2012

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

Nicolas P. Terry
Indiana University Robert H. McKinney School of Law, npterry@iupui.edu

Follow this and additional works at: https://digitalcommons.unl.edu/nlr

Recommended Citation

This Article is brought to you for free and open access by the Law College of at DigitalCommons@University of Nebraska - Lincoln. It has been accepted for inclusion in Nebraska Law Review by an authorized administrator of DigitalCommons@University of Nebraska - Lincoln.
Fear of Facebook: Private Ordering of Social Media Risks Incurred by Healthcare Providers

TABLE OF CONTENTS

I. Introduction .......................................... 703
II. Social Media and Healthcare Workers Misbehaving .... 705
   A. Social Media’s Exponential Growth .............. 705
   B. Healthcare Providers Misbehaving Online ....... 708
III. Ethical Codes and Provider Policies ................... 711
    A. Ethical Guidelines ............................. 712
    B. Employer Social Media Policies ............... 716
    C. Assessing Legal Limits on Policies ............ 720
       1. Labor Law ................................ 721
       2. Privacy Law ................................. 725
IV. Provider Access to Patient Social Media Data .......... 727
   A. From Voyeurism to Obligation .................... 727
   B. Risk Managing Access ............................ 733
V. Regulating Friendships and Controlling Adverse Feedback ............................................. 734
    A. Revisiting the “Boundary” Issue ................ 734
    B. Provider Comparison Sites ..................... 738
    C. Social Media Gag Agreements ................... 743
VI. Conclusion ............................................ 750

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.1 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.2

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. 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 analyzes 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.

---

2. Id. at 288.
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 and as many as 157.2 million U.S. visitors per month. Twitter, at only five-years-old, has 200 million users. Membership numbers aside, the traditional web metric of unique visitors is also telling, with Facebook receiving 590 million unique visits per month, Twitter 97 million, and the professional-oriented LinkedIn 41 million.

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. 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.” Social media platforms are growing by adding messaging, search, and video communication.

It has been predicted that “20 percent of business users will use social
networks as their primary means of business communications by 2014."14 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.15

The uses for social media are broadening, as are the demographics of active users.16 We have known for sometime that the majority (and a steadily increasing number) of Americans seek medical information on the Internet.17

Social media still lags behind “traditional” Internet destinations (such as established health web sites) for researching health information.18 According to a 2009 survey by Manhattan Research, 35% of U.S. adults use social media to acquire such information,19 while 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.20 Trust in these sites also is increasing, though it lags behind that expressed towards hospital web sites.21 Pew’s The Social Life of Health Information report for 2011 found that of adults who use social network sites (46% of all adults in the United States), only a relatively small number (11% of adults) followed their friends’ personal health experiences and only 7% used social media to acquire health information.22 Another 2011 poll suggested that 85% of sur-

14. Brad Reed, Gartner: Social Networking Slowly Taking Over E-mail, MACWORLD (Nov. 11, 2010), http://www.macworld.com/article/155663/2010/11/email_social_networking.html?src=rss_main.; see also Brian Barrett, Facebook Messages: Every Email, Text, and Chat in one Place, GIZMODO (Nov. 15, 2010), http://gizmodo.com/6690405/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.”).
15. Reed, supra note 14.
21. Id.
22. Fox, supra note 17, at 2, 6.
veyed 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 other 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 crowdsourced sites such as Patients Like Me, and use social media to create support and advocacy groups and to accelerate clinical trials.

Other narrowcast sites have a less organic background, such as Diabetic Connect and other sites built by Alliance Health Networks.

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 1,100 hospitals now have social networking sites, including over 1000 Facebook pages and nearly 800 Twitter feeds.

Exactly how many physicians use social media is difficult to determine. However, a survey published in 2011 concluded that personal


25. FOX, supra note 17, at 7.


30. DIABETIC CONNECT, supra note 26.


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.33 One aggregation site listed more than 1300 doctors actively using Twitter,34 while one research study analyzed Twitter feeds from 260 self-identified doctors with more than 500 followers each.35 Another study found that 44.5% of medical trainees had a Facebook account and that medical students were more frequent users than residents.36 Even the Centers for Disease Control and Prevention published a toolkit addressed to providers promoting the use of social media “as part of an integrated health communications program.”37

Use of social media by healthcare workers is also robust. A 2011 survey tracking social media use within healthcare institutions found that 84% of employees used sites such as Facebook for personal purposes and 68% for both personal and professional purposes.38

B. Healthcare Providers Misbehaving Online

Recently, the American College of Physician Executives published a study of offline disruptive conduct by physicians.39 More than 70% of physicians say that disruptive physician behavior occurs at least once a month at their organizations.40 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%).41 Unsurprisingly, similar behaviors occur online on social media platforms.

A 2007 cross-sectional analysis of medical students and residents at the University of Florida found 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 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.”

Sixty percent 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 warning (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

42. Thompson, supra note 36, at 955–56.
45. Id.
46. Katherine C. Chretien et al., Online Posting of Unprofessional Content by Medical Students, 302 JAMA 1309, 1309 (2009).
48. Video Insults Poor, supra note 47. For a more positive narrative about how an online video medical student project was used as a case study for developing responsible social media policies, see Jeanne M. Farnan et al., The YouTube Generation Implications for Medical Professionalism, 51 Persp. Biology & Med. 517, 517–24 (2008).
explicit content, 0.1% contained discriminatory content, and 0.7% involved a potential privacy violation.\textsuperscript{49}

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 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.\textsuperscript{50} In April 2010, four staff members were fired and three disciplined at St. Mary Medical Center in Long Beach, California.\textsuperscript{51} Allegedly, the staff members had taken pictures of a dying man who had been savagely attacked and then posted them on Facebook.\textsuperscript{52} In June 2010, Tri-City Medical Center in Oceanside, California terminated five nurses for discussing patients on Facebook.\textsuperscript{53}

Even apparently benign behavior involving social media is attracting adverse reactions. For example, in November 2008, nurses at a Fargo, North Dakota-based healthcare system used Facebook “to provide unauthorized shift change updates to their co-workers.”\textsuperscript{54} In 2011, Westerly Hospital in Rhode Island terminated the clinical privileges of a forty-eight-year-old emergency medicine physician and reported her to the state licensing board.\textsuperscript{55} The physician had written about some of her clinical experiences on Facebook albeit without using patient names or intending to reveal patient information.\textsuperscript{56} Subsequently, a third party was able to identify one of the patients because of the nature of an injury described.\textsuperscript{57} In a consent agreement with the licensing board, the physician accepted a reprimand for unprofessional conduct, paid $500 in administrative costs, and agreed

\textsuperscript{49} Chretien, \textit{supra} note 35, at 567 (limiting study to those with more than 500 followers).

\textsuperscript{50} Facebook Firings Show Privacy Concerns with Social Networking Sites, 31 HEALTHCARE RISK MGMT. 49, 49 (2009), available at http://www.khhra.org/fbfirings.pdf.


\textsuperscript{52} Id.

\textsuperscript{53} Id.; see also Roger Boyes, \textit{And This is Me on Facebook . . . Helping with Brain Surgery}, \textit{Times} (Aug. 18, 2008), http://www.timesonline.co.uk/tol/news/world/europe/article4560908.ece (reporting that Swedish nurse was suspended after posting photographs of brain and back surgeries on her Facebook page).


\textsuperscript{55} In the matter of Alexandra Thran, MD, St. R.I. DEP’r HEALTH (Apr. 14, 2011), http://www.health.ri.gov/discipline/MDAlexandraThran.pdf.

\textsuperscript{56} Id.

\textsuperscript{57} Id.
to attend a continuing medical education session dealing with patient confidentiality.58

III. ETHICAL CODES AND PROVIDER POLICIES

Divorce lawyers aside,59 employers were one of the first groups to leverage social media by including online data in their background checks.60 The majority of employers now include social media in their screening processes.61 In the healthcare environment, the seriousness of background checks has been further promoted by the growth of the negligent credentialing cause of action62 and the concomitant duties of disclosure placed on prior healthcare employers.63 While only the occasional physician recruit will leave behind social media evidence of an interest in witchcraft or “pictures of her topless and drink-
ing from beer bongs” for a recruiting firm to discover, zero tolerance for inappropriate social media behavior is becoming the norm.  

This section analyzes the recently published American Medical Association (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 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 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 invited “happy birthday” post by witness on judge’s Facebook page was “incidental contact” and not an ex parte communication.


71. New AMA Policy, supra note 70 (quoting AMA Board Member Mary Anne McCaffree, M.D.).

72. AMA Policy, supra note 65, ¶ (f).

73. Id.

74. Id.

75. 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.”).

76. Id. Subsection (b) states the following:

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.

Id.
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, "Physicians 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 products and services they review or discuss in online communities. This includes discus-

77. 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.”).
78. Id. ¶ (d) (“To maintain appropriate professional boundaries physicians should consider separating personal and professional content online.”).
79. Id. ¶ (a).
81. Compare Social Media Guidelines for Physicians, supra note 80, with AMA Policy, supra note 65.
82. Social Media Guidelines for Physicians, supra note 80, ¶ (d).
83. See AMA Policy, supra note 65, ¶ (e) (“When physicians see content posted by colleagues that appears unprofessional they have a responsibility to bring that content to the attention of the individual, so that he or she can remove it and/or take other appropriate actions.”); Social Media Guidelines for Physicians, supra note 80, ¶ (e) (same).
sions and reviews of products and services provided to the physician for free.”84

Additional useful caveats are to be found in the social media guide jointly prepared by the Australian and New Zealand medical associations.85 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.86

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.87 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.88

84. Id. ¶ (f). In 2010, the Ohio State Medical Association released Social Networking and the Medical Practice, OSMA LEGAL SERVICES GROUP (2010), http://www.osma.org/files/documents/tools-and-resources/running-a-practice/social-media-policy.pdf. The introduction contains information about risks (including legal risks posed by anti-discrimination and privacy laws), advice on navigating some of the employment issues in the healthcare environment, a “Best Practices” statement, and sample policies on prohibited and restricted uses at work applicable to physicians’ employees. Id.


86. Id. at 3.


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.89 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:

[The 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.90]

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, at least in part, is driven by 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,91 and Secretary Sibelius consolidated security

89. See generally Richard J. Cebula, Historical and Economic Perspectives on Lawyer Advertising and Lawyer Image, 15 Ga. Sr. U. L. Rev. 315 (1998) (discussing “the results of Gallup polls regarding the public’s ratings of the legal profession as having very high or high standards of honesty and ethics”).


and privacy enforcement in the Office of Civil Rights (OCR). 92 In its “statement” case against Cignet Health of Prince George’s County, Maryland OCR imposed a $4.3 million civil money penalty for HIPAA violations. 93 In July 2011, UCLA settled potential HIPAA violations for $865,500 stemming from unauthorized employee views of celebrities and other patients. 94 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.

Byrnes v. Johnson County Community College illustrates the necessity for such policies. 95 The plaintiff in Byrnes was a nursing student enrolled at the defendant community college. 96 With some other students and an instructor, she attended an obstetrics course at a local health system. 97 The instructor permitted the students to be photographed with an unidentified placenta. 98 After the students posted the photographs to Facebook, they were dismissed from the school and the plaintiff successfully applied for injunctive relief. 99 The court noted the following:

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 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. 100

Almost all U.S. medical schools now have guidelines or policies for their students relating to Internet use. 101 However, relatively few deal specifically with social media. 102 Two notable exceptions are the

96. Id. at *1.
97. Id.
98. Id.
99. Id.
100. Id. at *3.
102. Id.
social media policies posted by the Indiana University School of Medicine103 and Mount Sinai School of Medicine.104 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, personal and professional are blurred.”105 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.106

The Mount Sinai Guidelines include an addendum containing fictional case examples.107 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.108

Given the regulatory environment, patient privacy is likely 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,109 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. A 2011 survey noted one-third of institutions control access by employees, “typically due to security issues and concerns about employees’ productivity.”110

Social media policies are proliferating rapidly within all healthcare entities and generally will be designed to project the issues, norms, and values of individual institutions.111 Notwithstanding, some pro-


105. Indiana Guidelines, supra note 103, at 3.

106. Id. at 4.

107. Sinai Guideline, supra note 104 (Addendum to Social Media Guideline).

108. Id.


visions 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.112 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 commitments113 (some policies may even limit access to social media during work hours).114 Third, policies tend to highlight some specific legal restrictions.115 Thus, HIPAA compliance is likely to be mentioned accompanied by an express prohibition on posting identifiable information.116 Most policies explicitly ban abusive, profane, threatening, or offensive posts.117 Posting of copyright material also is likely to be expressly prohibited whereas the entity is likely to claim ownership of all posted material.118 Finally, most policies expressly note that violations will result in discipline or in termination of employment or clinical privileges.119

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


113. See, e.g., Social Media Guidelines for Employees, supra note 112; Sutter Health Policy, supra note 112, at 4.

114. See, e.g., Social Media Guidelines for Employees, supra note 112 (“Ensure that your blogging and social networking activity do not interfere with your work commitments.”); Sutter Health Policy, supra note 112, at 4 (“Individuals should limit participation in social media activities during work time unless required by their position . . . .”).

115. See, e.g., Social Media Guidelines for Employees, supra note 112 (discussing two patient privacy laws: HIPAA and the California Confidentiality and Medical Information Act); Sutter Health Policy, supra note 112, at 4 (discussing violations of patient privacy through HIPAA).

116. See, e.g., Social Media Guidelines for Employees, supra note 112; Sutter Health Policy, supra note 112, at 4.

117. See, e.g., Social Media Guidelines for Employees, supra note 112; Sutter Health Policy, supra note 112, at 3.

118. See, e.g., Social Media Guidelines for Employees, supra note 112; Sutter Health Policy, supra note 112, at 3.

119. See, e.g., Sutter Health Policy, supra note 112, at 6.
apply to content that is non-health care related or is otherwise unrelated to
Kaiser Permanente.  

The Ohio State Medical Association’s policy statement includes a
sample policy on “Restricted Use at Work.”  
The section dealing
with employee usage on personal property prohibits posts of proprie-
tary 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 is-
sues, 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.”  

As will be seen in the next section, this is an issue that has consid-
erable legal significance as healthcare entities seek to control activi-
ties 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, 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 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 har-
ass, intimidate, harm, or humiliate another.” His core argument
was this provision was facially and as-applied overbroad and

120. Kaiser Permanente Social Media Policy, K A I S E R P E R M A N E N T E, § 5.9 (Apr. 30,
pdf.
121. Social Networking and the Medical Practice, supra note 84 (Restricted Use at
Work).
122. Id.
123. Drew Glaser, Church Calls for Social Networking Accountability, C H A R I S M A
church-calls-for-social-networking-accountability.
124. Esfeller v. O’Keefe, 391 F. App’x 337 (5th Cir. 2010).
125. Id. at 338.
126. Id.
127. Id. at 340.
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 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 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. As one EEOC attorney remarked, “If you wouldn’t ask for it during an interview, don’t search for it online.”

128. Id. at 340–41.
129. Id. at 341.
130. Id.
131. No. 09-244-KSF, 2010 WL 4867630, slip op. at *1 (E.D. Ky. Nov. 23, 2010).
132. Id. at *4–5.
133. Id. at *9.
Both employees and potential employees may be protected under state non-work hours’ statutes. For example, the Colorado legislation provides, “It 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 . . . .”137 A narrower species of behavioral immunity applies in some states to non-work consumption of lawful products such as alcohol.138 Notwithstanding, these statutes tend to have safe harbors for employers in cases that impinge upon critical employer responsibilities.139

The National Labor Relations Act (NLRA)140 may have the most immediate impact and may cause employers to revise their social media policies or their enforcement. Section 7 provides: “Employees 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.”141 Section 8(a)(1) of the NLRA provides: “It 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].”142

In Guard Publishing Co. v. National Labor Relations Board,143 the National Labor Relations Board (NLRB) found 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.144 An administrative law judge found 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.145 NLRB broadly concurred with those findings except in holding that there was no evidence the employer allowed emails to solicit or support non-union organizations.146 The D.C. Circuit disagreed on this point on the basis that “neither the company’s written policy nor its express enforcement rationales relied on an or-

137. COLO. REV. STAT. § 24-34-402.5(1) (2010); see also N.Y. LABOR LAW § 201-d(2) (McKinney 2011) (prohibiting similar conduct in New York).
138. See, e.g., 820 ILL. COMP. STAT. ANN. 55/5 (West 2008).
139. See, e.g., COLO. REV. STAT. § 24-34-402.5(a)–(b).
141. Id. § 157.
142. Id. § 158(a)(1).
143. 571 F.3d 53 (D.C. Cir. 2009).
144. Id. at 54.
145. Id. at 57.
146. Id.
ganizational justification” and “the only employee e-mails that had ever led to discipline were the union-related e-mails at issue here.” 147

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. 148 In the Board’s first social media 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. 149 The board alleged the company had an overly broad social media policy regarding blogging, Internet posting, and communications between employees contrary to Section 8(a)(1). 150 However, the case settled in February 2011 when the company apparently agreed to rescind and revise its policy. 151

In an advice memorandum published on April 21, 2011, the NLRB commented on the dismissal of a newspaper reporter for posting unprofessional and inappropriate tweets to a work-related Twitter account, and concluded the dismissal was triggered by inappropriate and offensive postings that did not involve concerted activity protected under the NLRA. 152 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 stepsisiter. 153 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. 154

147. Id. at 60.
148. Some of the issues argued are peripheral. For example, in Flagstaff Medical Center, Inc., the NLRB decided that a hospital policy prohibiting employees from taking photographs was permissible. 357 N.L.R.B. No. 65, 2011 WL 4498271, at *6 (Aug. 26, 2011).
150. Id.
154. Id. at 3.
In August 2011 the NLRB’s general counsel released a report detailing the disposition of fourteen cases involving social media. 155 In four cases the NLRB’s Division of Advice held that employees’ social media activities were examples of protected concerted activity. 156 In five cases the Division held that provisions of employers’ social media policies were overly broad. 157 Subsequently, Hispanics United of Buffalo, Inc., one of the concerted activity cases discussed in the report, went forward for adjudication by the NLRB division of judges. 158 In that case, an employee at a New York nonprofit posted a co-worker’s complaints to Facebook that other employees were not doing enough to help the organization’s clients. 159 Other co-workers entered the social media conversation, defending their performance and complaining about working conditions. 160 The employer terminated five employees for bullying and harassing the original complainant. 161 The ALJ concluded: “Employees have a protected right to discuss matters affecting their employment amongst themselves. Explicit or implicit criticism by a co-worker of the manner in which they are performing their jobs is a subject about which employee discussion is protected by Section 7.” 162

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.”163

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 Board 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. 164 She

---

156. Id.
157. Id.
159. No. 3-CA-27872, 2011 WL 3894520.
160. Id.
161. Id.
162. Id.
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. 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., where private detectives posed as employees at one of the defendant’s distribution centers that had experienced theft, vandalism, sabotage, and drug use. Reports submitted by the investigators included employee family matters, sexual and romantic conduct, future employment 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 court 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 seclusion, the court felt the employees had a reasonable expectation of privacy when communicating with co-workers, particularly when

165. Id.
166. Id. at 610.
169. Id. at 1194.
170. Id.
171. Id. at 1193
172. Id. at 1198.
173. Id. at 1197.
174. 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 plaintiff’s 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.
such communications took place at social gatherings outside of the workplace. On the private facts count, the court believed 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 previously argued, “True to its context-based framework the law of boundaries should recognize private or secluded areas that have been established by users of social network sites.”

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 a case involving an applicant for a Department of Corrections (DOC) 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 cause of action. Notably, the SCA may contain more effective protections than the better-known Electronic Communications Privacy Act of 1986. Specifically, SCA applies to one who “intentionally accesses without author-

---

175. Johnson, 723 N.E.2d at 1196.
176. Id. at 1197.
177. See Terry, supra note 1, at 327–29.
178. See id.
180. Id.
181. Id.
184. Id. § 2707.
zation a facility through which an electronic communication service is provided." 187

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 Crispin v. Christian Audigier, Inc. 188 Crispin was an IP case in which defendants subpoenaed communications on Facebook and MySpace. 189 Plaintiff relied, inter alia, on the SCA to quash the subpoena. 190 The court concluded 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. 191

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 Pietrylo v. Hillstone Restaurant Group 192 for the proposition that access via a password obtained through coercion or provided under pressure was not authorized. 193

After receiving the ACLU’s letter the DOC suspended its practice. 194 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. 195

IV. PROVIDER ACCESS TO PATIENT SOCIAL MEDIA DATA

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-

187. Id. § 2701(a)(1).
188. 717 F. Supp. 2d 965 (C.D. Cal. 2010).
189. Id. at 968–69.
190. Id. at 969.
191. Id. at 991.
193. Letter from Deborah A. Jeon, supra note 179. The Pietrylo court had held that a jury issue was presented on this issue. Pietrylo, 2009 WL 3128420, at *3. 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 notes 229–34.
saving data, being available online. Should the 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:

The 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.196

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."197 The standard of due care includes being familiar with the state of current scientific and medical knowledge and technology.198 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 warn199 and informed consent cases.200 Furthermore, doctors are expected to be cognizant of some of the social situations of their patients.201

The standard of care clearly contemplates robust collection of information from and about the patient.202 For example, malpractice lia-

197. 466 So. 2d 856, 871 (Miss. 1985) (emphasis added).
bility has been 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 fifty-six year old woman presented herself 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

206. See, e.g., Manion v. Tweedy, 100 N.W.2d 124, 128 (Minn. 1959); Johnson v. Kokemoor, 545 N.W.2d 495, 505–06 (Wis. 1996).
210. Id.
211. Id.
212. Id.
213. Id.
214. Id.
throwing blood clots to the brain;” the team was then able to perform successful brain surgery, and bring the patient out of the coma.215

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:

[H]ow 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 [sic] or should he not mention this fact in order to avoid being accused of spying on his patient?216

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.217 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 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.218

The APA also addressed the question of handling data discovered online noting, “Clinicians who routinely act on information that cannot be verified as fact may be at risk of practicing incompetently.”219 The APA further stated, “It is prudent to identify the source of infor-

215. Id.
217. Jun Yan, Psychiatrists Must Beware the Perils of Cyberspace, 44 PSYCHIATRIC NEWS 9, 9 (2009), available at http://pn.psychiatryonline.org/content/44/14/9.1.full (quoting Jacob Sperber, M.D.).
219. Id.
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 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: “You will not share your

220. Id.
221. Indiana Guidelines, supra note 103, at subsection IV(d)(ii).
223. Id. § 22(1) (emphasis added).
224. Id. § 22(2)(d).
229. For example, many passwords are still found on post-it notes stuck to the subject’s computer.
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 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 should 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, 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 that “[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

---


233. *Terry, supra* note 1, at 329.

234. 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).

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 very frequent uses of social media and narcissistic tendencies or other psychological disorders.

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 *pro forma* access to patient social media data no doubt will risk characterization as adhesive and unconscionable. 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 conse-

---

239. Id.
241. See, e.g., Broumer v. Abortion Servs. of Phoenix, Ltd., 840 P.2d 1013 (Ariz. 1992) (finding that contractual requirement upon admission that patient arbitrate malpractice claim and waive right to jury trial was unenforceable as falling beyond patient’s reasonable expectations); Obstetrics & Gynecologists v. Pepper, 693 P.2d 1259 (Ne. 1985); cf. Cleveland v. Mann, 942 So. 2d 108 (Miss. 2006).
quences 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. 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 physicians increasingly are counseled about boundary issues when they interact with patients online is 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 borne out by the data. While the majority of doctors, residents, and medical students view 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 in-

242. See supra text accompanying notes 229–34.
244. Bosslet et al., supra note 33, at 1172.
teracting with patients on social media platforms “must maintain appropriate boundaries of the patient-physician relationship in accordance with professional ethical guidelines just, [sic] as they would in any other context.” Some commentators argue 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. Find the people [and] 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.” Similar advice is appearing in medical articles on professionalism. 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 . . . .”

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

246. AMA Policy, supra note 65, ¶ (c).
249. See, e.g., AMA Policy, supra note 65, ¶ (d).
252. LinkedIn, supra note 250.
253. AMA Policy, supra note 65, ¶ (d).
255. AMA Policy, supra note 65.
physician community in the US" where physicians are able to discuss
difficult cases, exchange observations about drugs, devices, clinical is-
ues, and “find potentially life-saving insights that have yet to be an-
nounced by conventional media sources.”256  Ozmosis257 and
Within3258 share a different business model that includes creating
“walled garden”259 search and collaboration services for hospital sys-
tems. 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.”260

Obviously, there will be outlying or exceptional cases that identify
advantages in accepting blurred professional and private relation-
ships notwithstanding generalized risks. For example, in the UK a
surgeon read some posts by a Facebook friend and immediately con-
tacted him, correctly suspecting appendicitis.261  Overall, however, in-
tervening in the health care of non-patients is fraught with medico-
legal peril, and the optimal method for avoiding the inadvertent cre-
tion of a physician-patient relationship is to strictly maintain a per-
sonal-professional boundary.262  The maintenance of boundaries and
avoidance of legal risk explains why many healthcare entities’ social
media plans frequently rotate around providing community forums for
engagement rather than the entity itself answering specific
questions.263

Whether or not a separate site is utilized for the physician’s profes-
sional profile, there is no doubt the physician should use strong pri-
vacy and security settings on any “personal” site. Users continue to
suffer privacy and security costs as social media platforms modify
their settings.264  Nevertheless, they remain a low friction risk man-
agement 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 es-

262. See generally Terry, supra note 1, at 330–33.
264. Kurt Opsahl, Facebook’s Eroding Privacy Policy: A Timeline, ELECTRONIC FRON-
chewed such protections.\textsuperscript{265} Using high privacy and security settings is also the best argument that a user has some expectation of privacy.\textsuperscript{266}

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 and Bradley Crotty recognize:

[\textit{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.\textsuperscript{267}]

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.”\textsuperscript{268}

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.\textsuperscript{269} 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 physicians (34\%) having received a friend request from a patient or a patient’s family member.\textsuperscript{270} Of the physicians who had received such requests 57\% had a blanket policy against accepting while 43\% accepted on a case-by-case basis.\textsuperscript{271} The dynamic is heavily asymmetrical; only a very few physicians had initiated a friend request to a patient.\textsuperscript{272}

The Mount Sinai Social Media Guidelines discussed above\textsuperscript{273} contains this hypothetical:

\begin{quote}
266. Terry, \textit{supra} note 1, at 294–96.
268. AMA Policy, \textit{supra} note 65, ¶ (b).
269. Moubarak et al., \textit{supra} note 216, at 102.
270. Bosslet et al., \textit{supra} note 33, at 1171.
271. \textit{Id.}
272. \textit{Id.}
\end{quote}
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.274

The British Medical Association (BMA) has also endorsed a policy that is more rigorous than the AMA’s.275 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” require a more absolutist approach.276 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.”277 This is similar to the position taken by the Australian and New Zealand medical associations, which recommend against social media relationships with current or former patients.278

Of course many of the above policies, suggestions, or precautions may be subsumed under a single, general question, which 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 . . . .”279

### B. Provider Comparison Sites

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.*,280 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

274. Id.


276. Id.

277. Id.


strategies including patient-centered care and consumer-directed healthcare.281

To the chagrin of many providers, a number of states entered the provider performance information space with web-accessible databases282 using similar data as is reported to the National Practitioner Data Bank283 (that is not publicly accessible284). Organizations such as HealthGrades then aggregated that limited data. Some state non-profit organizations such as the California HealthCare Foundation subsequently introduced ratings sites for hospitals,285 as did states such as Illinois,286 Maryland,287 and Minnesota.288 Healthcare entities were more likely to have national comparison information posted about them by private ratings companies such as HealthGrades.289 However, the Centers for Medicare & Medicaid Services

284. However, HRSA has made publicly available a deidentified version of the data for researchers and others. See Alina Selyukh, U.S. government draws fire for pulling doctor data, Reuters (Sept. 15, 2011), http://www.reuters.com/article/2011/09/16/us-usa-malpractice-database-idUSTRE78F03G20110916. This was withdrawn in September 2011 after a reporter was able to overlay other data and reidentify a physician’s record. Id. Correspondence that followed between the Association of Health Care Journalists and HRSA is also available. See Letter from Charles Ornstein et al., Pres., Ass’n of Health Care Journalists, to Mary K. Wakefield, Adm’r, Health Res. and Servs. Admin. (Sept. 15, 2011), available at http://www.healthjournalism.org/uploads/NPDB_HRSA.pdf; see also Duff Wilson, Senator Protests Agency Decision to Remove Doctor Data Online, N.Y. TIMES (October 7, 2011), http://prescriptions.blogs.nytimes.com/2011/10/07/senator-protests-agency-decision-to-remove-doctor-data-online (discussing Senator Charles E. Grassley’s criticism of the Obama administration’s decision to pull off the Web a database of doctor malpractice and disciplinary cases).
(CMS) has now extended its long-term care comparative data model (Nursing Home Compare) introduced in 2008 to hospitals. Recently, CMS added Hospital Acquired Condition (HAC) Measures to its Hospital Compare website. These HAC rates, derived from billing data, reflect per hospital incidences of common adverse events. In response, the American Hospital Association (AHA) published an advisory statement urging their members to check the accuracy of the HAC data published about them and 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.

The Department of Health and Human Services (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 is unlikely to be taken personally.296

However, private individuals who create adverse public reviews of identified providers do not seem to do so on a personal level. 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.297 Nevertheless, defenses of opinion, truth, and lack of malice make defamation cases difficult to win.298 For example, a Minnesota neurologist recently sued the son of a former patient regarding online comments the latter had posted concerning the doctor’s interpersonal conduct.299 Granting the defendant’s motion for summary judgment the Minnesota District Court noted, “Because the medium has changed [to the Internet], however, does not make statements of this sort any more or less defamatory.”300 The court continued, “Looking at the statements as a whole, the Court does not find defamatory meaning, but rather a sometimes emotional discussion of the issues.”301

In some cases a product disparagement cause of action may be appropriate,302 and, if the person giving the opinion has a financial stake in the market involved, unfair competition may become relev-

296. See also Robert A. Cherry & Gregory M. Caputo, Reporting Quality Data on Your Hospital Website: What? Why? How?, 37 PHYSICIAN EXECUTIVE 24 (2011) (“Physicians may be more supportive of a hospital’s efforts to publicly report quality metrics on its website if the data were considered accurate and reflective of the severity of illness of the patients cared for in their practices.”).

297. See, e.g., Colantonio v. Mercy Med. Ctr., 901 N.Y.S.2d 370, 374–75 (N.Y. App. Div. 2010) (holding statements to be “nonactionable expressions of opinion” where physician sued medical center and employees for defamation even though the physician raised a genuine issue of material fact as to whether the statements were made with malice).

298. See, e.g., Elite Funding Corp. v. Mid-Hudson Better Bus. Bureau, 629 N.Y.S.2d 611 (N.Y. App. Div. 1995) (holding the Better Business 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 where mortgage brokerage company brought a defamation suit against the bureau for rating the company “unsatisfactory” after failing to respond to several consumer complaints).


301. Id. at 12–13.

302. See, e.g., Bose Corp. v. Consumers Union, 466 U.S. 485, 514 (1984) (concluding actual malice had not been demonstrated and affirming the Court of Appeals reversal where district court found for petitioner’s claim of product disparagement based on alleged defamatory statements made by respondent magazine).

--

296. See also Robert A. Cherry & Gregory M. Caputo, Reporting Quality Data on Your Hospital Website: What? Why? How?, 37 PHYSICIAN EXECUTIVE 24 (2011) (“Physicians may be more supportive of a hospital’s efforts to publicly report quality metrics on its website if the data were considered accurate and reflective of the severity of illness of the patients cared for in their practices.”).

297. See, e.g., Colantonio v. Mercy Med. Ctr., 901 N.Y.S.2d 370, 374–75 (N.Y. App. Div. 2010) (holding statements to be “nonactionable expressions of opinion” where physician sued medical center and employees for defamation even though the physician raised a genuine issue of material fact as to whether the statements were made with malice).

298. See, e.g., Elite Funding Corp. v. Mid-Hudson Better Bus. Bureau, 629 N.Y.S.2d 611 (N.Y. App. Div. 1995) (holding the Better Business 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 where mortgage brokerage company brought a defamation suit against the bureau for rating the company “unsatisfactory” after failing to respond to several consumer complaints).


301. Id. at 12–13.

302. See, e.g., Bose Corp. v. Consumers Union, 466 U.S. 485, 514 (1984) (concluding actual malice had not been demonstrated and affirming the Court of Appeals reversal where district court found for petitioner’s claim of product disparagement based on alleged defamatory statements made by respondent magazine).
vant.\textsuperscript{303} Even well-established, objective opinion leaders are not immune from suit, as became apparent in the Suzuki-Consumers Union litigation a decade ago.\textsuperscript{304}

With regard to comments made on social media websites, the most important doctrine remains that introduced by the 1996 Communications Decency Act: “No 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.”\textsuperscript{305} This provision has been interpreted to shield ISPs and web publishers who host the work of others from liability for, inter alia, defamation\textsuperscript{306} and unfair competition.\textsuperscript{307} For example, \textit{Barrett v. Rosenthal}\textsuperscript{308} concerned defamation actions brought by two anti-quackery physicians. In \textit{Barrett}, a publicist for alternative medicine allegedly sent defamatory emails about the doctors.\textsuperscript{309} The defendant reposted that email on an alternative medicine newsgroup site.\textsuperscript{310} Most of the allegations were viewed as opinion or covered by California’s SLAPP law.\textsuperscript{311} However, a remaining factual statement republished with notice of its defamatory character was successfully defended under the federal safe harbor provision\textsuperscript{312} 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 pro-

\textsuperscript{303} See generally Cel-Tech Commc’ns, Inc. v. Los Angeles Cellular Tel. Co., 973 P.2d 527 (Cal. 1999).

\textsuperscript{304} Suzuki Motor Corp. v. Consumers Union, Inc., 330 F.3d 1110 (9th Cir. 2003). The case was eventually settled without any payment to Suzuki. Earle Eldridge, Consumers Union, Suzuki settle suit over tipping claim, USA TODAY (July 8, 2004), http://www.usatoday.com/money/autos/2004-07-08-suzuki-cu_x.htm.


\textsuperscript{306} Ezra v. AOL, Inc., 206 F.3d 980 (10th Cir. 2000) (holding a plaintiff who sued ISP for defamation by allegedly providing access to inaccurate information about plaintiff, was immune under section 230 of the Communications Decency Act); Zeran v. AOL, Inc., 129 F.3d 327 (4th Cir. 1997) (holding a customer, who sued ISP for alleged unreasonable delay in removing defamatory messages posted by an anonymous third party, was immunized 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).

\textsuperscript{307} See, e.g., Stoner v. eBay, Inc., No. 305666, 2000 Extra LEXIS 156 (Cal. Super. Ct. Nov. 7, 2000) (holding plaintiff who brought suit against company charging that use of eBay’s website by third parties to sell "bootleg" music, eBay was immune from liability under section 230 of the Communications Decency Act).

\textsuperscript{308} 146 P.3d 510 (Cal. 2006).

\textsuperscript{309} Id. at 513–14.

\textsuperscript{310} Id.

\textsuperscript{311} 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).

tect online freedom of expression and to encourage self-regulation, as Con-
gress 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.  

Although courts have made it increasingly practical for plaintiffs
aggrieved by the online conduct or speech of others to cut through ano-
nymity or pseudo-anonymity and bring actions such as defamation,
the congressional decision to fully protect host sites and even re-pos-
ters 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 Epinions which rates travel-related services, was founded one
year later. A new generation of opinion/rating sites that stress local-
ization, such as Yelp, CitySearch, Judy’s Book, and Angie’s List, 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, DoctorScorecard, and RateMDs.

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 sug-
gesting a lack of accuracy, at least until a relatively large number of
posts have been made (increasing the sample size). Not surprisingly,

313. See Barrett, 146 P.3d at 529.
315. See supra notes 297–313 and accompanying text.
services/58044_1790 (last visited July 25, 2011).
322. See Angie’s List, supra note 321; City Search Ch., supra note 319; Judy’s Book,
supra note 320; Yelp, supra note 318.
326. See generally David Streitfeld, In a Race to Out-Rave, 5-Star Web Reviews Go for
08/20/technology/finding-fake-reviews-online.html?_r=2&ref=technology.
counter sites have sprung up, and the subjects of opinion sites have filed class action lawsuits alleging dubious, even extortive marketing practices.

Outraged physicians have filed several conventional defamation suits against patient reviewers who use these sites. For example, a California plastic surgeon brought defamation, invasion of privacy, and interference with prospective economic advantage claims against anonymous posters at Yelp and DoctorScorecard. An earlier California case 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 and dismissed the claim, and ordered the dentist to pay $43,000 in costs.

A relatively small number of doctors favor 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

---


331. Id.

332. Id.

333. Id.

334. CAL. CIV. PROC. CODE § 425.16 (Deering 2011); see also Gilbert v. Sykes, 53 Cal. Rptr. 3d 752 (Cal. Ct. App. 2007) (finding respondent surgeon’s cross-compliant, in a medical malpractice action alleging defamation and loss of business due to false and misleading statements appearing on appellant patient’s website, qualified as a SLAPP, requiring surgeon to show statements were both false and published with actual malice, which he failed to do). See generally Tate, supra note 311.

335. Our View on Free Speech, supra note 330.

gag agreements.337 These surfaced in 2007 and first attracted critical discussion in 2009.338

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.339 Medical Justice now offers a rebranded service, eMerit, for “medical and dental reputation management.”340 In comments published in the New York Times, the CEO of Medical Justice described the function of these agreements as: “In the rare circumstance that a posting is false, fictional or fraudulent, the doctor now has the tool to get that post taken down.”341

These agreements, which 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.342 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.343 The assignment appears to be for a period of five years.344

Interestingly, Medical Justice has been countered by Doctored Reviews,345 a website created by two California law schools.346 Doctored Reviews refers to the mutual agreements as “anti-review contracts”

---

337. See generally Timothy B. Lee, Doctors and dentists tell patients, “all your review are belong to us”, Ars Technica (May 24, 2011), http://arstechnica.com/tech-policynews/2011/05/all-your-reviews-are-belong-to-us-medical-justice-vs-patient-free-speech.ars.
341. Dan Frosch, Venting Online, Consumers Can Find Themselves in Court, NY Times (May 31, 2010), http://www.nytimes.com/2010/06/01/us/01slapp.html.
346. Santa Clara University High Tech Law Institute and The Samuelson Law, Technology & Public Policy Clinic at the University of California Berkeley School of Law. Id.
and characterizes them as “poison 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 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. A doctor who owns the copyright in the forum post would demand a takedown of the adverse post and the website would have little choice because leaving the post up would endanger 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.

More serious claims recently leveled at Medical Justice involved attempts to post positive ratings about its clients on RateMDs and Yelp. The posts were filtered out or taken down after website administrators discovered that the IP addresses used for the postings were registered to Medical Justice. Medical Justice argued they had been testing a new service for clients and 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.

---

347. DocToRed Reviews, supra note 345.
349. Reitman, supra note 342.
351. See supra text accompanying note 306.
354. Id.
355. Id.
of Endorsements and Testimonials in Advertising that requires, inter alia, disclosure of “material connections.” For example, a “poster should clearly and conspicuously disclose her relationship to the manufacturer to members and readers of the message board.”359 The FTC clearly intends to apply this rule to social media. In 2010 a Public Relations firm entered into a consent agreement with the FTC after the firm caught its employees posting positive reviews for a video game client on the iTunes store.360 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.361

In November 2011, the Center for Democracy and Technology (CDT)362 filed a complaint with the Federal Trade Commission “to investigate the recent business practices of Medical Justice Corp.”363 CDT argues that Medical Justice contracts and posts are violative of section five of the FTC Act364 as constituting “unfair or deceptive practices.”365 In a statement posted on its website, Medical Justice claimed that its services were “honest, ethical, and legal” but that “we are going to use this situation as an opportunity to retire the written doctor/patient agreements we have had since 2007.”366

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.367 To that list perhaps should be added the substantive unconscionability principles that provided a founda-

359. Id.
tion for *Tunkl v. Regents of the University of California*, in which the California Supreme Court voided a release from liability in a hospital admission:

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 is frequently 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 the FTC’s sockpuppetry rules may not be generally understood. Third, as noted by the researchers “many of the patient’s complaints (e.g., ‘not enough parking,’ ‘didn’t spend enough time,’ ‘waited too long’) could be addressed without violating patient confidentiality.”

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.” The fourth principle includes the requirement that the “physician shall respect the rights of patients.” Other AMA reports and opinions are supportive of such a position. For example, one ethics opinion

368. 383 P.2d 441 (Cal. 1963).
369. Id. at 446–47; see also Butler, *supra* note 336, at 24 (2010) (discussing unconscionability, state consumer protection statutes, and other grounds for denying enforceability of such agreements).
371. Id.
372. Id.
373. Id. at 944.
374. Id. at 943–44.
376. Id. § IV.
on the physician-patient relationship notes, “The 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 . . . .”377 The AMA recognizes the following:

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.378

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.”379 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.380

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 the following:

What I find most striking . . . 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.381

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 commu-


379. Id.


The patients’ rights to personal expression are no less important.

VI. CONCLUSION

A social media savvy physician recently opined the following:

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.383

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.384 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 will likely 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 privacy385 and boundary issues.386

382. AMA Policy, supra note 65.
384. Terry, supra note 1, at 288.
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.387

The private ordering phase detailed in this Article has seen a few aggressive risk management models such as social media gag orders 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.
