In addition to their use of social media as marketing, public relations, or information-sharing tools, healthcare organizations of all types 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.

This Guidance Article reviews risks posed to employers in each of these three phases of employment and provides guidance on policies and practices that can be put in place to allow organizations to benefit from social media while minimizing harm.

**EXECUTIVE SUMMARY**

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, 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 screening process; 48% of respondents stated that they use Facebook; and 26% stated that they use Twitter (Gildea).

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, and at least 35% of the respondents used the information they found on those searches to eliminate candidates (Walker).

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.

For more general information on employment law and ADA, see [Human Resources](#).

**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. 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 (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 Guidance Article **Human Resources**.

**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.

**Action Recommendations**

- 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.
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, employers 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 pilot’s union; the union threatened to sue the pilot for alleged 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).