Fear of Facebook: Private Ordering of Social Media Risks Incurred by Healthcare Providers

Nicolas P Terry

Available at: https://works.bepress.com/nicolas_terry/3/
Fear of Facebook: Private Ordering of Social Media Risks Incurred by Healthcare Providers*

Nicolas P. Terry**

I. INTRODUCTION .................................................................................................................. 1

II. SOCIAL MEDIA AND HEALTHCARE WORKERS MISBEHAVING ........................................ 2
   A. SOCIAL MEDIA’S EXPONENTIAL GROWTH ............................................................................... 2
   B. HEALTHCARE PROVIDERS MISBEHAVING ONLINE .............................................................. 5

III. ETHICAL CODES AND PROVIDER POLICIES ...................................................................... 7
   A. ETHICAL GUIDELINES ............................................................................................................. 8
   B. EMPLOYER SOCIAL MEDIA POLICIES ...................................................................................... 12
   C. ASSESSING LEGAL LIMITS ON POLICIES .............................................................................. 15

IV. PROVIDER ACCESS TO PATIENT SOCIAL MEDIA DATA ...................................................... 20
   A. FROM VOUEREISM TO OBLIGATION ....................................................................................... 20
   B. RISK MANAGING ACCESS ................................................................................................. 25

V. REGULATING FRIENDSHIPS AND CONTROLLING ADVERSE FEEDBACK ............................. 26
   A. REVISITING THE “BOUNDARY” ISSUE ................................................................................... 26
   B. PROVIDER COMPARISON SITES .......................................................................................... 30
   C. SOCIAL MEDIA GAG AGREEMENTS ....................................................................................... 34

VI. CONCLUSION ..................................................................................................................... 40

I. Introduction

In a prior article, I identified four scenarios where doctors and patients faced legal or ethical peril because of their participation in social media. The imperiled scenarios described were physicians posting their social information online, patients exposing their own health-related information online, physicians and patients becoming social networking “friends,” and physicians “tweeting” or wall-posting about their work.

In the two years that have passed since that article was written, the unique or heightened risks associated with data posted on profile pages or interactions within those “walled gardens” have become widely appreciated. Equally, some of the previously identified pitfalls for professionals have materialized. In particular, online activities by healthcare professionals have increasingly jeopardized patient confidentiality. Other scenarios, happily, do not seem to have gained much traction.

*Copyright © 2011, Nicolas P. Terry. All Rights Reserved.
** Chester A. Myers Professor of Law, Saint Louis University. Email: terry@slu.edu. I thank Colleen Zern, Amanda Wong, and Professor Margaret McDermott for their excellent research assistance.
2 Constructing a Legal Framework, supra note 1, at 288.
For example, tweeting from the operating theater seems to be more popular on Grey’s Anatomy than in real life.\(^3\)

The last two years have seen important quantitative and qualitative shifts in social media use patterns as well as a rapid deployment of private ordering: social media policies and other contractual constructs emanating from physicians, professional organizations, employers and educators. Yet, these private, often contractual attempts to regulate online interactions or social media conduct are not all benign, themselves creating ethical or legal risk.

In this article I concentrate on social media and these new risk management constructs and do so primarily from the perspective of physicians. Part II provides updated statistics on Internet use by healthcare workers and explores some of the scenarios that have led medical schools and healthcare entities to expressly address social media behavior. Part III inquires into how professional organizations or those who employ or credential physicians have attempted to change the rules of the game by promulgating social media policies and analyses some of the legal constraints on those policies. Part IV deals with the reality of medically relevant information about patients increasingly moving online and asks whether physicians should attempt to access information that might be useful or even life-saving. Finally, Part V describes how the patient-physician dialog has increasingly spilled out of the consulting room and onto social media sites and explores how physicians should react not only to overtures for social media friendship but also to online critical patient comments.

II. Social Media and Healthcare Workers Misbehaving

A. Social Media’s Exponential Growth

In the last two years, the growth of social media has been relentless, with Facebook alone gaining 250 million users. Facebook has only been in existence for six years yet has as many as 750 million users worldwide\(^4\) and as many as 157.2 million U.S. visitors per month.\(^5\) Twitter, at only five-years-old now, has 200 million users.\(^6\) Membership numbers aside, the traditional web metric of unique visitors is

---


\(^4\) Jason Kincaid, *Facebook Now Has 750 Million Users*, TECHCRUNCH (June 23, 2011),

\(^5\) Andrew Lipsman, *The Network Effect: Facebook, Linkedin, Twitter & Tumblr Reach New Heights in May*, COMSCORE (June 15, 2011),

also telling, with Facebook receiving 590 million unique visits per month, Twitter 97 million, and the professional-oriented LinkedIn 41 million.7

This growth is showing few signs of slowing. Obviously the total number of users is capped, and Facebook is already reaching 73% of the U.S. Internet population.8 As a result, future growth will come in the time spent connected to social networks as they become core communications platforms. For example, Comscore reports “Facebook’s average U.S. visitor engagement has grown from 4.6 hours to 6.3 hours per month over the past year.”9 Social media platforms are growing by adding messaging,10 search,11 and video communication.12 It has been predicted that “20 percent of business users will use social networks as their primary means of business communications by 2014.”13 This is based in part on the tighter integration of mobile devices, such as smartphones with address books, and on messaging over social media services.14

The uses for social media are broadening, as are the demographics of active users.15 We have known for some time that the majority (and a steadily increasing number) of Americans seek medical information on the Internet.16

Social media still lags behind “traditional” Internet destinations (such as established health web sites) for researching health information, although the gap is

---


8 Lipsman, supra note 5.

9 Id.


13 Brad Reed, Gartner: Social Networking Slowly Taking Over E-mail, MACWORLD (Nov. 11, 2010, 3:50 PM), http://www.macworld.com/article/155663/2010/11/email_socialnetworking.html?src=rss_main.; See also, Brian Barrett, Facebook Messages: Every Email, Text, and Chat in One Place, GIZMODO (Nov. 15, 2010, 1:00 PM), http://gizmodo.com/#i5690405/facebook-email (“Facebook’s looking towards the future, towards a generation that’s steadily and increasingly been abandoning email for instant communication. And the more we abandon email for text and chat, the more Facebook’s going to be the communication hub.”).

14 Reed, supra note 13.


narrowing. According to one 2009 survey, 35% of U.S. adults now use social media to acquire such information. A 2011 survey by National Research Corporation suggests that 20% of Americans use social media websites as a source of healthcare information, with 94% of respondents saying they use Facebook for that purpose. Trust in these sites also is increasing, though it lags behind that expressed towards hospital web sites. Pew’s Social Life of Health Information report for 2011 found that of adults who use social network sites (46% of all adults in the US), only a relatively small number (11% of adults) followed their friends’ personal health experiences and only 7% used social media to acquire health information. Another 2011 poll suggested that 85% of surveyed Americans were not yet ready to use social media or instant messaging conduits to communicate with their doctors. However, a 2011 survey by Intuit Health found that 73% of Americans would use a secure online communication conduit with their doctor to, for example, get lab results or to make appointments.

The Pew report, noted above, found a larger utilization of social media for health information and support by caregivers than by the general population (20% of caregivers who use social network sites use them to acquire health information, compared with 12% of other users). Those users are also likely to be heavy users of narrowcast social media sites aimed at those, say, who suffer from or support sufferers of particular diseases. Some of these are crowd-sourced sites such as Patients Like Me, use social media to create support and advocacy groups and to

---

20 Id.
24 Fox, supra note 21, at 7.
accelerate clinical trials.27 Other narrowcast sites have a less organic background, such as Diabetic Connect28 and other sites built by Alliance Health Networks.29

The trend lines are unmistakable and remarkable. As people spend more time in social media, they will have more of their health-related experiences there as they gather and disseminate information (and misinformation). And, as patients turn towards social media, healthcare providers seem happy to provide an expanding number of destinations. Over 3,000 hospitals now have social networking sites including over 700 Facebook pages and almost as many Twitter feeds.30 Exactly how many physicians use social media is difficult to determine. However, a survey published in 2011 concluded that personal use of social media by medical students and physicians mirrors that of the general population (with almost all medical students and 42% of physicians being on social media).31 One aggregation site listed more than 1300 doctors actively using Twitter,32 while one research study analyzed Twitter feeds from 260 self-identified doctors with more than 500 followers each.33 Another study found that 44.5% of medical trainees had a Facebook account and that medical students were more frequent users than residents.34 Even the Centers for Disease Control and Prevention has published a toolkit addressed to providers promoting the use of social media “as part of an integrated health communications program.”35

B. Healthcare Providers Misbehaving Online

Recently, the American College of Physician Executives published a study of offline disruptive conduct by physicians.36 More than 70% of physicians say that disruptive physician behavior occurs at least once a month at their organizations. These behaviors include degrading comments and insults (observed by 59% of physicians), yelling (54%), discrimination (24%), inappropriate jokes (40%), profanity (41%), and spreading malicious rumors (21%).37 Unsurprisingly, similar behaviors occur online on social media platforms.

33 Katherine C. Chretien et al., Physicians on Twitter, 305(6) JAMA 566, 566-68 (2011).
34 Lindsay A. Thompson et al., The Intersection of Online Social Networking with Medical Professionalism, 23(7) J. GEN. INTERNAL MED. 954, 955 (2008).
37 Id. at 2-4.
A 2007 cross-sectional analysis of medical students and residents at the University of Florida found that the majority of accounts (83.3%) listed at least one form of personally identifiable information, that only a third (37.5%) were made private, and that some accounts displayed potentially unprofessional material. A 2010 follow-up study examined photographs published on those accounts and found a number of identifiable patient photographs involving children treated on a medical “mission.” A similar study of young New Zealand doctors found that 65% had Facebook accounts and that 37% of those Facebook users failed to use privacy settings. Exposed information was described as including “personal information that might cause distress to patients or alter the professional boundary between patient and practitioner, as well as information that could bring the profession into disrepute.”

60% of medical schools responding to another study reported incidents of students posting unprofessional online content. Violations of patient confidentiality were reported by 13% (6/46). Student use of profanity (52%; 22/42), frankly discriminatory language (48%; 19/40), depiction of intoxication (39%; 17/44), and sexually suggestive material (38%; 16/42) were commonly reported. Of 45 schools that reported an incident and responded to the question about disciplinary actions, 30 gave informal warnings (67%) and 3 reported student dismissal (7%). In 2011, two Baylor medical students faced disciplinary proceedings for a two year-old video taken at a private party that subsequently was uploaded to YouTube. The video apparently was offensive to Hispanic and poor patients at Ben Taub General Hospital.

Graduation is not necessarily a watershed. A recent study of tweets by 260 self-identified doctors on Twitter characterized 3% as “unprofessional,” 0.6% contained profanity, 0.3% contained sexually explicit content, 0.1% contained discriminatory content, and 0.7% involved a potential privacy violation. Increasingly, such behavior by healthcare workers is attracting adverse employment or credentialing decisions by hospitals. For example, in 2009 two nurses were terminated by Mercy Walworth Medical Center after photographing an

38 Thompson, supra note 34, at 955-56.
40 Joanna MacDonald et al., Privacy, Professionalism, and Facebook: a Dilemma for Young Doctors, 44 MED. EDUC. 805, 805 (2010).
41 Katherine C. Chretien et al., Online Posting of Unprofessional Content by Medical Students, 302 JAMA 1309, 1309 (2009).
43 See Jeanne M. Farnan et al., The YouTube Generation Implications for Medical Professionalism, 51 PERSP. BIOLOGY & MED. 517, 517-24 (A far more positive narrative about how an online video medical student project was used as a case study for developing responsible social media policies).
44 Katherine C. Chretien et al., Physicians on Twitter, 305 JAMA 566, 567 (2011) (the study was limited to those with more than 500 followers).
X-ray showing a sexual device lodged in a patient’s rectum; one picture was allegedly posted on a Facebook page and discussed on another. In April 2010, four staff members were fired and three disciplined at St. Mary Medical Center in Long Beach, California. Allegedly the staff members had taken pictures of a dying man who had been savagely attacked and then posted them on Facebook. In June 2010, Tri-City Medical Center in Oceanside, California terminated five nurses for discussing patients on Facebook.

Even apparently benign behavior involving social media is attracting adverse reactions. For example, in November 2008, nurses at a Fargo, North Dakota system used Facebook to provide unauthorized shift change updates to their co-workers. In 2011, Westerly Hospital in Rhode Island terminated the clinical privileges of a 48-year-old emergency medicine physician and reported her to the state licensing board. The physician had written about some of her clinical experiences on Facebook albeit without using patient names or intending to reveal patient information. Subsequently, a third party was able to identify one of the patients because of the nature of an injury described. In a consent agreement with the licensing board, the physician accepted a reprimand for unprofessional conduct, paid $500 in administrative costs, and agreed to attend a Continuing Medical Education session dealing with patient confidentiality.

III. Ethical Codes and Provider Policies

Divorce lawyers aside, employers were one of the first groups to leverage social media by including online data in their background checks. The majority of

---

47 Id. See also Roger Boyes, And This is Me on Facebook . . . Helping with Brain Surgery, TIMES (Aug. 18, 2008), http://www.timesonline.co.uk/tol/news/world/europe/article4560908.ece (Swedish nurse suspended after posting photographs of brain and back surgeries on her Facebook page).
51 See generally Belinda Luscombe, Facebook and Divorce: Airing the Dirty Laundry, TIME (Jun. 22, 2009), http://www.time.com/time/magazine/article/0,9171,1904147,00.html#ixzz1KZ8L7kVW; Leanne Italie, Facebook is Divorce Lawyers’ New Best Friend, MSNBC (June 28, 2010), http://www.msnbc.msn.com/id/37986320/ns/technology_and_science-tech_and_gadgets/;
employers now include social media in their screening processes. In the healthcare environment, the seriousness of background checks has been further promoted by the growth of the negligent credentialing cause of action and the concomitant duties of disclosure placed on prior healthcare employers. While only the occasional physician recruit will leave behind social media evidence of an interest in witchcraft or “pictures of her topless and drinking from beer bongs” for a recruiting firm to discover, zero tolerance for inappropriate social media behavior is becoming the norm.

This section analyses the recently published AMA Policy Professionalism in the Use of Social Media and healthcare employer policies and questions whether there are any legal limitations on such polices.

A. Ethical Guidelines

The legal profession generally got out in front of the medical profession in confronting the professionalism issue with social media. For example, in 2009 the Florida Supreme Court Judicial Ethics Advisory Committee considered the question of judges “friending” lawyers who might appear before the judge and concluded that “identification [as a “friend”] in a public forum of a lawyer who may appear before the judge does convey [the] impression [that the lawyer is in a position to influence


53 See, e.g., Larson v. Wasemiller, 738 N.W.2d 300, 306 (Minn. 2007).

54 Consider the undervalued Kadlec Med. Ctr. v. Lakeview Anesthesia Assocs., 527 F.3d 412 (5th Cir. 2008), holding that there could be liability for letters that were affirmatively misleading but that the defendants had no affirmative duty to disclose (referencing a form letter that was sent to the hospital by the Practice Group that confirmed the doctor’s prior privileges but said no more). I agree with Sallie Sanford’s argument that Kadlec notwithstanding “a requirement of greater candor is likely to be adopted either in a subsequent case, by statute, or through hospital accreditation standards.” Sallie Sanford, Candor After Kadlec: Why, Despite the Fifth Circuit’s Decision, Hospitals Should Anticipate an Expanded Obligation to Disclose Risky Physician Behavior, 1 DREXEL L. REV. 383, 386 (2009).


the judge] and therefore is not permitted.” Other judicial ethics advisory committees have been less absolute. For example, South Carolina permits social media relationships between a magistrate and law enforcement officers “as long as they do not discuss anything related to the judge’s position as magistrate.” New York held that there was nothing “inherently inappropriate” about a judge joining a social network but cautioned, “[a] judge must … consider whether any such online connections, alone or in combination with other facts, rise to the level of a ‘close social relationship’ requiring disclosure and/or recusal.”

At its mid-year meeting in November 2010, the AMA adopted its first policy on physician use of social media. At that time an AMA board member noted, “[u]sing social media can help physicians create a professional presence online, express their personal views and foster relationships, but it can also create new challenges for the patient-physician relationship.”

The AMA’s policy contains six sections with provisions that range from highly generalized statements to specific admonitions going to both process and substance. The most general statements are contained in the final section of the policy:

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.

The policy also makes clear that the responsibility for navigating the challenges posed by social media rests not only with individual physicians, but also with the profession generally. Thus, physicians have an obligation to bring

---


unprofessional content to the attention of posting colleagues and, if that fails to resolve the situation, to “report the matter to appropriate authorities.” The substantive provisions of the AMA Policy relate to the privacy and confidentiality of identifiable patient data, the utilization of privacy and security settings combined with the obligation to self-audit, and the maintenance of appropriate boundaries with patients, preferably by separating the personal from the professional.

Emerging policies and best practices emphasize the importance of physicians avoiding posts about patients. Thus, the AMA Policy statement provides that “[p]hysicians should be cognizant of standards of patient privacy and confidentiality that must be maintained in all environments, including online, and must refrain from posting identifiable patient information online.”

A small number of state medical associations have also provided information to physicians regarding the use of social media. In May 2011, the Massachusetts Medical Society published Social Media Guidelines for Physicians. The Guidelines closely track the AMA policy. Indeed, the first three guidelines (stressing confidentiality, using available privacy and security settings, and maintaining appropriate physician-patient boundaries) are worded identically. Massachusetts expands on the fourth AMA policy (separate professional and personal social media sites) with the statement “[p]hysicians should accept patient online invitations to connect only on a physician’s professional social networking site, and should not accept invitations from patients to connect on personal networking sites.” The two policies use similar wording to emphasize that physicians owe a professional responsibility to advise and, if necessary, report their colleagues’ inappropriate use of social media and to employ identical wording on their exhortation as to the reputational impact of their online activities. The Massachusetts policy adds an additional paragraph dealing with potential conflicts of interest as follows:

Physicians must disclose all financial or other material relationships they have with regard to the maker or provider of

64 AMA Policy: Professionalism in the Use of Social Media, supra note 61.
65 Id. (“(a) Physicians should be cognizant of standards of patient privacy and confidentiality that must be maintained in all environments, including online, and must refrain from posting identifiable patient information online.”)
66 Id. (“(b) 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.”)
67 Id. (“(c) 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.”)
68 Id. (“(d) To maintain appropriate professional boundaries physicians should consider separating personal and professional content online.”)
69 Id.
products and services they review or discuss in online communities. This includes discussions and reviews of products and services provided to the physician for free.\textsuperscript{71}

Additional useful caveats are to be found in the social media guide jointly prepared by the Australian and New Zealand medical associations.\textsuperscript{72} For example, compared to U.S. models their guide includes a more perceptive and informative explanation of the confidentiality challenges when alluding to patients on social media.

The accessibility and indexability of online information means that although a single posting on a social networking website may be sufficiently de-identified in its own right, this may be compromised by other postings on the same website, which are just a mouse click away.

In maintaining confidentiality, you must ensure that any patient or situation cannot be identified by the sum of information available online.\textsuperscript{73}

Although designed to address professionalism and ethical behavior, the AMA and state medical association policies are likely to have ramifications outside the ethics space. The AMA Policy, in particular, likely will be incorporated by reference into employment and credentialing agreements, and, of course, a few states already incorporate AMA ethical standards into their licensure standards.\textsuperscript{74} It is also likely that such policies will not only be admitted in actions complaining of physician conduct in social media cases but also will influence emerging common law standards.\textsuperscript{75}


\textsuperscript{73} Id. at 3 (emphasis in original).


\textsuperscript{75} See e.g., Hall v. Anwar, 774 So. 2d 41 (Fla. App. 2000) (discussing role of testimony of medical ethicist in medical malpractice case); Perna v. Pirozzi, 457 A.2d 431 (N.J. 1983) (AMA ethical standard E-8.16, applied in case as basis for the duty of the doctor to provide his or her personal services in accordance with the agreement with the patient); Neade v. Portes, 710 N.E.2d 418 (Ill. App. Ct. 1999) (“assure disclosure of any financial inducements” in Current Opinions § 8.132 used to support state cause of action for breach of fiduciary duty); Ketchup v. Howard, 543 S.E.2d 372 (Ga. Ct. App. 2000) (Code of Medical Ethics sets forth the medical profession’s standard on informed consent); Cf. Frey v. Goshow-Harris, No. 06C-01-057 J0H, 2009 WL 2963789 (Del. Super. Ct. 2009) (AMA ethical standard E-8.16, Substitution of Surgeon without Patient’s Knowledge or Consent, ruled not to be relevant to case or if relevant likely to confuse jury); Hartsell v. Fort Sanders Reg’l Med. Ctr., 905 S.W.2d 944
B. Employer Social Media Policies

One of the major reasons that professional bodies such as the ABA and the AMA are developing ethical codes for social media interactions by their members is that these bodies have long policed professional advertising. Social media is quickly becoming one of the most popular places for advertising and other forms of marketing. In fact, the likely onslaught of social media advertising that we are about to see must inform (in part driven by increasingly sophisticated location-based services) our analysis of the present, somewhat more benign, social media world that healthcare currently confronts.

Social media advertising and marketing is designed to monetize the new platforms. Recall the tough but accurate portrait painted by one commentator about Facebook:

[T]he whole point about Facebook is that users aren’t customers. Anyone who supposes that Facebook’s users are its customer has got the business model precisely backwards. Users pay nothing, because we aren’t customers, but product. The customers are the advertisers to whom Facebook sells the information users hand over, knowingly or not.76

Thus, developing ethical codes must be seen, at least in part, as a prophylactic reaction to how social media will present when fully monetized. It also explains the growth in employer policies that seek to regulate employee conduct online. Such regulation, again at least in part, is driven by the employers’ desire to control messaging about the employers’ goods or services.

Most of the troubling behaviors on social media that led to providers disciplining staff or terminating clinical privileges have involved potential privacy violations. In 2009, the HITECH Act strengthened HIPAA enforcement,77 and Secretary Sibelius consolidated security and privacy enforcement in the Office of Civil Rights (OCR).78 In its “statement” case against Cignet Health of Prince George’s County, Maryland OCR imposed a $4.3 million civil money penalty for HIPAA

---

76 Andrew Brown, Facebook is Not Your Friend, GUARDIAN.CO.UK (May 14, 2010, 5:30 PM), http://www.guardian.co.uk/commentisfree/andrewbrown/2010/may/14/facebook-not-your-friend; A similar sentiment has been expressed by Mike Elgan, Google’s Business Model: YOU Are the Product, DATAMATION (Feb. 5, 2009), http://itmanagement.earthweb.com/columns/executive_tech/article.php/3801006/Googles-Business-Model-YOU-Are-the-Product.htm (“Advertisers are Google's customer. What do they sell to advertisers? They sell you. Or, at least, they rent you out, or provide access to you.”).


violations.\textsuperscript{79} In July 2011, UCLA settled potential HIPAA violations for $865,500 stemming from unauthorized employee views of celebrity and other patients.\textsuperscript{80} Going forward, healthcare entities will likely be far more diligent about protecting patient privacy. This will probably include promulgating strengthened student, credentialing, and employment policies.

\textit{Byrnes v. Johnson County Community College} illustrates the necessity for such policies.\textsuperscript{81} The plaintiff was a nursing student enrolled at the defendant community college. With some other students and an instructor, she attended an obstetrics course at a local health system. The instructor permitted the students to be photographed with an unidentified placenta. After the students posted the photographs to Facebook, they were dismissed from the school and the plaintiff successfully applied for injunctive relief. The court noted:

Neither defendant JCCC's Nursing Student Code of Conduct nor any other code of conduct relating to JCCC and/or its nursing school regulates student photography of classroom or clinical events, nor prohibits the transmittal of photographs to others, including through social media such as \textit{Facebook}. The "violation" which the Plaintiff and other students committed was not of a published code of conduct, but of the sense of propriety of Defendants... Such standards are unclear, unpublished, and unfair to require students to comply with.\textsuperscript{82}

Almost all US medical schools now have guidelines or policies for their students relating to Internet use. However, relatively few deal specifically with social media.\textsuperscript{83} Two notable exceptions are the social media policies posted by the Indiana University School of Medicine\textsuperscript{84} and Mount Sinai School of Medicine.\textsuperscript{85} Both contain compelling guidelines suggesting best practices for the use of social media by medical students. For example, the Indiana policy stresses professionalism and the challenges of an online world where "the lines between public and private,

\begin{itemize}
  \item No. 10-2690-EFM-DJW (D. Kan. 2011).
  \item Id. at 3.
\end{itemize}
personal and professional are blurred.” It recommends constant review and audit of the user's online presence, the un-tagging of photographs posted by others, and strongly discourages social media interactions with patients.

The Mount Sinai Guidelines include an Addendum containing fictional case examples. These hypotheticals include suggested approaches to a patient attempting to “friend” a physician, a pediatric resident posting the picture of a recently discharged infant patient, and a photograph posted on Facebook of an inebriated student wearing a Mount Sinai t-shirt.

Given the regulatory environment, patient privacy remains the dominant driver behind employment and educational social media policies. However, it is not the only driver. Just as physicians seek to control the message about the quality of their services and the collision course they find themselves on with opinion sites as discussed below, so the recent proliferation of employment-based social media policies has been driven not only by risk management concerns but also by a desire to control the institution's social media message.

Social media policies are proliferating rapidly and generally will be designed to project the issues, norms, and values of individual healthcare entities. Notwithstanding, some provisions seem to be common across a sample of policies. First, most policies for social media postings insist upon expressing a clear distinction for employees between acting in a private capacity and acting in an official capacity or representing the entity. There will usually be a requirement that social media generated internally (including links to outside sites) must be expressly approved by the entity's communications department. Second, a typical policy will encourage good social media behavior, for example, by stressing accuracy and respect for co-workers and customers and by requiring an appropriate balance between social media usage and work commitments (some policies may even

---

86 Guidelines for Use of Online Social Networks for Medical Students and Physicians-in-Training, supra note 84, at 3.
87 Mount Sinai Medical Center Social Media Guideline, supra note 85, Addendum to Social Media Guideline.
88 See infra text accompanying note 226 et seq.
prohibit access to social media during work hours). Third, policies tend to highlight some specific legal restrictions. Thus, HIPAA compliance is likely to be mentioned accompanied by an express prohibition on posting identifiable information. Most policies explicitly ban abusive, profane, threatening, or offensive posts. Posting of copyright material also is likely to be expressly prohibited whereas the entity is likely to claim ownership of all posted material. Finally, most policies expressly note that violations will result in discipline or in termination of employment or clinical privileges. Some policies will also contain indemnity clauses.

One issue that not all policies yet address is the extent to which these behavioral restrictions apply to social media use outside business hours. The Kaiser Permanente policy addresses this as follows:

This policy applies to employees using social media while at work. It also applies to the use of social media when away from work, when the employee’s Kaiser Permanente affiliation is identified, known, or presumed. It does not apply to content that is non-health care related or is otherwise unrelated to Kaiser Permanente.91

The Ohio State Medical Association’s policy statement includes a sample policy on “Restricted Use at Work.”92 The section dealing with employee usage on personal property prohibits posts of proprietary information, information about patients covered by privacy laws, and “material that is fraudulent, harassing, embarrassing, sexually explicit, obscene, intimidating or defamatory against any other person employed by [Business].” While such restrictions may seem rooted in a sensible policy more draconian models will no doubt follow. Thus, the branch of one business that has experienced boundary issues, the Kentucky Annual Conference of the United Methodist Church, requires the passwords to all its clergy members’ social media sites and that the member add the Conference as a “friend.”93

As will be seen in the next section, this is an issue that has considerable legal significance as healthcare entities seek to control activities occurring outside the workplace and/or on social media not directly controlled by the entity.

C. Assessing Legal Limits on Policies

As school and employer-generated social media policies proliferate, the question arises as to whether there are any legal limits on their application. Some broad theories have been argued. For example, in Esfeller v. O’Keefe,94 a student at a state university allegedly harassed and threatened his ex-girlfriend on social media sites. The university investigated his conduct, and a hearing panel found him in

---

92 OSMA LEGAL SERVS. GRP., supra note, 71 at 8.
94 391 F. App’x. 337 (5th Cir. 2010).
violation of the institution’s Code of Conduct. In his suit, the plaintiff alleged various civil rights and constitutional challenges to the code provision prohibiting “extreme, outrageous or persistent acts, or communications that are intended or reasonably likely to harass, intimidate, harm, or humiliate another.” His core argument was that this provision was facially and as-applied overbroad and vague. The court noted that although the Code was broadly aimed at speech or conduct “that creates an intimidating, hostile, or offensive environment,” the prohibition required the expression “to be “persistent, extreme or outrageous and “reasonably likely” to cause harassment or intimidation.” As a result the court was able to conclude that the Code was directed “at speech that ‘intrudes upon ... the rights of other students’ and is legitimately subject to regulation.”

Two more narrowly drawn limitations promise more traction: one operating on labor law principles and the other based on some privacy principles and legislation.

1. Labor Law

Employers leveraging social media policies may run afoul of several employment and labor law principles. For example, *Gaskell v. University of Kentucky* was an employment discrimination case brought by an unsuccessful candidate to be the defendant’s observatory director. The search process followed conventional academic processes until a member of the search committee conducted an Internet search on the plaintiff and found information on his personal web site that led some to characterize him as creationist (which he denied). The court held that there was sufficient direct evidence of Title VII discrimination against the university. As employers increasingly scrape data about potential employees from social media sites they are at peril when they make improper use of some types of data. Risk management strategies include the adoption of (non-discriminatory) written and exclusive criteria for hiring decisions and the building of a firewall between a search committee and HR professionals tasked with performing background checks.

Both employees and potential employees may be protected under state non-work hours statutes. For example, the Colorado legislation provides “[i]t shall be a discriminatory or unfair employment practice for an employer to terminate the employment of any employee due to that employee’s engaging in any lawful activity off the premises of the employer during nonworking hours....” A narrower species of behavioral immunity applies in some states to non-work consumption of lawful products such as alcohol. Notwithstanding, these statutes tend to have safe harbors for employers in cases that impinge upon critical employer responsibilities.

---

95 *Id.* at 341.
96 *No. 09-244-KSF* (E.D. Ky. 2010).
97 *Id.* at 9.
99 See e.g., 820 ILCS 55 § 5.
100 See e.g., *Colo. Rev. Stat.* § 24-34-402.5(1)(a)(b) (2010).
The National Labor Relations Act (NLRA) may have the most immediate impact and may cause employers to revise their social media policies or their enforcement. Section 7 provides that “[e]mployees shall have the right to self-organization, to form, join, or assist labor organizations, to bargain collectively through representatives of their own choosing, and to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection.” 101 Section 8(a)(1) of the same Act provides that “[i]t shall be an unfair labor practice for an employer (1) to interfere with, restrain, or coerce employees in the exercise of the rights guaranteed in section [7].” 102

In Guard Publishing Co. v. National Labor Relations Board, 103 the National Labor Relations Board (NLRB) found that an Oregon newspaper committed unfair labor practices when it disciplined a copy editor, the paper's union president, for sending a union-related email to her fellow employees. An administrative law judge found that the paper had not violated the NLRA merely by maintaining an email policy but found it did violate the act by discriminatorily enforcing the policy to prohibit union-related e-mails while allowing a variety of non-work-related e-mails. 104 NLRB broadly concurred with those findings except in holding that there was no evidence that the employer allowed emails to solicit or support non-union organizations. The DC Circuit disagreed on this point on the basis that neither “the company's written policy nor its express enforcement rationales relied on an organizational justification” and that “the only employee e-mails that had ever led to discipline were the union-related e-mails at issue here.” 105

It appears that the NLRB has been seeking to test the extent to which these principles apply to social media policies and employee discussions on social media relating to employment conditions. In the Board’s so-called “Facebook Case” (against American Medical Response of Connecticut, LLC) a healthcare worker allegedly was discharged after posting negative comments about a supervisor on a personal Facebook page. The board alleged that the company had an overly broad social media policy regarding blogging, Internet posting, and communications between employees contrary to Section 8(a)(1). However, the case settled in February 2011 when the company apparently agreed to rescind and revise its policy. 106 In an advice memorandum published on April 21, 2011, the NLRB commented on the dismissal of newspaper reporter for posting unprofessional and inappropriate tweets to a work-related Twitter account, and concluded that the dismissal was triggered by inappropriate and offensive postings that did not involve concerted activity

103 571 F.3d 53 (D.C. Cir. 2009).
104 Id. at 57.
105 Id.
protected under the NLRA.\textsuperscript{107} The same result was arrived at in another case involving complaints about a bar’s tip-sharing policy that the employee posted on Facebook in correspondence with his stepsister. The employee did not discuss the post with fellow employees and they did not respond to it, leading to the conclusion that there was no protected concerted activity.\textsuperscript{108} Subsequently, the NLRB may have found its test case in a May 2011 complaint alleging a New York nonprofit violated the Act when it fired five employees for posting critical comments about working conditions on a Facebook page.\textsuperscript{109} According to Philip Gordon, “There can be no question that the [NLRB] appears to want to take the law in a direction that will open social media to virtually unfettered use by employees to communicate about work conditions, defined very broadly."\textsuperscript{110}

A related issue has arisen with regard to employees terminated for breach of social media and related policies who subsequently seek unemployment compensation. Chapman v. Unemployment Compensation Bd. of Review involved a registered nurse who used her cell phone to make a social media post critical of a co-employee at the same time as she was distributing medications to patients. She was discharged for breach of her employer’s cell phone policy. The court upheld a finding that she was ineligible for unemployment compensation because her discharge was for “willful misconduct;” there was sufficient evidence that she knew of the policy, that the policy was reasonable, and that the policy was breached.\textsuperscript{111} The court did not address the question whether her Facebook account had been searched illegally on procedural grounds.

2. Privacy Law

The existence of the HIPAA Privacy and Security rules provides context for the increasingly risk averse approach by medical schools and healthcare employers to social media. However, their substantive provisions have little salience with regard to the relationship between, say, a hospital and its employees. Those relationships are generally untouched by HIPAA. However, other privacy regimes may be applicable.

Take, for example, Johnson v. K-Mart Corp.,\textsuperscript{112} where private detectives posed as employees at one of the defendant’s distribution center that had experienced theft, vandalism, sabotage, and drug use. Reports submitted by the investigators included employee family matters, sexual and romantic conduct, future employment

\textsuperscript{112} 723 N.E.2d 1192 (Ill. App. Ct. 2000).
plans, complaints about the defendant, and even private matters such as personal health issues. When the investigation was exposed, some of the employees brought an action against the employer for Intrusion upon Seclusion, Publication of Private Facts, and Intentional Infliction of Emotional Distress. The Illinois appellate upheld the trial court’s summary judgment on the emotional distress count because of a failure to establish serious emotional distress. However, on the other two common law counts the court reversed the defense’s summary disposition. On the seclusion count, the court felt that the employees had a reasonable expectation of privacy when communicating with co-workers, particularly when such communications took place at social gatherings outside of the workplace. On the private facts count, the court believed that an issue of fact existed as to whether making such private facts public to the employer was highly offensive. Clearly there are lessons here for an employer who would snoop on the social media postings of an employee or employment applicant, at the very least when the employee has secured, say, his Facebook page with reasonable security and privacy settings.

As employees and applicants become more aware of the risks of exposing social media data and interactions and make better efforts to secure their spaces, employers have begun to request their social media passwords during the application process. In early 2011, such case involving an applicant for a Department of Corrections position led to the ACLU sending a strong letter to the employer, the Maryland DOC. In its letter the ACLU argued:

While employers may permissibly incorporate some limited review of public internet postings into their background investigation procedures, review of password-protected materials overrides the privacy protections users have erected and thus violates their reasonable expectations of privacy in these communications.

The ACLU constructed its primary legal arguments (including reasonable expectations of privacy) around the Stored Communications Act (SCA). The SCA prohibits unlawful access to stored electronic communications and permits a civil

---

113 See Busse v. Motorola, Inc., 813 N.E.2d 1013, 1017 (Ill. App. Ct. 2004). “The elements of the cause of action typically are stated as: (1) the defendant committed an unauthorized intrusion or prying into the plaintiffs seclusion; (2) the intrusion would be highly offensive or objectionable to a reasonable person; (3) the matter intruded on was private; and (4) the intrusion caused the plaintiff anguish and suffering.” Id.

114 See Constructing a Legal Framework, supra note 1, at 327-29.

115 Id. at 341.


cause of action.\textsuperscript{119} Notably, the SCA may contain more effective protections than the better-known Electronic Communications Privacy Act of 1986.\textsuperscript{120} Specifically, SCA applies to one who “intentionally accesses without authorization a facility through which an electronic communication service is provided.”\textsuperscript{121}

The first issue that arises in such a case is whether a social media space is capable of protection under the SCA, in contrast to, say, a publicly accessible web site or blog. Here the ACLU relied on \textit{Crispin v. Christian Audigier, Inc.}\textsuperscript{122} \textit{Crispin} was an IP case in which defendants subpoenaed communications on \textit{Facebook} and \textit{MySpace}. Plaintiff relied, inter alia, on the SCA to quash the subpoena. The court concluded that the SCA applied at least to the sites’ private messaging and to user areas with “restricted access” secured by privacy settings (notwithstanding the number of “friends” that could view the content).\textsuperscript{123}

Clearly the employer in the DOC case literally has “authorization” because it has received the account password from the prospective employee. However, the ACLU relied on \textit{Pietrylo v. Hillstone Restaurant Group} for the proposition that access via a password obtained through coercion or provided under pressure was not authorized.\textsuperscript{124}

After receiving the ACLU’s letter the DOC suspended its practice.\textsuperscript{125} In March 2011, legislation was introduced into the Maryland Senate that would prohibit an employer from requiring either employment applicants or employees from disclosing authentication information for any non-employer online account.\textsuperscript{126}

\textbf{IV. Provider Access to Patient Social Media Data}

\textbf{A. From Voyeurism to Obligation}

If the theme of the prior section was what doctors discover when they “Google” themselves, this part asks whether there are circumstances when physicians should “Google” their patients or examine their social media pages. Specifically, this section explores the implications of patient-related therapeutic information, maybe even life-saving data, being available online. Should the

\begin{flushleft}
123 Id. at 991.
124 No. 06-5754 (FSH) (D.N.J. 2009). The Pietrylo court had held a jury issue was presented on this issue. Using someone else’s password to access a social media site in violation of terms of use may also implicate some anti-hacking statutes. See infra text accompanying note 153.
\end{flushleft}
physician seek to access that information and, if that was recognized as possible, could such an opportunity morph into a legal obligation imposed on the physician?

Frequently a physician (particularly a psychiatrist or a pediatrician) who is interested in what the patient may have posted online will be in a position to request access to social media from the patient. The question is whether the physician is under a duty to make that request and then harvest this information about the patient. Distilled, the issue implicates both scope of duty and the standard of care. As to the latter,

[T]he law implies that a physician employed to treat a patient contracts with his patient that: (1) he possesses that reasonable degree of learning and skill which is ordinarily possessed by others of the profession; (2) he will use reasonable and ordinary care and diligence in the exercise of his skill and the application of his knowledge to accomplish the purpose for which he is employed; and (3) he will use his best judgment in the application of his skill in deciding upon the nature of the injury and the best mode of treatment.\textsuperscript{127}

\textit{Hall v. Hilbun}, the canonical malpractice case, defines the doctor’s professional services subject to due care as "the entire caring process, including but not limited to examination, history, testing, diagnosis, course of treatment, medication, surgery, follow-up, after-care and the like."\textsuperscript{128} The standard of due care includes being familiar with the state of current scientific and medical knowledge and technology.\textsuperscript{129} It is well established that the malpractice duty extends beyond mere physical presentation to broader circumstances, such as the dissemination of information in duty to warn\textsuperscript{130} and informed consent cases.\textsuperscript{131} Furthermore, doctors are expected to be cognizant of some of the social situations of their patients.\textsuperscript{132}

The standard of care clearly contemplates robust collection of information from and about the patient.\textsuperscript{133} For example, malpractice liability has been

\begin{footnotes}
\item[128] Hall v. Hilbun, 466 So. 2d 856, 871 (Miss.1985) (emphasis added).
\item[131] Truman v. Thomas, 611 P.2d 902 (Cal. 1980).
\end{footnotes}
predicated on a physician’s failure to take a history, the taking of an inadequate history, or failure to chart. Physicians who find themselves in the position of having inadequate information or knowledge may have duties to so disclose that state to the patient or to consult with colleagues.

Assume, however, that the patient does not give the physician access to their social media or that a hypothetical such as the following occurs.

As his patient lay unconscious in an emergency room from an overdose of sedatives, psychiatrist Damir Huremovic was faced with a moral dilemma: A friend of the patient had forwarded to Huremovic a suicidal e-mail from the patient that included a link to a Web site and blog he wrote. Should Huremovic go online and check it out, even without his patient’s consent?

Indeed, such an event may not be limited to the purely hypothetical. One neurosurgeon has related how in the summer of 2010 a 56-year-old woman presented at a Wisconsin hospital emergency room complaining of chest discomfort. There was evidence of prior strokes and fluid around her heart. The patient reported several hospital visits but then lapsed into a coma. There was no history, and family members had no useful information. However, the patient did have a Facebook page where she had posted her medications, symptoms, hospitalizations, and conditions. She also described how she had felt and other physical indications. From this information the medical team was able to deduce that “she’d been throwing blood clots to the brain,” perform successful brain surgery, and bring the patient out of the coma.

Assume, first, that the data is publicly available (because, for example, the patient has not set any privacy or security settings on a Facebook page). Then the question is, first and almost exclusively, a therapeutic one. If the physician proceeds to access the information (or, say, perform a Google search on the patient), will that dilute or otherwise impede the therapeutic relationship going forward? For example, one study raised the following hypothetical,

---

137 See, e.g., Manion v. Tweedy, 100 N.W.2d 124, 128 (Minn. 1959); Johnson v. Kokemoor, 199 Wis.2d 615 (1996).
How should a doctor react when he discovers that a patient is still smoking if this patient had assured the doctor that he has stopped? Should the doctor take advantage of this knowledge in order to provide additional patient information and counselling or should he not mention this fact in order to avoid being accused of spying on his patient?\textsuperscript{141}

Addressing the issue from an ethical perspective is difficult. Arguably, any such investigation by the physician violates patient dignity and autonomy and breaches the trust relationship.\textsuperscript{142} A more instrumental approach might be to permit such searches assuming that the purpose of the search is strictly related to treating the patient and that the patient has not, for example, prohibited such data collection by the physician. In 2009 the Ethics Committee of the American Psychiatric Association (APA) answered the question “Is it ethical to do a Google search on your patient’s name?” by making a similar point ("Googling a patient … should be done only in the interests of promoting the patient’s care and well-being and never to satisfy the curiosity or other needs of the psychiatrist") as follows:

The standard of practice for learning about a patient’s medical condition is through face-to-face interviews, and this information may be supplemented by collateral information, for example, medical records or family members. Refusal or inability by patients to provide important historical information is not uncommon; in this circumstance collateral data may assume an important role. “Googling” a patient in such a scenario may provide useful information. However, information obtained this way, such as on a MySpace Web site, may not be current or accurate, especially for clinical purposes. Similarly, newspaper articles may not be reliable. Information such as birth records and sexual-offender registration is more likely to be trustworthy. Whenever information is obtained through a Google search, it is important to corroborate it.\textsuperscript{143}

The APA also addressed the question of handling data discovered online noting, “[c]linicians who routinely act on information that cannot be verified as fact may be at risk of practicing incompetently. It is prudent to identify the source of information that is entered into a medical record.”\textsuperscript{144} It is likely that more social media policies will seek to address this issue. For example, the Indiana University Medical School Social Media Guidelines provide, “[p]rivate patient information

\begin{footnotes}
\item[142] Jun Yan, Psychiatrists Must Beware the Perils of Cyberspace, 44(14) PSYCHIATRIC NEWS 9, 9 (2009) (quoting Jacob Sperber, M.D.).
\item[143] Is it Ethical to 'Google' Patients?, 44(9) PSYCHIATRIC NEWS 11, 11 (2009), available at http://pn.psychiatryonline.org/content/44/9/11.1.full .
\item[144] Id.
\end{footnotes}
obtained on a social networking site should not be entered in the patient’s medical
record without the patient’s knowledge and consent.”

Neither federal nor state privacy regimes seem to address the issue. The
situation in Canada may be different. For example, Alberta’s Health Information Act
provides, “[a] custodian must collect individually identifying health information
directly from the individual who is the subject of the information . . . .” Although, the
same legislation provides exceptions such as “where collection from the individual
who is the subject of the information is not reasonably practicable.”

It is difficult to see any other legal issues arising unless, for example, the
doctor was working for an employer and somehow fell afoul of The Genetic
Information Nondiscrimination Act of 2008 (GINA) and its regulations. GINA
makes it illegal for employers to “request, require, or purchase genetic information
with respect to an employee or a family member of the employee.” The Equal
Employment Opportunity Commission’s November 2010 final rule makes clear that
conducting an Internet search likely to result in the discovery of such information is
included in that prohibition.

Assume in the alternative that the data lies behind a Facebook privacy setting.
The first problem is that unauthorized access (anything from using the patient’s
discovered login information without permission, successfully using a guessed
password, or outright hacking) likely will be a violation of the social media site’s
terms of use. For example, Facebook’s terms of use provide “[y]ou will not share
your password, . . ., let anyone else access your account, or do anything else that
might jeopardize the security of your account.”

At first sight this may not seem to be of particular concern to the third party
physician seeking access. However, a series of federal and state cases suggest
that at least some knowing violations of terms of use may be characterized as
criminal. A fortiori, the physician who enters a patient’s secured social media page is

---

146 Health Information Act, R.S.A. 2000, c. H-5 §22(1) (Can.) (emphasis added).
147 Id. at §22(2)(d).
§1635.8(a) (EEOC Nov. 9, 2010).
150 Regulations Under the Genetic Information Nondiscrimination Act of 2008, supra note 151. See
disclosure to the employer that employee allegedly omitted ADHD diagnosis on pre-employment
questionnaire potentially violated ADA confidentiality provision).
151 E.g., many passwords are still be found on post-it notes stuck to the subject’s computer.
152 Statement of Rights and Responsibilities, FACEBOOK 4. 8 (Apr. 26, 2011),
153 See, e.g., U.S. v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010) (Computer Fraud and Abuse Act
implicated when federal employee accessed employer’s database for non-business reasons); U.S. v.
Nosal,642 F.3d 781 (9th Cir. 2011) ("exceeds authorized access" triggered by employee violating
conviction under CFAA of defendant for violation of MySpace terms of service violates void-for-
154 E.g., Facebook, Inc. v. Power Ventures, Inc., No. C 08-5780 JF (RS) (N.D. Cal. May 11, 2009), No. C 08-
05780 JW (N.D. Cal. July 20, 2010); See generally CAL PENAL CODE § 502 (WEST 2010).
acting against the patient’s desire to define her “circle of intimacy” and as a result could have violated the Intrusion into Seclusion privacy tort. This would also be the case if the physician had been permitted access but then had exceeded the permission and accessed other data. Neither the HIPAA Privacy Code nor even more advanced state codes designed to reduce the HIPAA-free zone would apply to a physician accessing such information. However, once accessed by a healthcare provider, any recovered data likely would be subject to such protections going forward.

Assume, therefore, that there are situations where either unsecured health-related data resides on a patient’s social media pages that a physician can access without legal jeopardy or that the physician has the opportunity to request permission for access from the patient or from a surrogate. In such scenarios one psychiatrist has suggested, “[y]ou could almost make the argument that it’s negligent not to search online when there is public information available.”

Assuming such an affirmative duty is recognized, the narrow legal question likely to be addressed by the courts is whether to have an open-ended rule (such as one based on reasonable foresight in the circumstances) or a more narrowly defined one that will permit many such cases to be resolved in the physician’s favor on a motion for summary judgment. The Tarasoff line of cases is illustrative with courts moving away from open-ended tests for when a psychotherapist owes a duty to warn a potential victim to a more structured rule such as requiring “specific threats to a readily identifiable victim.” In this context, it would not be surprising to see the courts limiting physician liability for failure to access online information concerning a patient to cases where the physician has been informed that relevant information actually exists. To impose a duty to search for merely speculative information would constitute an unnecessary burden on the physician.

B. Risk Managing Access

A recent study published in *Pediatrics* recognized many positive aspects of social media but also highlighted the risks. The study concluded by encouraging pediatricians to engage their patients (and their parents) in the use of social media. Studies also suggest a correlation in teenagers and young adults between

---

155 *Constructing a Legal Framework*, supra note 1, at 329.
156 Social media sites are not covered entities under HIPAA and are not “organized for the primary purpose of maintaining medical information.” California Confidentiality of Medical Information Act, CAL. CIV. CODE § 56.06 (West 2008).
157 Scarton, *supra* note 139 (psychiatrist quoted by author).
158 Tarasoff v. Regents of the Univ. of Cal., 551 P.2d 334 (Cal. 1976).
very frequent uses of social media and narcissistic tendencies or other psychological disorders.\textsuperscript{161}

Given the nascent duty on providers discussed above, the key question is whether some private ordering tools can be brought to bear on the issue to effectively risk manage it. Overreaching contractual agreements granting \textit{pro forma} access to patient social media data no doubt will risk characterization as adhesive and unconscionable.\textsuperscript{162} However, there are other techniques for risk-managing such cases.

For pediatricians and psychiatrists, physicians most likely to want access to social media information, the first and most obvious approach is to discuss the issue in advance (even at the commencement of the physician-patient relationship) and request access to such social media data. Because of the potential criminal and civil consequences of a physician using the log-in information of another person discussed above, the physician should ask the patient to log on to show the social media information.\textsuperscript{163} It may be that these issues will become more commonly included in more general releases and consent forms that all physicians will present to their patients. Finally, in an extreme case where the physician is faced with an emergency situation and intends to access the social media without permission this should be charted and the reasons for the intrusive behavior and the narrow range of data sought should be recorded.

V. Regulating Friendships and Controlling Adverse Feedback

The persistent and arguably most difficult issue for physicians remains the extent to which they should engage with patients on social media. One of the reasons that physicians increasingly are counseled about boundary issues when they interact with patients online is that they might discuss and disagree about care issues in a public place. The second part of this section discusses a more extreme take on this dynamic and questions the extent to which providers can curtail social media commentary about their professional performance with what I term “social gag orders.”

A. Revisiting the “Boundary” Issue

There is ambivalence among physicians regarding social media that is born out by the data. While the majority of doctors, residents, and medical students view

\textsuperscript{161} See \textit{e.g.}, \textit{Social Networking's Good and Bad Impacts On Kids}, \textit{ScienceDaily}, Aug. 7, 2011, 

\textsuperscript{162} See \textit{e.g.}, Obstetrics & Gynecologists v. Pepper, 101 Nev. 105, 693 P.2d 1259 (1985); Broemer v. Abortion Services of Phoenix, Ltd., 840 P.2d 1013 (Ariz. 1992) (contractual requirement upon admission that patient arbitrate malpractice claim and waive right to jury trial was unenforceable as falling beyond patient's reasonable expectations). \textit{Cf.} Cleveland v. Mann, 942 So.2d 108 (Miss. 2006).

\textsuperscript{163} Cal. Penal Code § 502.
social media interactions with patients as ethically unacceptable, more than one-third were neutral or thought such interactions were acceptable. Of course, the underlying ethical position about boundaries transcends social media considerations. As stated by Nadelson and Notman,

An essential element of the physician’s role is the idea that what is best for the patient must be the physician’s first priority. Physicians must set aside their own needs in the service of addressing their patient’s needs. Relationships, such as business involvements, that coexist simultaneously with the doctor–patient relationship have the potential to undermine the physician’s ability to focus primarily on the patients’ well being, and can affect the physician’s judgment.

The social media version of this issue is now attracting detailed treatment from ethical frameworks and in the academic literature. The primary caveat in the new AMA guidelines is that physicians interacting with patients on social media platforms “must maintain appropriate boundaries of the patient-physician relationship in accordance with professional ethical guidelines just, as they would in any other context.” Some commentators argue that online friendships with patients “may open the door to interactions ... that are extraneous to the patient–doctor relationship, do not prioritise the therapeutic interests of the patient and lead to potentially problematic physician self-disclosure.” And, of course, in some specialties such as psychotherapy where the psychiatrist seeks to avoid self-disclosure in order to promote transference, exposing the physician’s social media presence to the patient could be strongly counter-therapeutic.

Given the necessity of maintaining boundaries the most frequent risk management recommendation is to use different sites to host the physician’s professional and personal profiles. For example, LinkedIn, unlike some direct Facebook competitors such as MySpace, has carved out a niche as a site for professional interactions rather than the more social or (dangerously) mixed uses of Facebook. Its espoused value proposition is:

Stay informed about your contacts and industry

164 Bosslet, supra note 31, at 5.
Find the people & knowledge you need to achieve your goals
Control your professional identity online

The specific AMA guidance is that “[t]o maintain appropriate professional boundaries physicians should consider separating personal and professional content online.” 172 Similar advice is appearing in medical articles on professionalism.173 The AMA guidelines acknowledge that participation in social media “can support physicians’ personal expression, enable individual physicians to have a professional presence online, [and] foster collegiality and camaraderie within the profession.”174

Seeking to fulfill some of this promise in a less risky environment several physician-only professional networking sites have been launched. For example, Sermo describes itself as “the largest online physician community in the US … [where physicians] collaborate on difficult cases and exchange observations about drugs, devices and clinical issues. And find potentially life-saving insights that have yet to be announced by conventional media sources.”175 Ozmosis176 and Within3177 share a different business model that includes creating “walled garden” search and collaboration services for hospital systems. Finally, Medpedia is a long-term project backed by leading healthcare providers around the world “to evolve a new model for sharing and advancing knowledge about health, medicine and the body among medical professionals and the general public.”178

Obviously, there will be outlying or exceptional cases that identify advantages in accepting blurred professional and private relationships notwithstanding generalized risks. For example, in the UK a surgeon read some posts by a Facebook friend and immediately contacted him, suspecting (correctly) appendicitis.179 Overall, however, intervening in the health care of non-patients is fraught with medico-legal peril, and the optimal method for avoiding the inadvertent creation of a physician-patient relationship is to strictly maintain a personal-professional boundary.180 The maintenance of boundaries and avoidance of legal risk explains why many healthcare entities’ social media plans frequently

171 LINKEDIN, supra note 169.
180 See generally the arguments made at Constructing a Legal Framework, supra note 1, at 330-33.
rotate around providing community forums for engagement rather than the entity itself answering specific questions.¹⁸¹

Whether or not a separate site is utilized for the physician’s professional profile, there is no doubt that the physician should use strong privacy and security settings on any “personal” site. Users continue to suffer privacy and security costs as social media platforms modify their settings.¹⁸² Nevertheless, they remain the lowest friction risk management technique for social media users. There is some evidence that the publicity given to Facebook’s privacy and security issues and the site’s improvement of their controls has led to an increase in their use even among groups (such as students) that previously had eschewed such protections.¹⁸³ Using high privacy and security settings is also the best argument that that a user has some expectation of privacy.¹⁸⁴

On their personal sites physicians should limit identifying information that relates to their professional activities and affiliations. A family name or initials rather than the full name used professionally might be appropriate, and care should be taken in choosing a profile graphic rather than an identifying picture. However, Arash Mostaghimi & Bradley Crotty recognize:

>[A]bsolute separation of professional and personal identities is nearly impossible. Although using a pseudonym may reduce the chances of incidental disclosure, patients who are motivated to identify information about their physicians probably will succeed. Physicians who are aware of their digital identities will be best able to address any questions that a search may reveal.¹⁸⁵

The AMA policy also is realistic, noting, “privacy settings are not absolute and that once on the Internet, content is likely there permanently” and recommending that “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.”¹⁸⁶

According to a survey of French residents and fellows, relatively few patients currently are looking to “friend” their doctors, with only 8% having received such a request.¹⁸⁷ A survey of over 3000 physicians and medical students published in 2011 painted a more troubling picture with considerable numbers of social media—using family practitioners (42%), obstetricians (38%), pediatricians (27%), and all

¹⁸⁴ Constructing a Legal Framework, supra note 1, at 294-96.
¹⁸⁵ Mostaghimi, supra note 173, at 561-62.
¹⁸⁷ Moubarak, supra note 141, at 102.
physicians (34%) having received a friend request from a patient or a patient’s family member. Of the physicians who had received such requests 57% had a blanket policy against accepting while 43% accepted on a case-by-case basis. The dynamic is heavily asymmetrical; only a very few physicians had initiated a friend request to a patient.\textsuperscript{188}

The Mount Sinai Social Media Guidelines discussed above contains this hypothetical:

A patient attempts to “friend” an attending physician on Facebook. This is almost always inappropriate, unless the doctor-patient relationship has ended. Even after the doctor-patient relationship has ended, it would be inappropriate to discuss health-related information.\textsuperscript{189}

The British Medical Association (BMA) has also endorsed a policy that is more rigorous than the AMA’s. For the BMA the increased likelihood of “inappropriate boundary transgressions” online and the ethical issues that might arise if “doctors become party to information about their patients that is not disclosed as part of a clinical consultation”\textsuperscript{190} require a more absolutist approach. Thus, the BMA’s recommendation is that "doctors and medical students who receive friend requests from current or former patients should politely refuse and explain to the patient the reasons why it would be inappropriate for them to accept the request."\textsuperscript{191} This is similar to the position taken by the Australian and New Zealand medical associations that recommend against social media relationships with current or former patients.\textsuperscript{192}

Of course many of the above policies, suggestions, or precautions may be subsumed under a single, general question that a physician should ask before engaging with a patient on social media: what is my motivation for doing this? The ethical underpinning of the patient-physician relationship is that it exists to serve a patient’s needs, and is “based on trust and gives rise to physicians’ ethical obligations to place patients’ welfare above their own self-interest.”\textsuperscript{193}

B. Provider Comparison Sites

\textsuperscript{188} Bosslet, supra note 31, at 4.
\textsuperscript{189} Mount Sinai Sch. Med., supra note 85, Addendum to Social Media Guideline (1).
\textsuperscript{191} Id.
\textsuperscript{192} Austl. Med. Ass’n, supra note 72, at 5.
There are numerous potential frames for this analysis, some of which are quite benign. For example, the New England prescriber information legislation that resulted in the Supreme Court’s speech-protecting opinion in *Sorrell v. IMS Health Inc.* was at root an attempt by physicians to control the distribution of information about their practices. Equally, the increasing dissemination of consumer-facing quality information is viewed as key to most cost curve bending strategies including patient-centered care and consumer-directed healthcare.

To the chagrin of many providers, states entered the provider performance information space with web-accessible databases using similar data as is reported to the *National Practitioner Data Bank* (that is not publicly accessible). Organizations such as *HealthGrades* then aggregated that limited data. Some state non-profits such as the California HealthCare Foundation subsequently introduced ratings sites for hospitals, as did states such as Illinois, Maryland and Minnesota. Nursing homes aside, healthcare entities were more likely to have national comparison information posted about them by private ratings companies such as *HealthGrades.* More recently, however, Centers for Medicare & Medicaid Services (CMS) has extended the Nursing Home Compare model to hospitals. Indeed, recently CMS added Hospital Acquired Condition (HAC) Measures to its Hospital Compare web site. The rates, derived from billing data, reflect per

---

hospital incidences of common adverse events. The American Hospital Association (AHA) published a “Quality Advisory urging hospitals to review and check the accuracy of the HAC data,” further noting:

Hospitals strongly oppose inclusion of the HACs for reporting on Hospital Compare. CMS has never made specifications available for the calculation of the HAC rates, so fundamental assessments of the accuracy of capturing the incidence of these conditions have never been conducted. Hospitals continue to urge CMS not to publish these data.

HHS recently raised the ire of physicians again in mid-2011 with a proposal to use "secret shoppers" to "collect data from physician offices in order to accurately gauge availability of Primary Care Physicians (PCPs) accepting new patients, assess the timeliness of services from PCPs, and gain insight into the precise reasons that PCP availability is lacking." After the plan was detailed in the New York Times accompanied by a "government snooping . . . -Big Brother" quote from a doctor, politics prevailed and the plan was shelved.

While providers may be upset over such developments, there is little to be done in the face of the acknowledged benefits of effectiveness and outcomes research. Further, such data tends to be aggregated, generally valid, and as a result viewed as objective (if unpopular) data rather than opinion. In other words it’s unlikely to be taken personally.

However, this does not seem to be the case with public reviews of identified providers by private individuals. In cases where the provider of a service or product disagrees with a review provided by a private entity or individual, the most likely cause of action contemplated would be defamation. Nevertheless, defenses of

---

206 Foreign object retained after surgery, Air embolism, Blood incompatibility, Pressure ulcer stages III and IV, Falls and trauma, Vascular catheter-associated infection, Catheter-associated UTI, and Manifestations of poor glycemic control. [Likely will delete this footnote]


212 See, e.g., Colantonio v. Mercy Med. Ctr., 901 N.Y.S.2d 370 (N.Y. App. Div. 2010) (Where physician sued medical center and employees for defamation, the court held many statements to be nonactionable expressions of opinion, however found the physician raised a genuine issue of material fact as to whether the statements were made with malice).
opinion, truth, and lack of malice make defamation cases difficult to win. For example, a Minnesota neurologist recently sued the son of a deceased patient regarding online comments the latter had posted concerning the doctor’s interpersonal conduct. Granting the defendant’s motion for summary judgment the court noted, “because the medium has changed [to the Internet], however, does not make statements of this sort any more or less defamatory. Looking at the statements as a whole, the Court does not find defamatory meaning, but rather a sometimes emotional discussion of the issues.”

In some cases a product disparagement cause of action may be appropriate, and, if the person giving the opinion has a financial stake in the market involved, unfair competition may become relevant. Even well-established, objective opinion leaders are not immune from suit, as became apparent in the Suzuki-Consumers Union litigation a decade ago.

With regard to comments made on social media, the most important doctrine remains that introduced by the 1996 Communications Decency Act that “[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.” This provision has been interpreted to shield ISPs and web publishers who host the work of others from liability for, inter alia, defamation and unfair

---

213 See, e.g., Elite Funding Corp. v. Mid-Hudson Better Bus. Bureau, 629 N.Y.S.2d 611 (N.Y. App. Div. 1995) (Where mortgage brokerage company brought a defamation suit against the Better Business Bureau for rating the company “unsatisfactory” after failing to respond to several consumer complaints, the court held the bureau was entitled to summary judgment because the complaints were true and the bureau enjoyed both the qualified “common interest” privilege and constitutional “fair comment” privilege).

214 Christa Lawler, Duluth Doctor Appealing Judge’s Decision to Toss Out Defamation Suit, DULUTH NEWS TRIB. (June 25, 2011, 12:00 AM), http://www.duluthnewstribune.com/event/article/id/202704/.


216 See, e.g., Bose Corp. v. Consumers Union, 466 U.S. 485 (1984) (Where district court found for petitioner’s claim of product disparagement based on alleged defamatory statements made by respondent magazine, the Supreme Court affirmed the Court of Appeals reversal concluding actual malice had not been demonstrated).


220 Zeran v. AOL, Inc., 129 F.3d 327 (4th Cir. 1997)Where customer sued ISP for alleged unreasonable delay in removing defamatory messages posted by an anonymous third party, the Court held ISP was immunized under Section 230 of the Communications Decency Act); Ezra v. AOL, Inc., 206 F.3d 980 (10th Cir. 2000) (Where plaintiff sued ISP for defamation by allegedly providing access to inaccurate information about plaintiff, the Court held ISP was immune under Section 230 of the Communications Decency Act); See generally David R. Sheridan, Zeran v. AOL and the Effect of Section 230 of the Communications Decency Act Upon Liability for Defamation on the Internet, 61 ALB. L. REV. 147 (1997).
competition.221 For example, Barrett v. Rosenthal222 concerned defamation actions brought by two anti-quackery physicians. A publicist for alternative medicine allegedly sent defamatory emails about the doctors. The defendant reposted that email on an alternative medicine newsgroup site. Most of the allegations were viewed as opinion or covered by California’s SLAPP law.223 However, a remaining factual statement republished with notice of its defamatory character was successfully defended under the federal safe harbor provision (§ 230) leading to the following sweeping conclusion:

The prospect of blanket immunity for those who intentionally redistribute defamatory statements on the Internet has disturbing implications. Nevertheless, by its terms section 230 exempts Internet intermediaries from defamation liability for republication. The statutory immunity serves to protect online freedom of expression and to encourage self-regulation, as Congress intended. Section 230 has been interpreted literally. It does not permit Internet service providers or users to be sued as “distributors,” nor does it expose “active users” to liability.224

Although courts have made it increasingly practical for plaintiffs aggrieved by the online conduct or speech of others to cut through anonymity or pseudo-anonymity and bring actions for, for example, defamation,225 the Congressional decision to fully protect host sites and even re-posters has been consistently endorsed by the courts.

C. Social Media Gag Agreements

Opinion sites were one of the earliest forms of social media. For example, since 1999 Epinions226 has aggregated reviews of and TripAdvisor227, which rates travel-related services, was founded one year later. A new generation of opinion/rating sites that stress localization, such as Yelp,228 CitySearch,229 Judy’s

221 See, e.g., Stoner v. eBay, Inc., 2000 Extra LEXIS 156 (Cal. Super. Ct. Nov. 7, 2000)(Where plaintiff brought suit against company charging that use of eBay's website by third parties to sell "bootleg" music, the Court held eBay was immune from liability under Section 230 of the Communications Decency Act).
222 146 P.3d 510 (Cal. 2006).
223 CAL. CIV. PROC. CODE § 425.16 (Deering 2011); See generally Kathryn W. Tate, California’s Anti-SLAPP Legislation: A Summary of and Commentary on its Operation and Scope, 33 LOY. L.A. L. REV. 801 (2000).
224 See Barrett v. Rosenthal, 146 P.3d at 529.
Book,\textsuperscript{230} and Angie’s List\textsuperscript{231} are now moving aggressively into the online service review space. Increasingly these sites include sections for medical and dental specialties. In addition, some new physician-specific rating sites have emerged such as Avvo,\textsuperscript{232} DoctorScorecard,\textsuperscript{233} and RateMDs.\textsuperscript{234}

Even a cursory examination of the reviews posted on these types of social media sites should attract skepticism. There seems to be no way to ascertain whether the anonymous posters are even patients of the rated physician, suggesting the potential for gaming. These sites also lack any discernible scientific basis, at the very least suggesting a lack of accuracy, at least until a relatively large number of posts have been made (increasing the sample size). Not surprisingly, counter sites have sprung up,\textsuperscript{235} and the subjects of opinion sites have filed class action lawsuits alleging dubious, even extortive marketing practices.\textsuperscript{236}

Outraged physicians have filed several conventional defamation suits against patient reviewers who use these sites. For example, a California plastic surgeon has brought defamation, invasion of privacy, and interference with prospective economic advantage claims against anonymous posters at Yelp and DoctorScorecard.\textsuperscript{237} An earlier California case had ended badly for the aggrieved provider. A San Francisco patient had used the phrase “mouth torture” in a review of a dental visit she posted on Yelp. The dentist apparently responded on Yelp that the bad review was posted after the dentist reported her to a credit bureau. The dentist subsequently sued for defamation. However, a trial court applied the SLAPP law,\textsuperscript{238} dismissed the claim, and ordered the dentist to pay $43,000 in costs.\textsuperscript{239}

\begin{flushleft}
\textsuperscript{234} RateMDs.com, http://www.ratemds.com/social (last visited July 25, 2011).
\textsuperscript{238} CAL. CIV. PROC. CODE § 425.16 (Deering 2011); See generally Kathryn W. Tate, California’s Anti-SLAPP Legislation: A Summary of and Commentary on its Operation and Scope, 33 LOY. L.A. L. REV. 801 (2000); See also Gilbert v. Skykes, 53 Cal. Rptr. 3d 752 (2007) (Where a respondent surgeon brought a cross-complaint in a medical malpractice action alleging defamation and loss of business due to false and misleading statements appearing on appellant patient’s website, the Court found cross-compliant qualified as a SLAPP, requiring surgeon to show statements were both false and published with actual malice, which he failed to do).
\end{flushleft}
A relatively small number of doctors favors a quite different approach to such critical comments, attempting to preempt the posting of adverse reviews with what are described as “mutual agreements,” but in reality are better described as non-disclosure or social media gag agreements. These surfaced in 2007 and first attracted critical discussion in 2009.

Some of these agreements apparently are the work of Medical Justice, an organization that previously had concentrated on defensive strategies regarding medical malpractice actions, particularly allegedly frivolous claims. Medical Justice objects to the “gag order” label preferring “mutual agreements,” and describes them in the following terms:

The Agreements provide an actionable tool to address fictional or slanderous posts. In return, patients are granted additional privacy protections by the doctor above and beyond those mandated by law.

These agreements, that apparently are proffered before medical services are provided, are contracts that prospectively assign the copyright of any online review or commentary that the patient may post to the healthcare provider. Furthermore, the agreement not only prohibits the patient from disparaging the physician but also holds the patient responsible for preventing the same by their family members. The assignment appears to be for a period of five years.

Interestingly, Medical Justice has been countered by Doctored Reviews, a website created by two California law schools. Doctored Reviews refers to the “Mutual Agreements” as “anti-review contracts” and characterizes them as “poison

---


245 Id.


247 Santa Clara University High Tech Law Institute and The Samuelsion Law, Technology & Public Policy Clinic at the University of California Berkeley School of Law.
pills.” In a 2009 interview with NPR, the CEO of Medical Justice defended the “Mutual Agreements” as being necessary because HIPAA privacy protection prevented physicians from responding directly to patient posts and noted that the agreements “give the patient additional privacy protections above and beyond that mandated by law.” In 2011, the Electronic Freedom Foundation (EFF) weighed in with a critical blog post in which it noted that Yelp and Avvo refuse to honor these “agreements.” Indeed, RateMDs has added a “Wall of Shame” to its website that purportedly lists doctors who use social gag agreements.

Doctored Reviews and the EFF apparently became interested because an assignment of copyright could create an end run around the federal safe harbor. If the doctor involved owned the copyright in the forum post then he or she could demand a takedown of the adverse post. In such a case the web site would have little choice lest it should leave its Digital Millennium Copyright Act (DMCA) safe harbor. More generally, of course, the mere existence of such an agreement is likely to chill the patient’s speech.

A more serious claim recently leveled at Medical Justice was that it attempted to post positive ratings about its clients on RateMDs and Yelp. The posts were filtered out or taken down after it was discovered that the IP addresses used for the postings were registered to Medical Justice. Medical Justice argued that they had been testing a new service for clients and that the posts were real.

If proved, such “sockpuppetry” (posting under multiple anonymous names) or “astroturfing” (posting propaganda disguised as grassroots support) may have serious legal repercussions. In 2009 the Federal Trade Commission issued its Guides Concerning the Use of Endorsements and Testimonials in Advertising that requires, inter alia, disclosure of “material connections,” such that, for example, a “poster should clearly and conspicuously disclose her relationship to the manufacturer to members and readers of the message board.” The FTC clearly intends to apply this rule to social media. In 2010 a PR firm entered into a consent agreement with the FTC after its employees were caught posting positive reviews

---

250 Doctored Reviews, supra note 248.
252 Reitman, supra note 245.
254 See text accompanying supra note 219 et seq.
for a video game client on the iTunes store. In 2011, the FTC fined the seller of an instructional guitar program $250,000 when its affiliate marketers falsely posed as ordinary consumers and posted positive reviews.

Commentators have ridiculed the Medical Justice claims that additional privacy rights are being given by providers to patients and have suggested various contractual and consumer protection remedies against their enforcement. To that list perhaps should be added the substantive unconscionability principles that provided a foundation for Tunkl v. Regents of University of California, in which a release from liability in a hospital admission form was voided.

In this situation the releasing party does not really acquiesce voluntarily in the contractual shifting of the risk, nor can we be reasonably certain that he receives an adequate consideration for the transfer. Since the service is one which each member of the public, presently or potentially, may find essential to him, he faces, despite his economic inability to do so, the prospect of a compulsory assumption of the risk of another’s negligence. The public policy of this state has been, in substance, to posit the risk of negligence upon the actor; in instances in which this policy has been abandoned, it has generally been to allow or require that the risk shift to another party better or equally able to bear it, not to shift the risk to the weak bargainer.

The rating experience frequently is unpleasant, although one study of online reviews of 300 Boston-area physicians found that 88% of reviews were positive (with only 6% negative and the remainder neutral). Three other findings from that survey are notable. First, the number of reviews was quite small, suggesting considerable immaturity in the physician-rating space. Only 30% of the randomly generated physician sample had any reviews at all, and the overall number was low (66 reviews across 33 sites). Second, some of the reviews appeared to be written by the physicians themselves or their agents, suggesting that the FTC’s sockpuppetry rules may not be generally understood. Third, as noted by the researchers “many of

---

263 Tunkl, supra note 262 at 446-47. See also discussion of unconscionability, state consumer protection statutes, and other grounds for denying enforceability of such agreements in Tobias J. Butler, The Realities Of Relying On Doctor-Patient Non-Disclosure Agreements For Reputational Protection, 22 HEALTH LAWYER 23, 24ff (2010).
the patient’s complaints (e.g., “not enough parking,” “didn’t spend enough time,” “waited too long”) could be addressed without violating patient confidentiality.\textsuperscript{265}

Most powerfully, however, it is difficult to see physician gag orders surviving ethical scrutiny. The AMA code’s very first ethical principle requires “compassion and respect for human dignity and rights.”\textsuperscript{266} The fourth principle includes the requirement that the “physician shall respect the rights of patients.”\textsuperscript{267} Other AMA reports and opinions are supportive of such a position. For example, one ethics opinion on the physician-patient relationship notes, “[t]he relationship between patient and physician is based on trust and gives rise to physicians’ ethical obligations to place patients’ welfare above their own self-interest....”\textsuperscript{268} The AMA recognizes that,

> From the numerous internet-based websites that are available to patients to rate physicians, it is clear that patients are searching for outlets to provide feedback on their doctors. However, these sites often have an unscientific and biased approach, collect small samples and fail to validate that the patient actually had an encounter with a rated physician. Additionally, these sites rarely provide dispute resolution procedures and almost never provide useful feedback to physicians for quality improvement.\textsuperscript{269}

As a result, the AMA makes available to its members a commercial patient satisfaction survey tool, “RealTime,” and encourages its members to “proactively measure and respond to patient satisfaction data.”\textsuperscript{270} And, in April 2011, HealthGrades introduced a new physician portal through which physicians or practice administrators may verify and modify the information the service places in its physician profiles.\textsuperscript{271}

Railing against a minority of critical patients or, worse, expending energy on trying to gag all patients misses the point of our information society. Writing in the New England Journal of Medicine Dr. Shaili Jain said:

\textsuperscript{265} Id. at 943-44.
\textsuperscript{267} Id. at § IV.
\textsuperscript{270} Id.
What I find most striking, though, is the democratizing potential of the Internet. These sites, though virtually useless for meaningful evaluation of an individual physician, seem to hold promise in the aggregate weight and significance of the stories they contain. These stories are nuggets of qualitative data on patients’ attitudes regarding the quality of care and their needs and preferences in their relationships with their doctors. The Internet has allowed patients to have their unfiltered voices heard in a collective and powerful way. \[272\]

The prologue to the AMA’s *Professionalism in the Use of Social Media* policy notes how “[p]articipating in social networking … can support physicians’ personal expression” and “provide opportunity to widely disseminate public health messages and other health communication.”\[273\] The patients’ rights to personal expression are no less important.

**VI. Conclusion**

A social media savvy physician recently opined,

> I can split my physician colleagues into two camps. There’s one camp that would not dream of being on Facebook. The mere mention of the F-word sends shivers down their spines: It is too personal, too much potential risk, a frivolous time-suck. Then, there’s the other camp of colleagues who are on Facebook and either: a) have awkwardly dealt with a patient who added them as a friend or b) actively dread having a patient add them as a friend…. Having a so-called dual relationship with a patient — that is, a financial, social or professional relationship in addition to the therapeutic relationship — can lead to serious ethical issues and potentially impair professional judgment. We need professional boundaries to do our job well.\[274\]

In the last two or three years there has been a marked increase in the discussion of social media risks in professional journals, the welcome publication of ethics-based guidelines, and signs of increasing rigor in employer social media use policies. Social media has continued its relentless march into all aspects of our lives. As we expand our circles of friends and acquaintances, inevitably professionals will have to confront ever more challenging boundary issues. Equally, as we spend more hours on social media sites we will record and disclose more health-related information and post more opinions of our healthcare providers.


The first step in this ongoing project exploring the ethical and legal impact of social media on health care was to identify the riskiest activities that patients and physicians faced on social media. This, the next step in the inquiry, has been to examine the private ordering or risk management steps taken by those immediately and seriously affected by healthcare providers behaving badly or foolishly online. It has analyzed social media policies and other constructs and suggested some legal boundaries that will control their application. The next stage in the development of the domain likely will be public regulation and the attendant speech and other challenges that will no doubt follow. States are already experimenting with regulatory models dealing with, for example, social network privacy and boundary issues.

For physicians (at least some generations of whom have been slow to comprehend, let alone adopt information technologies) and healthcare entities, the expansive growth of social networking has disrupted relationships and long-terms practices. As a result, healthcare professionals and entities have been faced with a new bundle of indeterminate risks requiring management. Some traditional risk management models will continue to enter this space. For example, the Doctors Company, the large, California-based medical malpractice insurer has recently added complementary coverage for its insureds against regulatory and liability claims arising from the theft, loss, or accidental transmission of confidential patient data.

The private ordering phase detailed in this article has seen a few aggressive risk management models such as social media gag developed by physicians. However, most of the private ordering has been developed by professional bodies and healthcare institutions and has been imposed on physicians and other healthcare workers. This somewhat contractual phase in the evolution of social media risk management is reactive. Indeed, some professional organizations and providers may be guilty of overreaction and many of their policies likely will be refined in the years ahead. But, it will be only one of the techniques employed as healthcare providers and patients re-craft their relationships in this new and evolving context.

275 Constructing a Legal Framework, supra note 1, at 288.
277 Mo. SB No. 54, http://www.senate.mo.gov/11info/pdf-bill/tat/SB54.pdf, to be codified (regulating social media relationships between teachers and students and mandating school district policies for same).