional content on social media, usually Twitter. The phenomenon is so widespread it even has its own descriptive term: “self-twimmolation,” or “firing over a quick, ill-advised tweet.” (Poniewozik)

Examples include the comedian Gilbert Gottfried, who made offensive jokes following the 2011 Japanese earthquake and tsunami and was immediately fired from an endorsement program; journalist Nir Rosen, who was fired from a position at New York University after making comments about a female journalist who was sexually assaulted while working in Egypt; an unidentified advertising agency representative who was fired after complaining about Detroit drivers via an account the agency maintains on behalf of the car manufacturer Chrysler, as the manufacturer was launching an ad campaign centering around Detroit; and U.S. Representative Anthony Weiner, who was forced to resign from Congress in June 2011 after sending lewd photos of himself via Twitter to a woman. (Poniewozik; Smith; Hernandez)

To varying degrees, these people did more harm to themselves than they did to the organizations or other individuals they represented. However, considering the case of the ad agency representative who tweeted about Chrysler on a corporate, rather than an individual, account, it is easy to imagine parallel examples that could arise in healthcare organizations, for which reputational harm could be real and lasting. Social media training, therefore, must emphasize repeatedly the need for constant vigilance against unprofessional conduct. See AMA’s Social Media Policy for a discussion of one review of physicians’ tweets and how the physicians fared in avoiding unprofessional, potentially damaging content.

Responding to Negative Posts

No matter how carefully they are in the content they produce, providers also face a risk from social media that they may seem to have no control over—negative posts by others on social media sites can affect the way a provider is regarded, even if the negative posts are not truthful. Whether and how to respond to such negative posts can present a dilemma for providers.

Respond offline. When providers become aware of negative posts, they are best served by approaching the comments as a customer service opportunity. An offline response to the author of the post can give the patient an opportunity to voice his or her concerns directly and, if appropriate, for the physician to take steps to rectify the situation or to correct misinformation.

Share positive stories. Not every patient who posts negative comments online will be receptive to their removal or revision following contact from the provider. To help present a more balanced picture of themselves online, physicians may consider asking patients who have had positive experiences to post their stories online as well.

Create your own online presence. Besides relying on patients to post positive commentary online, providers can help control their online reputation by creating their own sites and profiles and telling their own stories. This approach can have numerous benefits. For example, sites controlled by the provider will likely appear more prominently in online search results than will individual comments or reviews hosted on other sites, helping to drive negative reviews down and making them less likely to be seen by patients searching the physician’s name. Similarly, simply having a professional presence online can be seen as a sign of competence by patients.

In addition to taking active steps to improve their online reputations, providers must also be reminded to avoid common pitfalls that may do more harm than good and, in some cases, expose providers to more risk than the original negative comment.

Don’t ask patients to sign agreements. Some providers ask patients to sign agreements stating that the patient will not post negative reviews or comments online in the event of a bad outcome. Providers should avoid the temptation to propose such an agreement; besides introducing to patients the idea that there are negative reviews online, and likely being difficult to enforce legally, providers risk beginning the provider-patient relationship on a negative note, focusing on potentially negative outcomes rather than achieving positive outcomes.

Don’t make up positive stories. While it may be helpful to ask patients with positive experiences to post online about their stories, providers should resist the temptation to post false stories online anonymously. As with all social media use, providers need to assume that the truth will eventually come out and that their reputations will be significantly damaged if patients perceive them as dishonest.

Don’t respond to clarify negative posts. Providers should resist the temptation to respond to negative posts publicly to “clarify” their role or side of the story. Such clarifications run the risk of privacy violations. In addition, the conversation online could quickly devolve into a name-calling, he-said-she-said debate, where each comment will only serve to further damage the physician’s reputation.

Save lawsuits for extreme situations. Providers may wonder whether they can sue patients for defamation or other claims when the patients post false information online. In at least a handful of situations, this tactic has worked for providers. One prominent case emerged in late 2011, when a pair of Arizona plastic surgeons sued a former patient for defamation and ended up winning a $12 million verdict. In that case, the patient suffered an infection after she sought care from the surgeons. The injured patient questioned the two surgeons’ credentials and started a website dedicated to criticizing them. The surgeons sued her in 2008 as soon as the website launched. The patient complied with a restraining order to delete the site, but she followed it with a focused campaign to damage the physicians’ reputations by commenting on numerous online sites, lodging professional board complaints, and attending public meetings, all with the intent of ruining the practice. The campaign worked; the surgeons say that they were forced to stop being a $4.5 million practice to seeing one or two patients a week. Their lawsuit took three years to resolve, but they eventually prevailed, with a jury awarding them $11 million in actual damages and $1 million in punitive damages. (Gallegos)

Although the verdict was seen as a “triumph for doctors who often feel powerless when patients take to the Web and write untrue posts without facing consequences,” according to the surgeons’ attorney (Gallegos), physicians should be cautious when considering litigation. In cases where a single negative review or post is at issue, providers may be less likely to prevail. More importantly, physicians who sue patients over seemingly minor posts may do more damage to their reputations if they are perceived to be “going after” a patient than the initial post itself would have caused if left unanswered. Legal action should be reserved for extreme cases.

Other online responses. Besides clear-cut criticisms and compliments, providers are also likely to receive inquiries from consumers about the kinds of services they offer, their location and hours, and even their handling of specific medical conditions. For guidance on responding to these inquiries, see Repealing to Inquiries and Establishing Terms of Use.

Whatever their response is, providers must always maintain a courteous, professional attitude. There is no benefit to be had from insulting or demeaning anyone. Providers and their staffs must also explicitly be reminded that they cannot lie. If a staff member has been dishonest and the truth does come out, the resulting damage to the organization’s reputation will be significant.
Emerging Social Media

An important point for providers is that the risks posed by social media use will likely remain the same regardless of which medium is employed in a given situation. A well-designed social media plan should not focus on any particular media, but rather should be flexible and scalable enough to accommodate new social media and other tools that may emerge. This is particularly important because of the rapid nature of growth among social media—they may seem to appear out of nowhere, and providers will not be able to rewrite plans quickly enough to keep up with the rapidly changing technologies.

Social media that were emerging as of early 2012 and that will require risk management attention if they become more popular include the following:

**Google+,** A direct competitor to Facebook, Google+ launched in a beta version in the summer of 2011 to a limited number of users and has since become publicly available. It features many, but not all, of the same features as Facebook, including status updates, video and photo sharing, and the ability to link to and comment on content from outside websites. Google+ claims that it has greater privacy control than Facebook by making more prominent the ability to group friends into circles and determining which circles can see each status, photo, link, or other post. As Google+ becomes more prominent—and sooner, for providers who may be among early adopters—providers must be reminded that all the same precautions that can be taken on Facebook apply to Google+ and that users should not be lulled into a false sense of security by the service’s privacy claims. The privacy settings, after all, are dependent on a user to set them properly, and, as with anything Internet-based, are subject to hacking, viruses, or other unexpected problems. Users should not assume that they can share content only with certain circles in hopes that it will remain private permanently—content that is inappropriate to post is always inappropriate to post, regardless of the setting.

**Foursquare, SCVNGR, and Facebook Places.** These location-based social media focus on users checking in to various locations from global positioning system-enabled devices and, in many cases, offering reviews. Providers should be aware if their marketing team establishes a presence on any of these platforms and be aware of the specialists that may be offered to ensure that they do not raise any concerns. Likewise, providers should be aware of comments and reviews left on these sites about them.

**Quora and Yahoo Answers.** These sites bill themselves as user-organized question-and-answer sites where members may ask questions and the community drives the best answers to the top. Providers should carefully consider the risks before participating in these and similar sites in their professional capacity, particularly the risks associated with offering medical advice through these services.

**Groupon and LivingSocial.** These sites offer daily deals that represent deep discounts for goods or services, such as 70% off a pair of shoes or three-for-the-price-of-one cups of coffee. Besides run-of-the-mill consumer discounts, significant discounts are offered for medical services such as laser hair removal or laser eye surgery. While private-pay providers such as these may not implicate risk management concerns, any attempt to offer discounts on federally reimbursable services would trigger corporate compliance concerns and should be prohibited.

**Patient portals and apps.** As they grow more technologically advanced, hospitals and other organizations may develop increasingly sophisticated portals of their own or even apps for devices like smartphones and tablet computers. These portals or apps could include services such as the ability to communicate with physicians, make appointments, manage health records, or view test results. Such portals implicate all the risk management concerns discussed throughout this Guidance Article, and risk managers should be included in plans for the development of such services.

**Action Recommendations**

- Develop a social media plan that outlines the organization’s goals and intended audience in using social media.
- Assign an individual or group accountable and responsible for posting content, monitoring usage, ensuring overall execution of the social media plan, and monitoring for policy violations.
- Define which social media tools will be used to support the various goals listed in the social media plan.
- Include social media in all HIPAA privacy training, and include information on the obligations HIPAA imposes on staff and volunteers in social media training. Consider having staff sign a form indicating that they completed privacy training and that they understand the consequences for failing to protect patients’ privacy.
- Ensure that privacy policies specifically address the use of photos of patients, staff, volunteers, and visitors and that use without authorization is prohibited.
- Monitor social media for mentions, positive or negative, of the organization.
- Establish a policy that defines whether and how the organization will reply via social media or other means to criticism, complaints, and compliments that appear on social media.
- Remind users of social media that they must, in all circumstances, be honest and respectful toward other users.
- Create policies that are general and flexible enough to adapt to emerging social media without requiring constant updating.

**REFERENCES**


Facebook forges show privacy concerns with social networking sites. *Healthc Risk Manage* 2009 May;31(5):49-52.


RESOURCE LIST
American Medical Association
(800) 621-8335
http://www.ama-assn.org


National Council of State Boards of Nursing
(312) 525-3600
http://www.ncsbn.org


Social Media Health Network
Mayo Clinic Center for Social Media
(507) 538-1092
http://network.socialmedia.mayoclinic.org/


ADDITIONAL MATERIALS
AMA's Social Media Policy

In 2010, AMA published a policy on physician professionalism in the use of social media that emphasizes many of the risks physicians face and the steps physicians should take to minimize them. AMA acknowledges the many possible benefits for physicians in the use of social media but advocates a cautious approach. The policy applies equally well to hospitals and other organizations, regardless of the care setting.

AMA's policy has six main points, as follows:

- Physicians should be cognizant of standards of patient privacy and confidentiality and refrain from posting identifiable patient information online.
- Physicians should use privacy settings to safeguard their personal information to the greatest extent possible but should realize that privacy settings are not foolproof and can be overcome. In addition, physicians should remember that once information is available on the Internet, it is likely there permanently. Consequently, physicians should monitor their own Internet presence to ensure that the personal and professional information posted about them online is accurate and appropriate.
- Physicians who choose to interact with patients on the Internet must maintain appropriate boundaries of the patient/physician relationship consistent with professional ethical guidelines.
- To aid in maintaining appropriate boundaries, AMA recommends that physicians separate their personal and professional online content.
- Physicians who see content posted by colleagues that appears unprofessional are encouraged by AMA to bring that content to the attention of the individual. AMA further states that if the behavior "significantly violates professional norms" and the notified individual does not resolve the situation, the physician should report the matter to appropriate authorities.
- Finally, AMA reminds physicians that actions online and content posted may negatively affect their reputations, may have consequences for their medical careers, and can undermine public trust in the medical profession.

A 2011 research letter that examined the tweets of 260 physicians assesses, to some extent, how physicians perform in regard to this standard, particularly with regard to ensuring that content posted online maintains a level of professionalism and avoids violating patients' privacy. Unprofessional content was the most frequently observed violation, occurring in 144 of the 5,156 observed tweets (2.8%). Privacy violations were much less common, occurring in 38 tweets (0.7%). Profanity (33; 0.6%), sexually explicit comments (14; 0.3%), and discriminatory statements (4; 0.1%) were even less common.

Interestingly, 27 users were responsible for the 38 privacy violations. All but two of the users who committed privacy violations were themselves identifiable, such as through their full names on their accounts or websites they linked to or through use of personally identifiable profile photographs. In addition, 55 other tweets that were not categorized by the researchers as "unprofessional" included potentially problematic content, such as possible conflicts of interest, unsupported claims about products they were selling, and statements that run counter to existing medical knowledge or guidelines.


Table. Choosing the Right Medium

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Potential Tool</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communicate news or events with patients and families</td>
<td>Private blog, Facebook group</td>
</tr>
<tr>
<td>Show potential patients and families the facilities</td>
<td>YouTube, Flickr, Tumblr</td>
</tr>
<tr>
<td>Make senior staff available as experts</td>
<td>Public blog, Facebook page</td>
</tr>
<tr>
<td>Facilitate staff collaboration on care issues</td>
<td>Instant messaging, intranet</td>
</tr>
<tr>
<td>Share news on the profession with staff at multiple sites, encourage community</td>
<td>Twitter</td>
</tr>
<tr>
<td>Recruit professional staff</td>
<td>Linkedin</td>
</tr>
</tbody>
</table>


Replying to Inquiries and Establishing Terms of Use

When providers establish social media profiles, regardless of the particular tools they use, consumers are likely to use those media as another way to contact the provider with a wide range of inquiries, and providers should have a plan for how they will respond.

Simple questions about hours, locations, or services provided can likely be handled through social media, whether by directing users to a webpage where the relevant answer is or
answering directly. A question, for instance, about which day a provider is in which of her office locations can be answered easily, quickly, and accurately via social media. Other inquiries could be less innocuous. Patients may ask for specific medical advice, for example, or even use social media to reach out to providers in cases of emergencies—instances when social media are definitely not the appropriate tools for responding. All providers and their staffs, whether participating in social media in their own name or on behalf of an organization, should be instructed to never give out medical advice using social media. Doing so may be construed as establishing a physician/patient relationship, and advice that could be alleged to contribute to a bad outcome could become grounds for a lawsuit. Even advice that a caregiver may perceive to be innocuous may not be perceived that way by patients—or juries—and conveying the advice via social media creates a permanent electronic record of the exchange that will likely be discoverable during litigation. Besides educating staff on what constitutes an appropriate response, providers may consider creating public-facing terms of use for every social media tool that they use. Terms of use could specify, for instance, that specific medical advice will not be provided and that patients with emergencies should call 911 or go to the emergency department. Inquiries that are made despite these terms of use can be addressed by directing patients to make an appointment to talk with a provider and by giving detailed information on how to make an appointment. This information should be repeated every time a patient asks, even if it is posted elsewhere on the site. Usage policies should address issues in addition to how medical questions will be handled. Any kind of social media tool that invites user feedback—blogs, specifically, but also Facebook—should be accompanied by basic do's and don'ts—reminders to keep on topic, avoid swearing or using ethnic or other slurs, and keep the conversation respectful—as well as an outline of what will be done about offenders. Facilities will need to decide whether they will moderate content on blogs and Facebook pages and, if so, who will do the monitoring and what their criteria will be; how offending comments will be handled (e.g., by deleting them, by moderating before posts are made public to prevent their appearing); and whether repeat offenders will be temporarily or permanently banned from the site. However a provider decides to handle these issues, the answers should be clearly delineated in terms of use, and the policies should be enforced consistently.