Developing Social Media Strategies and Policies

By: Caroline J. Patterson, Esq., Jill S. Garabedian, Esq.
Wade, Goldstein, Landau & Abruzzo, P.C.
61 Cassatt Avenue, Berwyn, PA 19312

I. Introduction

The use of social media and social networking has exploded in recent years and internet usage by employees is almost inevitable, whether on their desktop computers or on smart phones. Almost everyone has access to a device that can give them instant access to information via the internet or social media/networking websites. This article addresses how your practice can effectively manage your employees' use of social media, utilize social media in hiring and to protect your physicians' use of social media in communicating and treating patients.

"Social Media" can be defined as a "group of Internet-based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of user generated content."[1] In essence, that encompasses any Internet based platform that would allow a user to post information (words, images, etc.) and interact with other users. The most common forms of social media are as follows:

a. Collaborative projects in which users collectively create something together. The most commonly known and popular collaborative project is Wikipedia.

b. Blogs and Microblogs are websites that allow users and creators to publish their own messages and information. Some blogs are run by companies or professional associations for the purposes of exchanging information. Individuals sometimes use blogs as a personal diary or journal. The most common microblog is Twitter (www.twitter.com), which allows users to blog entries that may be shared among followers.

c. Content communities, such as YouTube (www.youtube.com), allow users to upload and share content that they have created (videos, etc.).

d. Social networking sites, such as Facebook (www.facebook.com) and LinkedIn (www.linkedin.com), allow users to make connections ("friends") and share content.

e. Sites such as Instagram allow registered participants to post content through photos. Instagram can be linked to other sites, such as Facebook and Twitter, so that content posted is shared on multiple sites.

II. Employees Use of Social Media and Email

a. Areas of Concern. It is important to understand the main concerns you face as an employer in terms of internet and social media usage, so that you can craft a policy to be implemented as a part of your employee handbook to address these issues.

i. HIPAA and State Privacy Law Concerns.

[1] Kaplan, Andreas M.; Michael Haelein (2010), "Users of the world unite! The challenges and opportunities of Social Media". Business Horizons 53 (1): 59-68. Doi:10.1016/j.bushor.2009.09.003.ISSN 0007-6813.

Most employers deal with the concerns raised by employee use of the internet and social media in terms of productivity and harassment issues, yet physicians have a unique concern as employers since their employees are dealing with Protected Health Information every day ("PHI"). The Privacy Rule of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") protects PHI and limits the use and disclosure of that information. Alternatively, the HIPAA Security Rule provides standards and guidelines for covered entities to ensure that patients' PHI is held securely and confidentially. Posts on social media websites are unencrypted and unsecured disclosures of PHI. Employees need to be aware that even a seemingly innocent tweet about a patient can be a HIPAA violation and cause major problems for the practice. While patients are free to post about their own medical issues, physicians and staff must be careful when responding to posts from patients on Facebook pages or commenting on blog posts to make sure that they are not disclosing PHI, or if they are, they have received the consent of the patient. This concern extends to the practice's social media sites, as well as, personal sites for employees and physicians.

ii. Privacy and confidentiality issues.

Beyond HIPAA, the use of social media and email presents some additional issues related to privacy and confidentiality. The ability to transmit information instantaneously and virtually presents problems with breaches of confidential information, trade secrets, and know-how.

iii. Time Management/Privacy.

Excessive internet and social media use by employees is a big concern for many employers, especially those who have employees that sit at or near a computer, as many front desk personnel do, for the entire day. This concern has only increased with the invention of smart phones giving access to the internet away from a desk. According to International Data Corporation ("IDC") research, thirty to forty percent (30-40%) of employee internet activity is non-work-related. Employers, of course, can limit the ability of their employees to access certain websites, like Twitter and Facebook, on work computers. However, as your practice begins to use social media and networking to its advantage, you may have some employees whose job duties include updating Twitter and Facebook accounts or monitoring your website and reviewing websites for comments from patients. Therefore, an absolute ban on internet use in the office may be near impossible to monitor and enforce. Like a forbidden fruit, a complete prohibition on internet and social media use has been found to actually increase employee use of the internet using other methods in secrecy, which may have an even greater impact on productivity. A well-written policy can limit non-business related internet activity and set boundaries for your employees that are reasonable and legitimate.

iv. Endorsement Issues.

One area of liability that some employers may not consider with employee use of social media is in endorsements. The Federal Trade Commission ("FTC") has, through the Federal Trade Commission Act ("FTC Act"), put in place certain rules to prevent unfair methods of competition, and unfair or deceptive acts or practices in or affecting commerce. Basically, employers may be liable for an endorsement made by an employee. The FTC Act provides that endorsements "must reflect the honest opinions, findings, beliefs, or experience of the endorser." Additionally, an endorsement "may not convey any express or implied representation that would be deceptive if made directly by the advertiser." Here, the practice is the advertiser and the employee would be the endorser. The increase in social media use has

brought about more opportunity for employees to endorse their employer in one way or the other; for example, by posting positive reviews on a review site or writing a positive blog post about the practice on the employee's private blog. Although an endorsement is a positive thing, employers must be aware of what their employees post online and take proactive steps to provide adequate guidelines to them or they may be subject to liability based upon those actions. Specifically, in accordance with FTC guidelines, if it is not obvious to readers that the employee works for the employer, the employee must disclose this relationship before making any statements endorsing the employer.

v. Harassment and Anti-discrimination Laws.

Another issue employers may face is minimizing and addressing harassment and discrimination in the workplace. As if office gossip and harassment weren't already a concern for employers, the internet has opened up a whole new forum for office bullies. Most employers have a policy that addresses harassment and discrimination in the workplace, but does that policy extend to statements and comments made via social media sites? Even when an employee is using social media on their own time and on their own personal sites, the comments they make can have an effect on the workplace and other employees. Employers should understand and address in their policies that employees' participation in social media, either as an employee or personally, needs to be consistent with other policies in the handbook, including the discrimination and harassment policies.

vi. NLRB.

It is clear that employees in a medical practice must keep patient PHI confidential, but a general confidentiality policy that limits an employee's ability to discuss anything work related may be too broad and could be problematic under the National Labor Relations Act ("NLRA"). The NLRA ensures that employees have the right to discuss certain terms of their employment such as wages and work conditions.

The National Labor Relations Board ("NLRB") is charged with protecting the rights of employees to act together to address conditions at work, with or without a union, under the NLRA.[2] The NLRB has specifically stated that "this protection extends to certain work-related conversations conducted on social media, such as Facebook and Twitter."[3] In response to complaints related to employer social media policies and to specific instances of discipline for Facebook postings, the NLRB has increasingly found instances where there is reasonable cause to believe that some policies and disciplinary actions violated the NLRA. In other cases, investigations found that the communications were not protected and disciplinary actions did not violate the Act. The issue of whether the NLRA is implicated hinges on whether or not the NLRB considers the actions of the employee to be a protected or "concerted activity".[4] In addition to union and collective activities, the NLRA protects employees who take part in grievances, on-the-job protests, picketing, and strikes. In the context of social media, that can apply to any kind of "concerted activity" online, including "liking" a fellow employee's comment regarding their employer.[5][6] Generally, the NLRB is taking the position that overly broad social

[2] See http://www.nlrb.gov/node/5078.

[3] Id.

[4] 29 U.S.C. § 157.

[5] *See Three D, LLC d/b/a Triple Play Sports Bar and Grille,* 361 NLRB 31 (2014). The employer in this case has appealed to the Second Circuit Court of Appeals based on the argument that the employees' comments were disloyal, maliciously false and not intended to improve working conditions, and

media policies that infringe on, or have the potential to infringe on, an employee's rights are unacceptable under the NLRA.[7]

b. How to Address.

i. Create A Policy.

As we have discussed, use of social media has become pervasive in and out of the work-place. An all-out ban on an employee's use of social media will not work. The bottom line is that employees are going to use social media and having a well-crafted social media policy protects the employer from liability on a number of fronts, including accusations of discrimination in hiring, allegations of termination based upon online activity and claims of HIPAA violations by employees.

The following is some guidance on how to prepare a well-crafted social media and email policy:

- This policy should clearly and broadly define social media to include all areas including collaborative projects, blogs, content communities, social networking sites, virtual game worlds, text messages, bulletin boards, chat rooms, etc. The policy should make clear that all policies apply to online conduct even if not enumerated. It should also contain clear statements about limitations of the employee's expectations of privacy, including the employer's ownership of the computer, the employer's right to monitor (see discussion below) all company services during and after employment, and the existence of an "audit trail" as to activity conducted on a company computer.

- The policy should also define prohibited and limited activities. For employer sponsored sites, a policy may prohibit employees from disclosing company confidential information and trade secrets; posting personal and privileged information like attorney-client and doctor patient communications; soliciting for non-company activities; connecting with subordinates on social networking sites; and violating other company policies through the use of social media. For non-employer sponsored social media sites, employers may also prohibit employees from endorsing the employee without disclosing its employment relationship and/or violating company mandated blackouts for securities purposes.

- A good policy should prohibit "off duty" activity as well. Off-duty prohibited activity can relate to conduct that could severely damage the employer's business reputation or subject the employer to legal liability. Examples of acceptable prohibitions include

---

therefore are not protected by the NLRA. An Amicus Brief was filed by the Service Employees International Union on October 1, 2015.

[6] Most recently, in March 2015, the NLRB extended NLRA protection to an offensive and, arguably obscene, comment about an employer posted on an employee's personal Facebook profile based on its union subject matter, employer's pattern of permitting profanity in the workplace and lack of a policy prohibiting such language. *See Pier Sixty, LLC and Hernan Perez*, 362 NLRB 59 (2015) (after receiving a reprimand, employee posted on Facebook page that manager was "a NASTY MOTHER F*****. . .!!!! F*** his mother and his entire f****** family!!!!").

[7] O'Brien, Christine Neylon, The Top Ten NLRB Cases on Facebook Firings and Employer Social Media Policies (June 11, 2013). Forthcoming Oregon Law Review, Vol. 92, Issue 2, 2014. Available at SSRN: http://ssrn.com/abstract=2277900

disclosure of trade secrets, disparagement of employer's products or services or the products or services of a competitor, endorsements that do not adequately identify the source, and unauthorized posting of images or personal information of patients or co-workers.

- For medical practitioners especially, a social media policy must address HIPAA concerns and responsibilities. Even innocent and well-intended social media communications about patients can lead to HIPAA violations for employers. If writing about practice issues, employees should be instructed to write about fictionalized patients or post nothing without patient consent. Also, the practice's HIPAA policy should extend to all employees' online activity.

- A thorough social media policy should also address the FTC and endorsement issues discussed above. Practices should carefully set guidelines for employees on how to handle endorsement issues, but also make sure that your social media policy is not too broad that it could be construed to prohibit protected activities of employees under the NLRA. Recently, the NLRB has struck down social medial policies that require employees to post a disclaimer on social media sites, restrict discussions on wages and hours and prohibit employee use of company e-mail for "non-business purposes".

- While having a social media policy is helpful for employers, the big question is how do you enforce it and how do you monitor employee use? Keeping tabs on employees is a fine line. The courts in some cases uphold employee monitoring, particularly if the employer is monitoring their own equipment. However, the issue gets tricky when it comes to employees use of social media outside of work. The balance is between the employee's privacy rights and the employer's rights to property, to manage its public image, to thwart potentially damaging behavior and to ensure compliance with policies. If an employee's social media profile is unrestricted and public, an employer typically may access it and take the information into consideration when making certain determinations. The courts have found that an employee has no expectation of privacy in a posting if access is unrestricted and available to anyone who may have a computer. Many employees, however, restrict access to their social media profiles and accounts in some way by adjusting privacy settings so only their "friends" can see their profile. While using a fake name to gain access to an employee's site might seem an appealing solution to that problem, the federal Stored Communications Act makes it illegal to gain unauthorized access to electronic communications stored at a third-party communications provider and in at least one case, a court has found that using false pretenses, such as a fake account or other method to gain access, could amount to unauthorized access. When monitoring employee use of social media, employers should (i) make employees aware that anything they do on practice computers may be monitored; and (ii) have a monitoring policy in place that is consistently applied across the board for all employees.

- Last, but not least, in order to be effective, the policy should be consistently enforced within the office. It should also identify clear disciplinary action for violations, consistent with other employee policies and procedures then in effect.

III. Using Social Media in Hiring

a. Pros and Cons.

Social media and networking sites clearly open opportunities for employers in the hiring process that were not there before. Outlets such as LinkedIn allow employers to post job opportunities and search candidates. Posts regarding open positions on Facebook or Twitter can increase an employer's potential applicant pool to thousands of people instantaneously. However, the use of social media and its increased prevalence in the hiring process raises some legal concerns for employers, such as a duty to research applicants, compliance with the Fair Credit Reporting Act ("FCRA"), discrimination issues and reliability issues.

b. Researching Candidates.

Generally there is no duty to do any "searches" on a candidate. An employer does, however, have a legal duty to run a criminal background check on an applicant if (1) the employer learns facts indicating that the applicant may pose a threat to others; and (2) if the nature of the employee's potential work creates a serious risk of harm to third parties. Examples of such work would include employees of schools, security companies, childcare providers, and employees who have regular contact with children. In Pennsylvania, employees who have regular contact with children include hospital personnel, mental health professionals, and doctors. [8]

The ability to do "social searches" on a candidate for purposes of background screening raises issues under the FCRA. In July, 2011, the FTC published a letter regarding its investigation into whether an "internet and social media background screening service used by employers in pre-employment background screening" complied with the FCRA. The FTC's letter indicated that if an employer relies on a social search service, such as Social Intelligence, it runs the risk of that search not being compliant with the FCRA because services like that are considered to be a "consumer reporting agency". In order to be compliant under the FCRA, an employer would need to take the following steps regarding an applicant:

i. Make sure any notice and authorization presented to any applicant includes social media searches.

ii. If an applicant would be eliminated based upon the results of a social search, the employer must provide a pre-adverse action notice with a summary of the search performed, the FTC's "Summary of Rights Under the FCRA" and an opportunity to dispute the adverse action with the service provider who performed the social check.

iii. If the applicant is rejected, the employer should send a final adverse action notice to the applicant containing all language required by the FCRA.

The FCRA would only apply to social searches performed by a third party at the request of the employer and not those that are performed by the employer itself. However, all information obtained on a candidate in a social search should be carefully evaluated by the employer before it is considered. For example, social media posts may contain information that employers cannot lawfully consider, such as a disability, protected and lawful off duty conduct,

[8] *See* Pa. Cons. Stat. § 9125. Also in Pennsylvania, an applicant's criminal history record can be considered only to the extent that an individual's felony and misdemeanor convictions relate to the applicant's suitability for the specific position in question. If a decision not to hire is based in whole or in part on the applicant's criminal history, the applicant must be notified. *See* 18 P.S. § 9125.

or genetic information. In some cases knowledge of this information can even give rise to liability under state and federal discrimination laws. On the opposite end, information uncovered by a social search can no doubt warrant rejection of a candidate. Employers are cautioned to consider carefully the impact of the information found in performing social searches on potential employees.

iv. Passwords—Can you ask for them?

The answer is more and more becoming an unequivocal "no". This past summer, Washington State enacted a law pursuant to which an employer may not "[r]equest, require, or otherwise coerce an employee or applicant to disclose login information for the employee's or applicant's personal social networking account".[9] The law further prohibits requiring an employee or an applicant from accessing a social networking site in the employer's presence and requiring that the employee or the applicant "add a person, including the employer, to the list of contacts associated with the employee's or applicant's personal social networking account".[10] Other states, such as Oregon and Colorado are considering similar measures. Michigan, Illinois, California and Maryland have already enacted password protection statutes. The bottom line is that the trend is increasingly moving toward protecting this information and directly asking for it could easily subject an employer to liability even in jurisdictions where statutes have not yet been enacted.

v. Reliable Sources

Information found on social media sites is inherently unreliable. Social media itself is fraught with biased, opinionated and, sometimes, falsified information. Even if the employer only considers social media posts coming directly from the candidate and not third parties, there is still the risk that such information itself has been forged by the candidate or someone with unauthorized access to the candidate's account. The bottom line in balancing the concern of reliability versus the importance of probative information uncovered in a social search, is that if an employer is going to rely on a social search in evaluating and eliminating candidates, they would be well advised to provide applicants with pre-adverse notice of such action. Even if there is no legal obligation to do so, allowing an applicant the opportunity to explain the unfavorable information that is discovered opens up the ability of the employer to determine (1) if the information is falsified or otherwise misleading; and (2) to evaluate the employee's character in addressing the situation.

c. Recruitment and Advertising.

Social media sites like Twitter, Facebook and LinkedIn are excellent resources to use in the recruiting process. Advertising job openings is a quick, easy and cost effective way to attract interest and reach a larger candidate pool. Employers should, however, be aware of the legal concerns discussed above regarding discrimination and reliability of information obtained on social media sites in the hiring process when recruiting on social media sites. In addition, employers should make sure the settings on their own social media sites have the correct privacy settings to ensure protection against HIPAA violations and other potential breaches of confidential information.

The content of the recruitment advertisements should state that an employer is an equal employment opportunity employer, committed to providing all applicants fair and equal

[9] *See* WA ST § 49.44.0003.
[10] Id.

consideration without regard to race, religion, national origin, color, sex, age or disability. In addition, notices, postings, and advertisements must accurately and fairly reflect the functions of the job and the necessary qualifications to avoid false expectations.

IV. Malpractice Issues

As health care providers, physicians are able to use social media to reach patients in more ways than just in the exam room. It is no doubt that a large number of people use social media in their personal lives and, as with anything related to social media, it is catching on to professional use. Physicians are no exception. A recent survey in the ***Journal of Medical and Internet Research*** has shown that about one in four physicians use social media daily to explore medical information and fourteen percent (14%) use social media each day to contribute new information.[11] The increased use of social media provides many benefits to medical practitioners: it is a tool to connect with existing and potential patients, it allows them to provide pertinent medical information, engage in research, converse with colleagues, establish communication within the profession and advertise the medical practice. Nonetheless, the use of social media by health care providers does raise concerns related to HIPAA, violating professional responsibility, overstepping the boundaries between patients and their physicians, and, of course, potential liability.

The American Medical Association has issued an opinion favoring the use of social media in the medical practice. In so doing, the AMA recognizes that participation in social networks and other Internet usage "can support physicians' personal expression, enable individual physicians to have a professional presence online, foster collegiality and camaraderie within the profession, provide opportunity to widely disseminate public health messages and other health communication"[12] The AMA further recommends that physicians weigh the following factors in establishing their online presence:

- Be cognizant of standards of patient privacy and confidentiality that must be maintained in all environments, including online, and refrain from posting identifiable patient information online.

- When using the Internet for social networking, physicians should use privacy settings to safeguard personal information and content to the extent possible, but should realize that privacy settings are not absolute and that once on the Internet, content is likely there permanently. Thus, physicians should routinely monitor their own Internet presence to ensure that the personal and professional information on their own sites and, to the extent possible, content posted about them by others, is accurate and appropriate.

- If they interact with patients on the Internet, physicians must maintain appropriate boundaries of the patient-physician relationship in accordance with professional ethical guidelines just as they would in any other context.

- To maintain appropriate professional boundaries, physicians should consider separating personal and professional content online.

---

[11] Brian S McGowan, Molly Wasko, Bryan Steven Vartabedian, Robert S Miller, Desirae D Freiherr, Maziar Abdolrasulnia, Understanding the Factors That Influence the Adoption and Meaningful Use of Social Media by Physicians to Share Medical Information, J Med Internet Res 2012 (Sep 24); 14(5):e117

[12] American Medical Association Opinion 9.124, Professionalism in the Use of Social Media, June, 2011.

- When physicians see content posted by colleagues that appears unprofessional, they have a responsibility to bring that content to the attention of the individual, so that he or she can remove it and/or take other appropriate actions. If the behavior significantly violates professional norms and the individual does not take appropriate action to resolve the situation, the physician should report the matter to appropriate authorities.

- Physicians must recognize that actions online and content posted may negatively affect their reputations among patients and colleagues, may have consequences for their medical careers (particularly for physicians-in-training and medical students), and can undermine public trust in the medical profession.[13]

Based upon the AMA's guidance, it is clear that any presence online by a medical practitioner should avoid giving specific medical advice via the internet or social media; never disclose specific patient information in a social media setting without consent; keep personal social media use separate from any professional use; and be vigilant about checking privacy settings on social media sites. The use of the internet and social media present major concerns for physicians in the area of professional responsibility, malpractice liability and unauthorized disclosures under HIPAA. Those concerns, however, should not discourage physicians from taking advantage of the upsides to using social media for health care providers.

V. Regulatory Concerns

a. Daily Deal Websites

Daily deal websites such as Groupon and Living Social are sites that offer discounted services or products from local business' to consumers. It is a business that is constantly growing. The websites work by having local businesses advertise discount rates for services (i.e money off a certain procedure). The site then pays the business 50% of the amounts they collect from the coupons. Many health care providers view these deal-of-the-day websites as a great way to market and also fill up empty appointment slots. However, these sites can also cause issues for a practice if too many coupons are sold and the practice cannot keep up with the volume of new patients. It could ultimately tarnish a practices' reputation. There are also several regulatory concerns surrounding these sites.

i. Fee Splitting

Medical practices use of deal-of-the-day website could create fee-splitting arrangements, which are prohibited in many states. Also the AMA considers fee-splitting to be unethical. Since the deal website retains part of the payment, which technically is a part of the fee the health care provider would have generated, depending on the state, this may equal to a fee-splitting arrangement.

Many state licensing agencies have already issued rulings regarding if they consider these types of arrangements illegal. States such as Illinois issued a rule that stated advertising on daily deal websites did not constitute fee-splitting, so long as the vouchers include the following:

[13] Id.

- A description of the discounted price in comparison to the actual cost of services;
- A disclosure that patients should not make health care decisions in haste; and
- A disclosure to prospective patients that the patient's purchase price will be refunded in its entirety if it is later determined that the patient is not a candidate for the vouchered service.

States such as North Carolina have similar regulations. It is pertinent that health care providers consult their state regulations or consult with their attorney prior to creating coupons on one of these websites.

ii. Federal Anti-Kickback Statue

The Federal Anti-Kickback Statue ("AKS") prohibits the payment or receipt of kickbacks, or remuneration, in return for or to induce the referral of Medicare or Medicaid business. The AKS also prohibits the offer or payment of any remuneration to any person to induce the person to purchase or recommend purchasing any service for which payment may be made in whole or in part under a Federal health care program.[14]

The Office of Inspector General ("OIG") addressed this topic in an Advisory Opinion issued in March, 2012. The opinion did not directly address daily deal sites, yet did discuss how proposed arrangements that allowed providers to offer coupons and advertisement on a website were low risk under the AKS. They based this on the following factors:

- the coupon website is not a health care provider or supplier;
- the payments from providers and advertisers to the company do not depend in any way on consumers using the coupons or obtaining services from the providers or advertisers;
- the consumers remain relatively anonymous, and other than through a consumers' use of keyword search, no advertisement would be specifically directed at any particular consumer; and
- the proposed arrangement required no up-front investment by the patient.

The OIG concluded that the proposed website acted as more of general avenue for providers to advertise, rather than a website providing remuneration to a beneficiary in order to induce their choice.

Although the OIG considers these websites low-risk, it is still possible that payment made to or retained by a deal-of-the-day site could be determined to violate the AKS. Medical practices must be aware of the risk associated with these websites. Failure to conduct

[14] 42 U.S.C. § 1320a-7b

proper due diligence prior to participating in a daily deal site may put a practice at risk for violating the AKS.

VI. Conclusion

As social media use increases and becomes more prevalent, medical practices need to be aware of the risks of social media and the best ways to plan for and prevent mishaps from occurring.