

**Regulating the Medical Workplace in the World of Web 2.0**  
*Policies for Facebook, Twitter, Blogs and Other Social Media Postings are a Must*

by Susan Keating Anderson  
Walter & Haverfield LLP

In a few short years, social media has gone from fad to fact. Facebook and Twitter, the two most widely recognized social media vehicles, in addition to the countless number of other social media sites, online forums, chat rooms and weblogs (aka blogs), have become indelibly woven into the fabric of daily life – both personal and professional - at a rapid-fire pace. American adults are “Facebooking,” “tweeting” and blogging not just at home, but also at the office during work hours, using work-owned equipment, and sometimes, discussing work issues, for good and bad.

Consider the following statistics. A study conducted by Pew Internet & American Life reveals that more than 57 million Americans read blogs. A Nielsen study reveals that in 2009, U.S. internet users spent about 16 percent of their online time on social networking websites and about 12 percent of the time e-mailing. By 2010, the social networking time increased to 23 percent, while e-mailing dropped to 8 percent. The Pew study also revealed that 75 percent of Facebook users admit to checking their Facebook page while at work.

Aided by the advent of widespread WiFi, PDAs and other smartphone devices, access to social media is also becoming easier for all age ranges. In fact, Nielsen found that the number of Americans aged 50 and older who visit social media sites is twice that of the 18 years and younger group. Simply put, social media isn’t just for kids anymore and, because of that, it has found its way into the modern workplace – medical practices and hospitals included.

So what does the proliferation of Facebook, Twitter, blogs and other methods of social networking and communication mean for Northeast Ohio physicians? Like employers in other industries, physicians face a multi-faceted issue: how to implement and regulate their own presence in the social media marketplace (personal and professional) *as well as* that of their employees (again, in both the personal and professional realm).

This issue presents a proverbial minefield of legal and ethical hazards for today’s physician – not to mention potential civil or criminal liability – if the murky waters of this dynamic, instantaneous communication method aren’t navigated carefully.

**Presenting a professional (and legal, and ethical) social media presence**

Social media provides the opportunity to reach potentially millions of people to share information easily, quickly and efficiently. It’s no wonder that physicians have begun to turn to Facebook, Twitter and blogging, as well as other social media vehicles specific to the medical field, as a way to establish a presence and reputation online.

If used correctly, social media can be a valuable tool for a medical practice, giving doctors an accessible outlet to connect with peers nationwide without leaving their office and a way to market their practice and expertise and disseminate public health information to a wider

audience. However, pitfalls can arise when a physician's postings, or that of the physician's employees, crosses over to the realm of inappropriate, illegal or unethical.

### **Applicable laws**

In determining what is and is not appropriate for dissemination by a physician-employer through social media, the myriad of laws that could potentially reach a physician's online communications must be considered. Perhaps most obvious is the responsibility to guard patient privacy under HIPAA and, in Ohio, under the more stringent privacy protections arising from the Ohio Supreme Court case *Biddle vs. Warren General Hospital*, 86 Ohio St.3d 395, and its progeny.

In a broader context, the same laws and regulations that apply to the everyday work environment also apply online. Thus, physician-employers have to be cognizant in their online communications of the possible application of laws such the federal Title VII of the Civil Rights Act of 1964 (applicable to employers of 15 or more employees) and Chapter 4112 of the Ohio Revised Code (applicable to employers of 4 or more employees). These laws prohibit discrimination based upon such things as race, color, sex, religion and other protected classes. Similarly, federal laws such as the Americans with Disabilities Act (ADA), the Age Discrimination in Employment Act, the Pregnancy Discrimination Act (and comparable Ohio Ohio laws), and the more recent Genetic Information and Non-Discrimination Act (GINA) of 2008 could apply.

In the context of regulating employee use of social media inside and out of the workplace, privacy issues are again paramount, but in a somewhat different context. In *Housh v. Peth*, 165 Ohio St. 35, the Ohio Supreme Court established the tort of invasion of privacy as including "the wrongful intrusion into one's private activities in such a manner as to outrage or cause mental suffering, shame or humiliation to a person of ordinary sensibilities." This case has been used by employees to bring invasion of privacy claims against their employers for things like accessing an e-mails sent through or held in a business e-mail account, monitoring employee internet usage and accessing employee blogs and social media postings.

In addition, depending on the context and conduct involved, either or both of the following two laws could apply. These are the federal Electronic Communications Privacy Act, which prohibits the unauthorized interception of wire, oral or electronic communications and the Stored Communications Act, which makes it illegal to "intentionally access a facility through which an electronic communication service is provided...and thereby obtain...access to a wire or electronic communication while it is in electronic storage in such a system." 18 U.S.C. § 2701.

Finally, and, importantly, physician-employers should take heed from a recent National Labor Relations Board (NLRB) complaint dealing with social media. In November 2010, the NLRB charged American Medical Response of Connecticut, Inc., an ambulance company, with improperly terminating an employee for making negative comments on her Facebook page about her supervisor. The NLRB claimed that the employee was terminated for engaging in protected concerted activities by criticizing her supervisor to other employees.

While the case was settled between the parties in January, the complaint signals a focus by the NLRB on an employer's regulation of employee's social media posting when such regulations arguably restrict an employee's right to engage in concerted activity protected under the National Labor Relations Act (NLRA). I don't have to worry about NLRA because I'm not a union employer, you say? Think again – the NLRA's protection of concerted activity applies to non-union workplaces too.

### **Physician use of social media**

So what is a physician to do, or not, with respect to his or her own social media use? First, physicians should not rely upon the false security of "privacy settings" that may or may not actually protect the data posted to social media sites. As a result, doctors must think carefully before they accept patients as a "friend" on site like Facebook or allow an open "following" on a Twitter page. Even if they are careful about who they accept as friends or have what they believe to be strict privacy filters in place, their posts may still be passed along to other people or otherwise accessed by unintended recipients, creating a documented trail that can be used in potential litigation or audits down the road.

For the same reasons, physicians who are creating pages on social networking sites would be best served to create a personal page for non-professional interaction with family and friends and a separate page for use solely in their practice where they can maintain appropriate professional, ethical boundaries of the patient-physician relationship as they would in any other context. No matter how the pages are constructed, however, it cannot be stressed enough that when it comes to communications online, physicians must be vigilant to maintain the required standards of patient privacy and confidentiality at all times when communicating and conveying information.

Additionally, it's important to remember that providing advice online also creates a documented trail of communications that may exist in perpetuity. If a physician's "Facebook friend," who is not a patient, asks a health-related question online, the ramifications of responding can be quite different than if the physician has a casual, in-person discussion with the friend on the topic. In a worst case scenario, the documented exchange on Facebook could be used as evidence of a physician-patient relationship in a courtroom or before many regulatory bodies.

Finally, if other employees of the practice are permitted or required to post and otherwise maintain the content of a physician's social media site, it is recommended that policies setting forth the parameters of this responsibility or discretion be created and the relevant employees trained on those policies. Since it is the physician's name and medical reputation at stake, it is also imperative that the physician himself or herself monitor the postings and follow-up on questionable or inappropriate content.

### **Developing an effective social media policy for employee use**

Beyond carefully developing and maintaining their own social media presence, physician-employers face a second challenge – monitoring their employees' presence on social media as it relates to the workplace.

While physician-employers do have the right to monitor employee personal internet and e-mail usage, particularly when the employee is using equipment owned by the practice or hospital and engaging in such activity during work hours, it is highly recommended that physician-employers have written policies in place that inform employees of the parameters of this monitoring. Such policies should include a clear, direct statement that employees should have no expectation of privacy in their use of practice-owned equipment, e-mail accounts, internet providers, or software.

Specific to social media, the issue gets a little muddier because employee posts to social media often, but not always, occur outside of work hours and are arguably personal in nature, even if the postings address practice-related issues. Despite this, employers do have the right to regulate such postings within the context of the potential effect on the workplace and practice.

Again, it is important that there be a written social media policy in place, which should include *but not be limited to* the following provisions:

- Prohibit the use of employer-related information of any kind in employee postings;
- Prohibit the disclosure or use of any sensitive, proprietary, confidential or financial information about the practice, hospital or any of its patients;
- Prohibit the employee from implying the endorsement of the practice or hospital in any statement or posting;
- Prohibit the employee from posting material that is obscene, defamatory, libelous, threatening, harassing, abusive, or hateful about the practice or hospital, its physicians, employees or patients; and
- Inform employees clearly that violations of the policy may result in discipline, up to and including termination of employment.

The social media policies should also be tied in to other policies, such as harassment, discrimination and acceptable-use policies.

Equally important to maintaining written policies is taking the time to train practice employees on the policies. Employees need to realize that what is unethical, unprofessional and even illegal in the office environment also holds true online and that their posts, even if intended to be private or personal in nature, could result in civil liability or other legal consequences.

### **Going forward in the social realm**

Without a doubt, social media presents an efficient, effective and immediate way to share information with colleagues, peers, employees and patients and can help promote a medical practice in ways that reach beyond traditional marketing and advertising.

As the countless number of Facebook indiscretions reported in the news reflect, however, it's easy to forget that what is posted online, even if protected by so-called "privacy settings" is rarely anonymous and is easily shared, searchable, and generally permanent. For that reason, physician-employers must recognize that their actions online, as well as that of their employees, could negatively affect their reputations, practice and careers and lead to significant legal consequences.

Physician participation in social media should be approached with care and common sense, whether the site is a wide-reaching one such as Facebook or one of the many sites specific to the medical community. Likewise, the same care and common sense needs to be applied in the workplace by developing social media policies for employees of a medical practice or hospital setting. With a little bit of thought and effort, modern medical practices and hospitals can reap the benefits of the ever-evolving World of Web 2.0.

*Susan Keating Anderson is a member of the labor & employment law group at the law firm of Walter & Haverfield LLP and may be reached at [sanderson@walterhav.com](mailto:sanderson@walterhav.com). This article presents general information and education on legal developments and does not constitute legal advice.*