Key Recommendations

- Develop a social media plan that outlines the organization’s goals and intended audience in using social media.
- Define which staff may participate in the organization’s official social media.
- Include social media in HIPAA privacy training, and include information on HIPAA in social media training.
- Remind users of social media that they must in all circumstances be honest and respectful toward other users.
- Use employees other than hiring managers to screen candidates’ social media profiles during the hiring process.
- Create policies that are general and flexible enough to adapt to emerging social media without requiring constant updating.

See page 16 for more Action Recommendations.

Supplementary Material

- Table 1. Hospital Social Media Use
- Table 2. Choosing the Right Medium
- AMA’s Social Media Policy
- Respecting Staff Privacy

For more tools on this topic, see the HRC members’ website at http://www.ecri.org.

Social Media in Healthcare

There is no question that use of social media is exploding in the United States and around the world. 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 many risks it poses to organizations. Accompanying those risks, however, are significant potential benefits, most prominently improved patient and community outreach and communication.

WHAT HRC FOUND

Hospitals and other healthcare organizations have begun to use social media in ways that attempt to meet consumer demand. In doing so, they must create and enforce social media plans that define how engaged the organization will be, who its audience will be, and who will be responsible for managing social media outlets, as well as establish policies and procedures for managing risks related to privacy, reputation management, and employment issues.
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 many risks it poses to organizations. Social media can, for example, make it easy to violate patient privacy, potentially exposing individuals and the organization 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 organizations they represent that cause serious reputational damage.

Accompanying those risks, however, are significant potential benefits. As consumers increasingly flock to social media for every aspect of their lives, including guidance about their health, healthcare providers and organizations can take advantage of new tools to reach consumers 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 are increasingly adding social media to their communications arsenal. As their colleagues move into this arena, competitive pressures will likely lead to more and more organizations following suit, lest they be left out.

This Risk Analysis 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, both as a provider and as an employer.

**WHAT IS SOCIAL MEDIA?**

Because social media is a recent phenomenon, one that is largely technology driven and given to buzzwords, the terminology used to describe it can be confusing, particularly for new users. Therefore, risk managers and others must ensure that they are using common definitions when working on social media plans.

First, risk managers should understand the distinction between the terms “social network” and “social media.” Although they are often used interchangeably, they have distinct meanings: a social network describes a group of people, whereas social media are the tools people use.

The idea of a social network is not new, even if the phrase is only recently in vogue in popular culture. Simply put, a social network is a group of people linked to each other by one or more common attributes, such as family, friendship, interest (i.e., hobby, industry, career), or even alma mater. Most people belong to many social networks based on those attributes.

Although social networks are not new, the technology that has sprung up in the past decade that lets members of various social networks connect in different ways is new. These tools, collectively, are referred to as social media; they are characterized by a fluid shift in roles between the author and the audience that encourages feedback and interaction (Kaplan and Haenlein).

**Major Kinds of Social Media**

Social media is a nearly endlessly broad term. New technologies and tools come and go every day, so any attempt to capture a comprehensive list of social media...
Blogs. Blogs, short for “weblogs,” are websites where an author or group of authors can post articles that encourage reader feedback. Although they are popularly associated with opinion-based writing, blogs can be built around many kinds of writing, including research-driven, nonopinion content. The defining characteristic of blogs is not the type, style, or content of writing; rather, it is web-based functionality that provides for open-ended interaction between the author and the reader in the form of comments and replies.

Microblogs. Microblogs function similarly to blogs, in that authors publish content with the intent to spur reader feedback or interaction. However, while traditional blog posts may be of any length, microblog posts come with a constraint on length. The most famous microblog is Twitter, which limits posts to 140 characters; on Twitter, posts are called “tweets.”

File-sharing sites. Many social media sites are based on concepts that emphasize sharing files of various media. Common examples are YouTube, which houses videos, and Flickr, a photo-sharing site. There are many others focused on all kinds of media—music, photos, videos, slide presentations, and more. What unifies them is the idea of a “social” element that invites user feedback by way of user comments and offers tools so that users can recommend or share files.

Integrated social media. Some social media sites integrate many kinds of social elements. Facebook, for example, combines microblogging through its “status” update, full blogging through its notes feature, photo and video sharing, and much more, such as groups and marketing pages that can be created and shared among groups of friends with more or less open access. LinkedIn is similar and has many of the same elements as Facebook but a decidedly different focus—rather than “friends,” LinkedIn is organized around professional relationships. Google+, a recently launched service, is another example.

Location-based social media. Finally, a handful of sites, most prominently Foursquare and Gowalla, allow users to check in to locations from GPS-enabled devices such as smartphones. Location owners, including hospitals, can claim locations and offer specials based on check-ins and other loyalty-based rewards; users also earn points for check-ins and compete with one another.

These are just a handful of examples. There are hundreds of others, some focused on hobbies and interests, specific industries, or any number of other characteristics. Although risk managers will not be able to maintain an awareness of or participation in all the various sites that emerge, they must be aware of the most common services, particularly those that are likely to be used on behalf of their organizations. “Resource List” includes information on websites that offer general social media guidance; risk managers would be well served to follow some of these sites as part of an effort to remain up to date.

The growth of social media

There is no question that use of social media is exploding in the United States and around the world. One June 2010 report estimated that social media use accounted for nearly a quarter of all Internet time logged in the United States (Nielsen Company). Individual services boast staggering numbers of users; Facebook, for instance, announced in mid 2011 that it had passed the 750 million user mark—nearly half of all Internet users worldwide (Facebook). Twitter, which does not regularly release information about its user base, reportedly had more than 190 million users by mid 2010 (Schonfeld).

YouTube, the video sharing site, boasts about 2 billion views per week and says that more video is uploaded to its site every 60 days than the three major U.S. networks—ABC, CBS, and NBC—created in their first 60 years. More than 5 million users subscribe to at least one channel, and more than half of the videos on the service either have been rated or include comments—a testament to YouTube’s social media aspect. (YouTube)

The number of blogs available on the Internet is difficult to ascertain, mostly because, unlike Facebook, Twitter, or YouTube, there is no single major blog provider. One tracking service, BlogPulse, has estimated that there were 154 million blogs and counting as of early 2011, with more than 60,000 new blogs and 800,000 posts added every day (BlogPulse).

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 ORGANIZATIONS’ USE OF SOCIAL MEDIA**

Hospitals and other healthcare organizations have begun using social media in ways that attempt to meet this demand from consumers. For hospital social media, the definitive source of data about use is compiled by Ed Bennett, the manager of web operations at the University of Maryland Medical Center in Baltimore. On his private website, Bennett has maintained a list of hospital social media use since at least 2008; the most recent data, as this Risk Analysis was published, is included in “Table 1. Hospital Social Media Use” and shows that nearly 4,000 social media sites were owned by U.S. hospitals as of June 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); see “Resource List” for information on accessing the site.

Although Bennett’s data shows that social media has not achieved total adoption among hospitals, its growth is substantial. Risk managers in organizations that do not yet maintain a social media presence can expect that their facilities will do so soon—as social media growth expands in the community and among consumers, hospitals will feel increased pressure to communicate and be active in social media.

In settings other than hospitals, little data is available on how healthcare providers are using social media, but anecdotal evidence suggests that all types of providers use social media. Risk managers with responsibility for physician practices and long-term care settings, for example, should anticipate that if those organizations are not yet using social media, they soon will, for the same reasons that hospitals will.

**How Are Healthcare Organizations Using Social Media?**

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. Each of these potential uses is discussed briefly below; their associated risks and mitigation strategies are discussed throughout this document. The discussion Identify Resources outlines how healthcare organizations can choose from among various social media tools based on their goals, the audience they plan to reach, and the information they plan to share.

**Organizational news and services.** Most social media use by organizations, rather than people, starts with sharing news about the organization itself. For healthcare organizations, this is valuable because it provides an opportunity to engage in social media without creating any new content. Rather, the hospital’s social media staff (see the discussion Define Authorized Users) can post links to press releases, advertisements, and other content that has already been created for other uses—raising awareness about the organization and driving traffic to its websites without investing substantial resources.

**Sharing general news.** Most websites offer options to share links to stories via major social media tools, most prominently Twitter and Facebook. Users typically have the option to include comments or messages about the

---

**Table 1. Hospital Social Media Use**

<table>
<thead>
<tr>
<th>Media</th>
<th>Number of Hospitals Using Medium</th>
</tr>
</thead>
<tbody>
<tr>
<td>YouTube channel</td>
<td>548</td>
</tr>
<tr>
<td>Facebook page</td>
<td>1,018</td>
</tr>
<tr>
<td>Twitter profile</td>
<td>788</td>
</tr>
<tr>
<td>LinkedIn page</td>
<td>458</td>
</tr>
<tr>
<td>Blog</td>
<td>137</td>
</tr>
<tr>
<td>Foursquare</td>
<td>913</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>3,952 Social Media Sites</td>
</tr>
</tbody>
</table>

shared article within certain character limits or other space constraints. Healthcare organizations can use this feature, for example, to post links to stories from local or national media such as stories about major studies, legislation, or general-interest health-related stories, along with community-focused stories that may not be related to healthcare but are of interest to the hospital’s patients.

**Community events.** Many hospitals host community events, such as blood pressure screenings, child safety days, or lectures. Some tools (e.g., Facebook) specifically allow the creation of “events” with invited attendees that hospitals can use to promote the events; Facebook and Twitter can also be used to link to promotional materials. After events, sites like YouTube and Flickr can be used to share photos and videos of events.

**Success stories.** Whether they are highlighting a staff member who has received an award or a patient who has overcome long odds to survive a serious illness, healthcare organizations often use success stories as marketing material. Social media provide an excellent venue to promote these stories. Blogs, for example, can provide a venue for patients to tell stories in their own words, and interviews with patients and caregivers can be recorded and posted on YouTube. Although using social media in this way can require more resources—rather than simply linking to existing materials, hospitals must now create new content—sharing success stories can be a powerful marketing strategy.

**Customer outreach and engagement.** Unlike other uses discussed here, which focus on material that the hospital either identifies or creates and then promotes via social media, customer outreach and engagement shifts the hospital’s focus to being aware of what patients and other consumers are saying about the facility and then responding appropriately. This could include, for example, providing a dedicated Facebook discussion forum where patients can ask about the kinds of services that the hospital provides, or monitoring Twitter for complaints about the hospital that must be addressed. For more on this use of social media, see the discussion Reputation Management.

Social media, of course, can be used for much more than marketing and public relations. Uses have been proposed or enacted for everything from disaster management to live coverage of an ongoing surgery. To see how some organizations are engaging in more advanced uses of social media, see “More Than Just Marketing.”

**Physician Social Media Use**

Unlike hospitals, which often 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 1 in 7—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. For more information about the 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.”

**Health Insurers**

Although professional liability insurers are not yet active in social media, consumer health insurers are increasingly active. They use social media for many of the same reasons as hospitals and other corporate users, such as disseminating information, providing customer service, and protecting their brands.

As of early 2011, almost all the activity among the seven largest private health insurers is focused on customer service—making sure “no gripe goes unanswered,” as one writer put it. Health insurers frequently offer “healthy lifestyle” tips to consumers on topics such as smoking cessation, healthy dieting, and preventive medicine. Some use social media for advocacy communications, such as discussing implementation of the Patient Protection and Affordable Care Act of 2010. (Berry)

Health insurers and other insurers—and defense lawyers—use social media to find information about patients and plaintiffs. For example, defense attorneys and insurers will look at a patient’s social media to see if
More than Just Marketing

Although its most obvious and most common use among healthcare organizations may be marketing, social media has many other potential uses. One nurse has posited 140 additional uses for Twitter in healthcare, some of them public-facing, some of them among providers. They include ideas like recruiting blood donations, communication during disasters, weight management and support, epidemiological tracking, arranging outpatient care, real-time satisfaction surveys, adverse event reporting, and food and product safety alerts. (Baumann) Not all of his ideas will work for all patients or in all settings, but they can serve as useful thought-starters for organizations seeking to branch out in their social media use.

For example, in a few instances hospitals have allowed clinical staff to use Twitter to publicly share commentary in real time about an ongoing surgery (Belluck; Cohen; Parker-Pope). Unlike harmless tweets, like links to press releases, real-time updates from the operating room (OR) pose more complicated issues. Will the surgeons be fully focused on the patient if they are also dictating tweets? What if complications arise during surgery? If other media are used, like live webcasts, what if inappropriate information or images are inadvertently included? Risk managers will need to help develop plans to ensure that appropriate consent or authorization is obtained; that state and federal privacy laws and regulations, including those under HIPAA, are followed; and that plans are in place to terminate the session if complications develop during the procedure.

For example, some hospitals have implemented plans that allow them to gently break away from live Twitter commentary in the event of dire complications. Similarly, one hospital that webcasts surgeries keeps recordings of previous procedures available on stand-by in case the camera in the OR needs to stop filming. (Belluck) Despite concerns that patients’ families may be uncomfortable with sharing of their loved ones’ information via Twitter, one family of a pediatric patient welcomed live coverage of her surgery as a way to keep the family informed during the procedure and reduce anxiety in the waiting room. Even in this case, however, the nurse tweeting the surgery could have been ordered out of the OR at any time had complications emerged. (Parker-Pope)

One ethicist, however, notes that hospitals should not strictly avoid all mention of complications. “If you don’t show the bad along with the good, people can end up misinformed or with excessively optimistic expectations,” states E. Haavi Morreim of the University of Tennessee College of Medicine (Memphis) (Belluck).

References


Anything posted there will invalidate claims, such as if a patient is engaging in activity that would be impossible given the injuries that they are alleging. (Berry) In one case, however, such postings were barred from discovery by a Pennsylvania judge. In that case, the plaintiff was a passenger in a car driven by the defendant. The car was in a one-car accident, the plaintiff suffered lacerations to her lip and chin from her impact with the airbag, and she alleged that she suffered permanent scarring. Although the defense was given access to photos of the plaintiff before and after the accident, the defense sought access to a photo and status update posted on the plaintiff’s private Facebook profile. The judge denied access to this photo; he noted that although there was no specific privilege from discovery for the content under Pennsylvania law, the defendant already had “all the photographs she can reasonably use from every different period before and after the accident and she has not asserted that there is likely to be any text in the non-public postings that is material or will likely lead to the discovery of material evidence” and that allowing the information to be discovered would “cause unreasonable annoyance, embarrassment, oppression or burden” as defined by state law. (Passarella)

Creating a Social Media Plan

Although the presented data indicate 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
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.

to other users and will damage the organization’s credibility and reputation.

Organizations can start by identifying goals. Will the organization limit itself to passively monitoring social media, or will it be an active participant in the social conversation? Is the audience internal—existing staff, clients, and families—or external—the local community?

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

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

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 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—the hospital 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 organization 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 other peoples’ work, hospitals willing to invest greater resources may consider creating original content. This could include hosting a blog with contributions from the hospital’s staff or creating a YouTube channel where videos can be posted. This content can be an extension of the 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 organization’s credibility.

Define the Audience

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

Part of the audience could be internal—the organization’s staff and current patients, for example. In this case, the organization 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 made 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, organizations would still likely discuss activities and events going on at the organization that they would share with internal staff, but they may also share general healthcare news. In using social media to talk to external audiences, organizations 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 an organization shares via social media is not different; only the specific tool to share it changes.

Identify Resources

Once 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 2. 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 of 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 organization 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 organization. An individual or group within the organization 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 or group will want to bring others from the organization into the process for individual elements of the social media plan to establish a diverse voice for the public—and any individual is ultimately responsible for the content that they post—the main group retains overall responsibility.

Before others are asked to participate in social media, the organization 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 organization’s behalf.

Finally, all staff, including those who are explicitly not 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 organization’s 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 the facility’s 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, use of social media creates a permanent electronic record that is likely discoverable in litigation. Numerous examples demonstrate how nurses, physicians, and other hospital employees have violated patients’ privacy rights and how risk managers can take steps to help lower the likelihood of violations. For a more detailed discussion of HIPAA privacy regulations in general, see the Risk Analysis “Health Information Privacy Standards,” in the Laws, Regulations, and Standards section of the Healthcare Risk Control (HRC) System.

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 Firings”)

The case emphasizes 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.

In another, more recent 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 Wisconsin nurses, 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.

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.

Finally, 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 individually face discipline for using social media in a way that violates patients’ privacy. The Wisconsin nurses and the Rhode Island physician can be used as examples.

Risks from Former Employees

Risk managers may become aware that groups of former employees or volunteers are using social media to talk about the organization and that some of their conversations may violate patient privacy. It is unlikely that the hospital can be sanctioned for potential HIPAA privacy rule violations that occur after employment ends or a volunteer is no longer working for the hospital. Because the HIPAA privacy rule refers to the “workforce” and “staff,” former employees or volunteers are not explicitly covered (HHS).

It is possible, however, that a healthcare organization could be sanctioned for privacy violations that occur after employment ends if it can be shown that the organization did not properly educate its staff or volunteers regarding their HIPAA obligations. To mitigate this risk, HIPAA education, including a clear definition of what constitutes protected health information, should be mandatory for all staff and volunteers and should include a reminder that their obligation to protect a patient’s privacy continues after their employment or volunteer time ends. Employees should sign an acknowledgment that they received the training and understand their obligations.

When risk managers become aware that violations have occurred among former employees, they may consider having the facility’s legal counsel identify the individuals responsible for the violations and notify them, in writing, that they must remove the posts or comments in question. They should be reminded of their ongoing obligation not to violate patient privacy. This could be perceived as a good-faith effort to comply with the rule should sanctions be considered.

REPUTATION MANAGEMENT

After privacy, one of the most significant risks that any organization must manage when using social media is that to its reputation. In healthcare, as in any other industry, this encompasses two distinct elements: first, being aware of and responding to criticism and
complaints that originate outside the organization, and second, ensuring that the content published or posted via social media accurately reflects the organization’s message and does not harm its reputation. 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.

**Content That Originates Outside the Organization**

Awareness should be the most straightforward of these areas to maintain. An individual or department should be assigned responsibility for monitoring what is being said about the facility online, just as should already be taking place with regard to other, traditional media. This person or department should look for both positive and negative coverage. Most social media tools include inherent mechanisms to alert users when they have been mentioned or tagged in a post, and simple, saved Internet searches, such as those facilitated by Google, will help identify other instances of which the facility should be aware. Staff responsible for monitoring social media should understand how these various mechanisms work.

The facility should have a policy regarding whether and how to respond when it becomes aware of discussions about the facility on social media. It may be impractical to respond to every instance when a facility is mentioned; a small hospital, for example, may not have sufficient staff to do so, and a larger facility with a very high patient volume may be unable to keep up with a similarly high-volume discussion. A more practical approach may be, for instance, to limit responses to cases in which a social media user is voicing a specific, actionable concern or complaint. Regardless of the threshold a facility uses in deciding whether to respond, staff should consistently adhere to the policy.

Responses, when they do occur, should be timely and respectful. Social media is used around the clock and, although a facility will not be able to respond 24 hours a day, it should make every effort to ensure that responses do not come days after an initial post—an eternity in Internet time. Offering a rapid initial acknowledgement of a compliment or complaint, even without any specific follow-up, is better than waiting two or three days to respond.

When a social media user is complimentary about the facility, maintaining a respectful tone is generally not a challenge. A staff response should thank the commenter and express appreciation for the post; a response, for example, could be, “Thanks for the kind words! We’re really proud of our staff, and glad to hear that you had a good experience here.” Even in these situations, however, staff should be sure that their response is consistent in tone and language with the organization’s expectations.

In responding to complaints—whether about care received, specific staff persons, amenities, billing practices, or any other aspect of the organization—staff should be instructed not to try to solve problems through social media. Rather, they should reply to the complaint by acknowledging it and inviting the user to contact the facility through some other established mechanism, such as by phone or e-mail, to communicate with professionals who are responsible for handling similar problems. A possible response is, “We’re sorry to hear that you’re having trouble with billing, and we’d like to work with you to resolve the problem. Please get in touch with us at [phone number] so that we can help.”

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

Whatever the response is, policies should explicitly remind staff to always maintain a courteous, professional attitude. There is no benefit to be had from insulting or demeaning anyone. Staff 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.

**Content That Originates within the Organization**

Besides responding to social media discussions that originate outside the organization, and ensuring that the response is appropriate and protects the organization’s reputation, risk managers must also ensure that policies address content that originates within the organization—that is, posts or updates that are generated as new content, not in response to an outside person or entity. Although anonymity, which gives individuals the
Replying to Inquiries and Establishing Terms of Use

When hospitals establish social media profiles, regardless of the particular tools they use, consumers are likely to use those media as another way to contact the hospital with a wide range of inquiries, and the staff monitoring social media should be trained in how to 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 whether one of the hospital’s locations offers magnetic resonance imaging, or where to park when visiting someone in the maternity ward, can be answered easily, quickly, and accurately via social media, and staff should be trained on the appropriate answers to these and similar questions and on where to find information if they do not know the answers themselves.

Other inquiries could be less innocent. Patients may ask for specific medical advice, for example, or even use social media to reach out to hospitals in cases of emergencies—instances when social media are definitely not the appropriate tools for responding. If hospitals make clinical staff available on social media as “experts” in various topics, the risks of such inappropriate questions increase.

All staff members, whether participating in social media in their own name or on behalf of the 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, hospitals may consider creating publication-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 and use of 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 facility decides to handle these issues, the answers should be clearly delineated in terms of use, staff should be educated about them, and they should be enforced consistently.

ability to express themselves without fear of recrimination, is often hailed as a benefit of the Internet, when 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 are 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,
HEALTHCARE ORGANIZATIONS AS EMPLOYERS

In addition to their use of social media as marketing, public relations, or information-sharing tools, healthcare organizations use social media in their role as employers. When they are hiring, employers may use social media to screen applicants for positions or may use social media as a recruiting tool. Once on staff, employees may use social media in their personal lives in ways that affect the organization. And, finally, former employees may use various social media to ask for recommendations or otherwise interact with the organization in a way that requires a response and poses some risk.

Screening Applicants

The use of the Internet in general and social media in particular as applicant screening tools is increasingly common. Surveys vary in terms of how they indicate hiring managers are using social media, but in one study conducted in 2010, at least 75% of recruiters used the Internet as part of the applicant screening process, and at least 35% of the respondents used the information they found on those searches to eliminate candidates (Walker).

A separate survey showed that these online searches rely heavily on social media. In the second study, 75% of respondents stated that they use LinkedIn as part of the applicant screening process; 48% of respondents stated that they use Facebook; and 26% stated that they use Twitter (Gildea).

Although there are risks to this practice, screening applicants through social media is not necessarily a problem and can in fact yield useful information for the hiring manager. Useful information could include, for example, insight into a candidate’s work ethic and judgment. Do former employers recommend them on LinkedIn? Do candidates’ posts frequently brag about skipping work or about how much they hate their jobs? Do they post racist or other inflammatory content? Similarly, communication skills can be assessed, particularly based on the candidate’s posts on blogs or other long-form communications. Any adverse information along these lines could be considered legitimate grounds for eliminating a candidate from consideration.

However, much of the information revealed through social media is likely to be information that employers are prohibited from considering as part of the hiring process. Federal laws that could be implicated include those that follow; additional state or local statutes could also be brought into play (Hinson):

- The Civil Rights Act of 1964 prohibits consideration of a candidate’s race, color, religion, sex, or national origin.
- The Pregnancy Discrimination Act prohibits consideration of a candidate’s current or recent pregnancy or related medical conditions.
- The Americans with Disabilities Act (ADA) prohibits discrimination based on a qualified candidate’s disability.
- The Age Discrimination in Employment Act prohibits discrimination against employees who are 40 years old or older.
- Even the Genetic Information Nondiscrimination Act, which prohibits consideration of a candidate’s genetic information (EEOC), could be implicated if, for instance, a candidate talks about participating in a cancer fundraiser in memory of her mother, who succumbed to breast cancer. From that information, the employer could infer that the candidate has a family history and a genetic risk for developing breast cancer.

Once an employer sees any of this prohibited information, regardless of how it is discovered or how it is used or not used as part of the hiring decision, the employer may find it difficult to argue that this information did not factor into the hiring decision.

To gain the benefits of information that can be learned from social media while limiting the risk of various discrimination allegations, organizations should consider having a neutral third party—someone other than the hiring manager—screen social media profiles of candidates. The screener should be a hospital employee and should be trained in what to look for, such as signs of poor judgment or poor communication skills, and should relay them to the hiring manager. The screener should also be trained in what not to convey back to the hiring manager, such as any of the characteristics that the Civil Rights Act, ADA, and the other employment laws prohibit employers from considering.

Screeners and hiring managers should limit their searches to information that is publicly available.
Attempts to view information that a candidate intends to keep private, such as by guessing a candidate’s password or sending Facebook friend requests under false pretenses, may be illegal and will cast a negative light on the organization engaging in the action. Hiring managers should be cautious in how they consider information obtained through screens of social media profiles. Before disqualifying a candidate for poor grammar, for example, employers should ensure that the candidate is the person who actually posted the information and that other extenuating circumstances are not in play (e.g., a user may have a disability and use speech-recognition software to post information, which may not always display clearly).

Finally, all actions related to screening and recruiting of applicants should be thoroughly documented. A hiring manager should always be able to show a legitimate, nondiscriminatory reason a candidate was not considered in the event of accusations of discrimination.


**Recruiting Applicants**

In addition to using social media as an applicant screening tool, hiring managers may want to use social media as a recruitment tool. Although such a practice is likely acceptable, hiring managers should be wary of using social media as their sole source of recruiting applicants.

The primary concern with such a practice is that social media users are not representative of the U.S. population as a whole in terms of ethnic or racial diversity. For example, the U.S. population is roughly 13% African American and 15% Hispanic, but LinkedIn users are only 5% African American and 4% Hispanic. If hiring managers or other recruiters limit their searches to social media, they could be open to charges of “disparate impact.” Using a search of LinkedIn as the only recruitment strategy would significantly underrepresent important parts of the pool of potential applicants. (Fisher)

Instead of relying on social media as the sole recruitment avenue, hiring managers should treat it as one part of the hiring strategy—just as social media can be viewed only as one piece of the marketing, customer relations, or applicant screening processes, as discussed throughout this Risk Analysis. In doing so, managers can avail themselves of the benefits of social media without unduly increasing their risks.

**Employees’ Personal Use of Social Media**

Risk management concerns related to social media use and employment do not end once employees are hired. Although policies related to patient privacy and how social media users can represent the organization cover one class of use—that by employees in their official capacity—additional policies are necessary to outline expectations for employees’ social media use outside their official work capacity.

For example, nursing staff may use social media to discuss their supervisors, the facility itself, the shifts they work, or their wages. Their discussions may be very public and may not always present the facility in a flattering light. Such use will likely not violate patient privacy but could raise concerns about the facility’s reputation and could prompt an employer to want to take disciplinary action.

Whether such disciplinary action is permissible depends on the type of information that the employees post. In late 2010, the National Labor Relations Board (NLRB) charged a Connecticut ambulance service provider with violating an employee’s right to engage in concerted organizing activity in this type of situation. According to NLRB, the employee was asked to prepare a report concerning a customer complaint about her work. The employee requested and was denied representation from her union. Later that day from her home computer, the employee posted a negative remark about the supervisor on her personal Facebook page, which drew supportive responses from her coworkers and led to further negative comments about the supervisor from the employee. The employee was suspended and later terminated for her Facebook postings and because such postings violated the company’s Internet policies. (NLRB; Martinez)

NLRB argued that the employer’s policies, such as one that prohibits employees from making disparaging remarks when discussing the company or supervisors and another that prohibits employees from depicting the company in any way over the Internet without company permission, violated the National Labor Relations Act. According to NLRB, such provisions
constitute interference with employees in the exercise of their right to engage in protected concerted activity. The two parties eventually settled, with the company agreeing to revise its policies. (NLRB; Martinez)

It is important to note that this was not a court decision, and the settlement does not set legal precedent. In addition, NLRB does not appear to be saying that employers have no room to regulate what their employees say off-hours. Rather, in the narrow area of speech that could be construed as concerted organizing activity, that speech is protected. Speech that simply disparages an employer’s products or services may be made subject to regulation—for example, NLRB has previously upheld company policies that prohibit a department store’s staff from going online to disparage products that the store sells. (Martinez)

In light of the NLRB complaint and settlement, risk managers should ensure that policies specifically outline the types of posts that are prohibited, including those that present the hospital itself or its services in a negative light. Consequences for such actions should be defined, and all employees should be educated about the policy.

An example from outside healthcare illustrates the kinds of posts that should be prohibited while remaining within the limits of what NLRB would consider acceptable. In February 2011, a high school English teacher in Bucks County, Pennsylvania, was suspended indefinitely without pay when the school board found that she had been writing a personal blog including offensive posts about her students. In her posts, she made statements such as the following (Larson):

- “A complete and utter jerk in all ways. Although academically ok, your child has no other redeeming qualities.”
- “Just as bad as his sibling. Don’t you know how to raise kids?”
- “There’s no other way to say this: I hate your kid."

Other posts were more offensive, even profane. All of the posts, indeed the whole blog, were signed with the teacher’s first name and the initial of her last name only, and the school was never identified; neither were individual students. (Larson)

The teacher was suspended as soon as the blog came to public light; her long-term employment status has not been publicly disclosed. The school board met in February 2011 to discuss terminating her, but no decision had been publicized as of June 2011. (Quinones)

In this situation, the speech in question had nothing to do with anything that NLRB would consider “concerted organizing activity.” It was not protected in any way. A policy governing employees’ personal use of social media can point to this example as representative of posts that are prohibited—and an employer would be well within his or her rights to discipline an employee based on posts such as these.

Although privacy policies should prohibit healthcare workers from discussing specific patients via social media in any context, policies should explicitly instruct staff to never speak badly about a patient and should strongly discourage such criticisms of colleagues via social media. As noted earlier, certain kinds of posts about colleagues, particularly supervisors, may be protected speech, but employers remain well within their rights to remind users that such criticisms are likely to be used if litigation arises concerning the parties in question. There may be a natural inclination on the part of healthcare workers to want to talk about the frustrations of their jobs, but they should be told repeatedly that social media cannot be the venue for such discussions, even if they think the media is private.

Although healthcare facilities and other employers rightly are concerned about what their employees say about them via social media, employers must recognize that there are limits to how far they should go in obtaining this information. See “Respecting Staff Privacy” for examples of how employers’ attempts to view information from staff members’ use of social media has led to penalties against the employers.

For more information on policies regarding hiring and firing employees, see the Risk Analysis “Hiring and Firing,” in the Employment Issues section of the HRC System.

Social Media Employment Recommendations

LinkedIn and other business-related social networking sites allow users to recommend or “endorse” one another. Risk managers should ensure that the human resources department has policies in place that govern whether, and how, management staff will be allowed to endorse current and former employees. The policy should be consistent with policies in place for giving out recommendations in other contexts, and management staff should be educated about the policy so that they do not feel forced to make ad hoc decisions if they are asked by an employee to provide a recommendation.
Respecting Staff Privacy

In their personal use of social media, staff members acting in their own name (not on behalf of the organization) could post information that prompts disciplinary action. These posts could reveal inappropriate or dishonest actions on the employee’s behalf (e.g., taking a sick day and then posting pictures that show the employee attending a baseball game) or could represent complaints about the organization or the employee’s supervisors or other information that violates the organization’s social media policies. When deciding whether to take action against the employee, risk managers and human resources personnel must take into account how they became aware of the offending information.

Whether such information can be used to discipline an employee often hinges on how the information was obtained. When the information is posted publicly, employees who become aware of it are free to take disciplinary action, including terminating employment. Information that is intended to be private and is discovered by deception or subterfuge may be protected, and employers have been penalized for taking employment actions based on information that was presumed to be private.

Two cases in industries other than healthcare illustrate how employees have used the Stored Communications Act (SCA), a federal statute, to argue that their interest in keeping information private outweighs an employer’s interest in obtaining that information and using it against them.

In the first case, a pilot had set up a private website on which he and other pilots posted information that was critical of the airline he flew for and its union. The website was restricted to authorized users—its contents were not publicly available. The site’s terms of use specifically forbade airline management from viewing the site, and forbade otherwise authorized users from sharing the contents with airline management. An airline vice president became aware of the website, and using two other pilots’ names and passwords—with those pilots’ permission—the vice president accessed the site more than 30 times. The vice president relayed the information he found there to the airline’s president, who told the pilots union; the union threatened to sue the pilot for allegedly defamatory information posted on the website. The pilot was also eventually placed on medical suspension. (Konop)

The pilot determined who had accessed the site. He sued, alleging, among other things, that the suspension was retaliatory and that the vice president had violated SCA by accessing the information under false pretenses. The Ninth Circuit Court of Appeals agreed that SCA had been violated; the airline was ordered to pay $9,000 in damages. (Konop)

In the second case, the plaintiffs argued that the defendant restaurant owners had accessed a private chat group on their MySpace page without authorization. The employers had allegedly accessed the chat group, as well as other parts of the private MySpace account, at least five times without authorization by posing as other users. Some posts on the site were highly critical of the employers. The two site owners were fired; they sued, again alleging violations of SCA, eventually receiving compensatory and punitive damages totaling more than $10,000. (Pietrylo)

For risk managers, the cases offer similar lessons. Subterfuge or deception can never be used to obtain information that is intended to remain private. Even when an employee volunteers access to a site he or she does not own, management should be hesitant to use that information. Rather, if the employer believes that something there needs investigation, the employer should go directly to the site owners to ask for access.

References

Konop v. Hawaiian Airlines. 302 F.3d 868 (9th Cir., 2002).


OTHER RISKS

Although the risks covered throughout this Risk Analysis (privacy, reputation, medical liability, employment issues) are the most prominent, there are others that risk managers and their information technology (IT) staff will need to consider in the context of social media.

Network security is a significant concern throughout healthcare organizations and in many situations other than social media. In at least one case study, however, a company hired consultants to use information that its employees make available on their own social media profiles to gain access to the company’s private networks. They did so by guessing the employees’ social media passwords, which the consultants then used to access the corporate networks, where employees used the same passwords as they used on social media sites. Risk managers should ensure that their IT staff plays a role in educating staff about risks related to password management and network security. (Esola)

Risk managers should also be aware that information created or shared via social media could be subject to e-discovery in the course of litigation. For more information on e-discovery rules and the obligations they expose on parties to litigation, see the Risk Analysis “Discovery: Paper Records and Electronic Information,” in the Medical Records section of the HRC System.
Finally, risk managers should ensure that any training for social media use includes reminders about the kinds of competitive intellectual property that should not be shared. For example, employees knowledgeable about a proposed merger or a new service to be offered must be sure that this information is not prematurely shared outside the organization.

**EMERGING SOCIAL MEDIA**

An important point for risk managers 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 risk managers will not be able to rewrite plans quickly enough to keep up with the rapidly changing technologies.

Social media that were emerging as of mid 2011 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; as this Risk Analysis is printed, it has not yet 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 hospital staff who may be among early adopters—risk managers should ensure that all the same precautions taken on Facebook apply to Google+ users and should emphasize in particular 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, Gowalla, SCVNGR, and Facebook Places**. As described in the discussion Major Kinds of Social Media, these location-based social media focus on users checking in to various locations from GPS-enabled devices. Risk managers should be aware if their marketing team establishes a presence on any of these platforms and be aware of the specials that may be offered to ensure that they do not raise any concerns.

**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. Risk managers should provide guidance to their staff regarding whether they can participate in these and similar sites in their professional capacity and with their organizational affiliation, and should remind them of the risks associated with offering medical advice through these services.

**Groupon and Living Social**. These sites offer daily deals that represent deep discounts for goods or services, such as 70% off a pair of shoes or 3-for-the-price-of-1 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 may develop increasingly sophisticated portals of their own, or even apps for devices like smartphones and tablet computers. These could include services such as the ability to communicate with physicians, to make appointments, to manage health records, or to view test results. Such portals implicate all the risk management concerns discussed throughout this Risk Analysis, and risk managers must be aware of any plans for 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 staff other than the accountability group or individual may participate in the organization’s official social media.

- Identify 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 and 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.

- Use only employees other than hiring managers to screen candidates’ social media profiles during the hiring process. Train designated screeners in the kinds of information that they may and may not relay to hiring managers.

- Limit preemployment screens of social media profiles to information that is publicly available; refrain from attempting to access private information by deception or guessing passwords.

- Document legitimate, nondiscriminatory reasons for not hiring a candidate.

- Ensure that policies regarding employees’ personal use of social media do not attempt to regulate speech that could be considered concerted organizing activity by NLRB.

- Describe and offer examples of types of posts that are prohibited by employees in their personal time, such as posts that negatively portray the hospital or its services.

- Educate managers regarding policies for using social media to endorse or recommend current and former employees.

- Create policies that are general and flexible enough to adapt to emerging social media without requiring constant updating.

References


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


Kaplan AM, Haenlein M. Users of the world, unite! The challenges and opportunities of social media. Bus Horizons 2010 Jan-Feb;53(1):59-68. Also available: http://www.sciencedirect.com/science/article/B6W4S-4XFPZ50-1/2/600db1bd6e0c9903c744aa5f34b0b12e1.


