Pre-Publication Draft

PLEASE DO NOT COPY, DISTRIBUTE OR CITE WITHOUT THE PERMISSION OF THE AUTHOR

PHYSICIANS AND SOCIAL MEDIA: UNTANGLING THE WEB

By Daniel F. Shay, Esq.

Alice G. Gosfield & Associates, PC
2309 Delancey Pl.
Philadelphia, PA 19103
215-735-2384
215-735-4778
agosfield@gosfield.com
www.gosfield.com

"Accepted for publication in the Health Law Handbook. 2014 Edition. Alice G. Gosfield, Editor, ©Thomson Reuters. A complete copy of the Health Law Handbook is available from West by calling 1-800-382-9252 or online at www.west.thomson

Physicians and Social Media: Untangling the Web
By Daniel F. Shay, Esq.

__.1 Introduction.

Social media is all the rage. Massive numbers of individuals are living their lives in electronic communities, through social media. In January, 2013, Facebook alone reported having 1.06 billion active users per month.[1] Social media acts as both a pipeline to communicate with other individuals, and a means through which virtual communities can be built. Physicians are beginning to recognize the importance of this phenomenon with respect to both marketing and quality improvement for the health care they provide to patients.

For example, social media websites such as Twitter have been shown to be useful in tracking epidemics, such as cholera outbreaks or the spread of the H1N1 virus.[2] A study from 2009 estimated that 61% of American adults look online for health information, and that adults between the ages of 18 to 49 are more likely than older adults to participate in social technologies relating to health.[3] Social media can also be used as "the platform for collaboration with [doctors'] patients by creating an improved healthcare delivery system that emphasizes patient accountability, cost containment, and quality of care."[4] Physicians are also recognizing the business value of social media, for patient education and marketing.[5] However, the benefits to physicians from social media come hand-in-hand with risks, including malpractice exposure and privacy concerns. Physicians engaged this way must also monitor and manage their online presence, including their online reputations on social media sites, responding to bad reviews from patients. In relation to all of these issues, physicians will need to develop employee policies for using

[1] Tam, Donna, "Facebook by the numbers: 1.06 billion monthly active users," CNET.com, January 30, 2013. http://news.cnet.com/8301-1023_3-57566550-93/facebook-by-the-numbers-1.06-billion-monthly-active-users/.

[2] Chunara, Rumi, Jason R. Andrews and John S. Brownstein, "Social and News Media Enable Estimation of Epidemiological Patterns early in the 2010 Haitian Cholera Outbreak," 86 Am. J. Trop. Med. Hyg. 39, 2012; Signorini, Alessio, Alberto Maria Segre, and Philip M. Polgreen, "The Use of Twitter to Track Levels of Disease Activity and Public Concern in the U.S. During the Influenza A H1N1 Pandemic," PLoS One, vol. 6, no. 5, May, 2011.

[3] Fox, Susannah & Sydney Jones, "The Social Life of Health Information," Pew Internet & American Life Project, p. 2, http://www.pewinternet.org/~/media/Files/Reports/2009/PIP_Health_2009.pdf.

[4] Soyer, Adam, D.O., "Social Media in Healthcare -- A Primer for Orthopaedic Surgeons," American Academy of Orthopaedic Surgeons and American Association of Orthopaedic Surgeons, February, 2012, p. 6.

[5] Hart, Brittany, "Patients Flock to Facebook for Health Care Needs," Dayton Business Journal, March 20, 2011, http://www.bizjournals.com/dayton/news/2011/03/18/patients-flock-to-facebook-for-health.html. Glatter, Robert, M.D., "Using Social Media to Increase Awareness of Medical Specialties Among Physicians," Forbes, November 10, 2013, http://www.forbes.com/sites/robertglatter/2013/11/10/using-social-media-to-increase-awareness-of-medical-specialties-among-physicians/.

social media, so as to minimize risks of improper HIPAA disclosures, malpractice, and damaging the practice's reputation.

This chapter provides an overview of forms of social media, a discussion of specific platforms and some of their functional differences. It then turns to potential problems that can arise for physician practices in such contexts, including privacy and confidentiality, malpractice, and defamation concerns. Last, this chapter offers practical suggestions and guidance for physicians engaged with social media.

__.2 Overview of Social Media.

The Merriam-Webster website defines "social media" as "Forms of electronic communication (as web sites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (as videos)."[6] How a social media platform functions will determine the way in which such communities are formed and such information is shared. For physicians and patients alike, questions of privacy or the capacity for a social media site to be rendered private are also a serious consideration. The answers to these questions depend largely on the tools, options, or settings available to users of a given social media site.

__.2.1 Social Media in General.

Generally speaking, social media websites share certain common features. These typically include the ability to post images and links to other content (including web pages, other social media pages and sites, images, and videos). In some cases, social media sites include the ability to "embed" content in the site itself, by placing content located on another website directly into the social media page, rather than requiring the user to view the content by "clicking through" a link on the social media site to visit a separate site. By way of example, a YouTube video "embedded" on a social media site would display the actual video player on the social media site. By contrast, a mere link to the video would require the user to click the link, which would then either take the user from the social media site to YouTube, or would open a separate browser window to the YouTube site.

Social media also provides users the ability to post text, although the amount of text a user can post depends on the site. Some sites permit users to post thousands of characters, while other sites limit users to only a handful of characters.[7] The "social" aspect of social media sites usually also allows users to connect to each other on the site. This may require consent by users, or may permit passive "following" where a user can simply view another's posted content without permission, or both.

---

[6] www.merriam-webster.com/dictionary/socialmedia.

[7] The term "characters" refers to all keystrokes, including letters, numbers, punctuation symbols, and even spaces.

Most social media sites also permit users to see the other users to whom a given user is connected. It is by this "six degrees of separation" feature that social media "communities" spread. For example, a person's best friend from high school may have connected with other friends who changed their names after marrying, enabling the first user to establish connections with them. By searching the second user's connections list, the first user can see those connections and connect to them directly. Many sites permit users to share a wide variety of demographic information, as well, such as their name, birthday, employer, marital status, which schools they attended, music, movies, and television shows they like, familial connections to other users on the site, even favorite restaurants, foods, and beverages. This wealth of information may be viewable by only specific people to whom the user grants permission, or by anyone casually browsing the site, without regard to any established connection to the user.

Because different sites permit different degrees of information to be shared, and allow information to be shared in different ways, and because different sites provide different levels of privacy controls to their users, it is important to understand the general contours of some of the more popular sites. Understanding how the different sites function on a practical level can help in the crafting of effective social media policies, as well as in maximizing the business benefits of social media use.

__.2.2 Facebook.

Facebook is, without question, one of the most popular social media sites in existence. According to an October, 2012 Forbes article, Facebook estimates that it has 1 billion users.[8] This figure suggests that roughly half the people in the world who have internet access use Facebook. Because it is one of the most popular sites with a multitude of features, Facebook provides a helpful "baseline" against which to compare other social media sites.

Facebook has most of the common features described in general. It permits users to post videos and images, as well as to embed certain types of links (such as news stories from websites, YouTube videos, etc.). Facebook permits users to connect with other users – and see to whom those users are connected. It also allows users to view other users' postings both on their own pages, and on other pages. In many ways, Facebook offers "one-stop shopping" in comparison with other sites. The design of the site permits users to do the bulk of things that other sites permit them to do, and more.

Facebook permits users to create two different types of accounts: "Profile" or "personal" accounts, and "Pages" or "business" accounts. Facebook states that Profiles must be used by named individuals only, and for non-commercial purposes. These Profiles usually have a separate login and password tied to an email account. By contrast, Pages are run by "administrators" who are, themselves, individual users with their own Profiles. A Page permits the administrator to track who has followed or "liked" the Page, to see how

[8] Their, David, "Facebook has a billion users and a revenue question," October 4, 2012, http://www.forbes.com/sites/davidthier/2012/10/04/facebook-has-a-billion-users-and-a-revenue-question/.

many people have posted to the Page and to review and edit (or delete) the content of those posts, as well as to promote the administrator's own posts. Personal Profiles lack many of these features.

Profiles cannot be duplicates of other existing Profiles. There cannot be two "John Smith" profiles about the same John Smith (although different John Smiths may have their own Profiles). Thus, there can be a profile for a John Smith who happens to be a family physician practicing in Portland, OR, a John Smith profile for a neuro-opthalmologist practicing in Chicago, IL, and a John Smith profile for a professional poker player. Profiles can also not be about fake or fictional individuals; thus someone who is not John Smith cannot create a John Smith Profile.[9] Facebook's policies on these matters help prevent both individuals from having their identities hijacked by others. When false Profiles are encountered, Facebook will disable them. If, on the other hand, a user has mistakenly established a Profile for a company, such as an office manager accidentally creating a "Cardiovascular Associates of Boise" profile, Facebook will convert the misclassified Profile into a Page.

Each user's Profile (or administrator's Page) permits the user to share content on what is known as their "timeline."[10] The "timeline" is an ongoing record, stretching back for as long as the user has been on the site, with all posts and events the user has chosen to share. For example, if a user changes their status from "single" to "married," that event will appear in the timeline. Likewise, a user's casual musing about a twinge in their elbow will also appear on the timeline, as well as the user's complaint about a long wait in the doctor's office to have their elbow checked. In contrast to these more public postings, users can also send private messages to each other. This feature functions essentially as Facebook's own internal email system -- with the key difference being that Facebook messages cannot be sent outside of Facebook.

Unlike Profiles, there can be multiple Pages about a business, both official and unofficial. For example, a popular band can have an "official" Facebook Page, but other users may start unofficial fan Pages about the band. Facebook also permits users to "check in" at physical locations, which means the user has indicated on their own timeline that they have visited a particular physical location. When this is done and no official page exists for the company which includes the location, Facebook may create a page simply for the "check in" location itself. It is this practice of "checking in" at a location that can give rise to unofficial Pages about a medical practice, particularly when the practice has multiple physical locations. For example, a cursory search of Facebook reveals multiple different LabCorp Pages for various LabCorp offices. It is likely that these Pages were created by user check-ins. Alternatively, other individuals may have created duplicate Pages for a given company. However, Facebook allows companies to assert ownership

[9] See, https://www.facebook.com/help/www/112146705538576. Pretending to be someone other than who you are is not permitted on Facebook Profiles.

[10] Readers who are only vaguely familiar with Facebook may also have heard of a user's "wall." The "timeline" used to be referred to as the user's "wall." This change in nomenclature was adopted by Facebook after a site redesign in 2012.

of a Page, and will make a designated company representative the Page administrator, if the company can prove that it is the rightful owner of the Page and the current user has no right to administer the Page.

As of this writing, users also have a "newsfeed" and a "sidebar," each of which will show the activities of other users with whom they're "friends."[11] The newsfeed on Facebook is essentially the home page for the site. It depicts posts that the user posts, as well as posts from the user's friends, and those Pages that the user has "liked."[12] Similarly, the sidebar will depict additional information, such as activities by friends on other Pages or Profiles to which the user is not connected.

Facebook also permits users to interact with content posted by others. In addition to commenting on other users' posts, Facebook permits users to interact in two ways. First, users can "share" posts from friends and Pages they follow. In essence, "sharing" functions similarly to forwarding an email. The user clicks "share" on a post from another user, and then can either post the other user's post on the first user's own timeline, or post it to a friend's timeline. For example, a user might "share" a friend's post about the recent birth of the friend's child, or an article about fibromyalgia treatment, or share a comment on their own timeline from another user.

As the above may suggest, vast swaths of information can be found – and are frequently shared – by users on Facebook. A user can post a picture to their timeline, which appears in their friends' newsfeeds, as well as on their status bar, which those friends can subsequently share with their friends, and so on. This necessarily has given rise to concerns about privacy. Facebook does offer certain privacy controls for users' Profiles and administrators' Pages, which can be critical for managing the privacy of information posted to these accounts. For example, users may create separate lists of friends, and group friends by category, such as "High School Friends," "Family," "Co-workers," etc. A user's own posts to their Profile, as well as demographic information, can be shared with the general public, with only friends and friends of friends, with only friends, or with only specific friend sub-groups. Thus, a user can post the results of a medical test they just had to "Family" only, rather than to all their friends. Users can also delete content posted on their Profile by other people, and can delete their own posts on their own Profiles and on other Profiles or Pages, or simply make them viewable only to the user themself. With respect to demographic information (such as birthdate, marital status, employer, etc.), users can restrict who can view each specific field, or can simply elect to leave the field blank.

__.2.3 Twitter.

[11] A "friend" on Facebook is another user to whom a user connects. The act of connecting to another user is frequently called "friending."

[12] "Liking" a Page is the colloquial term used to describe the act whereby users elect to receive updates and information from a given Page.

Twitter and Facebook each are social media giants. However, while they share some general similarities, like the ability to post messages and links, Twitter is very different. The key difference is that all posts on Twitter are limited to 140 characters (including spaces) per message. Thus, while the user can post photos and web links to longer articles or other web pages, all such content will be reformatted into a shorter link. These posts are known as "tweets."

Similar to Facebook's ability to "share" other users' posts, Twitter permits its users to "retweet" messages. As with Facebook, this feature essentially functions like forwarding an email. However, while Twitter permits a user to delete their own message, retweets of that message will not be deleted. Thus, the original message will be preserved. Similarly, tweets posted to a user's own timeline by other parties cannot be deleted, and a user's own tweets can only be deleted individually; there is no mechanism for mass deletions. These limitations of the Twitter system mean that, depending on how far the tweet itself was shared, there may be no way to fully delete a tweet. If, for example, a patient intake employee at a dermatology practice tweets that a celebrity just walked into their office, and that tweet is retweeted by a follower of the employee, the employee will not be able to completely erase the tweet itself; although the tweet on the employee's own account may be deleted, the retweet will still exist.

Twitter users connect to each other by "following" each other, which is similar to "liking" a Page on Facebook. It is fundamentally a passive connection, merely providing the user who is "following" to view posts from that account. However, if the Twitter user has opted to protect their tweets by activating Twitter's privacy features, they must approve each request to follow their account.

With respect to privacy controls, Twitter essentially has only two settings: "protected" and public. A protected account must approve each individual request to "follow" the account, and only those followers who have been approved are able to see content posted to the account, as well as limiting other aspects of communication on Twitter, discussed below.[13] As of this writing, there is no ability to create custom lists for tweets the way there is on Facebook. This is known as "protecting" an account.

Twitter also utilizes a mechanism known as tweeting "at" another account, whereby a user can add "@username" to a message, which will post the message to the so-named other user's account. Thus, a user could type "@NEJM, Great article on stents!" and the message would appear on the New England Journal of Medicine's Twitter account.[14] Of

[13] By comparison, Facebook offers more nuanced privacy controls for Profiles and Pages. Profiles generally have to approve who they "friend," while Pages usually do not do so (but can still control, through the administrator tools, who can post on their timeline). On Twitter, a protected account -- one that has activated Twitter's privacy controls -- must approve each individual user who asks to follow the account. As of this writing, there is no ability for Twitter users to create custom lists, as there is on Facebook. Even on protected accounts, all approved followers will see all of the user's tweets.

[14] And yes, the New England Journal of Medicine does have a Twitter account.

note is the fact that a protected account will only see tweets directed "at" it from approved followers, and only those approved followers will see tweets from the protected account when directed "at" the approved follower.

Twitter also pioneered the use of "hashtags." A hashtag itself is simply a phrase with a "#" symbol at the beginning, such as "#HealthReform." At their core, hashtags are an indexing tool, whereby a post may be labeled with a given hashtag, so that it will appear in collections of posts also containing that hashtag. Thus, all tweets with "#HealthReform" (or any other hashtag) would appear in an index -- searchable on Twitter, as well as on search engines like Google.[15] The use of hashtags also allows a user's posts to potentially become more visible, by virtue of having been part of a popular discussion. This can be an effective tool in promoting one's comments.

The nature of Twitter, and particularly its interconnectedness and brevity, allow it to be used as a platform to rapidly disseminate information. Because individuals can follow almost anyone (if their profile is not protected), and because even people who are not themselves Twitter users can see public content, information -- good, bad, accurate, or inaccurate -- can spread incredibly quickly. The use of the hashtag and retweet functions only serve to speed the process.

__.2.4 Other Social Media Sites.

While Facebook and Twitter are generally regarded as the two juggernauts of social media, other outlets also exist. These include Google+ (or G+), Pinterest, Instagram, and LinkedIn.[16]

Google+ was launched as a competitor to Facebook in 2011. However, despite an initial flood of curious users, G+ failed to attain the critical mass necessary to overtake Facebook in terms of popularity. However, in spite of internet memes such as "Nobody uses Google+," the site is still being used, if not as much as Facebook or Twitter.

Functionally, Google+ is similar to Facebook, with user pages containing demographic information, and allowing the posting of text, images, videos, etc. Google+ was actually the first of the major social media networks to use the concept of customizable lists of individuals to whom a user was connected. Google+ termed this feature "circles." Users can drag and drop the profiles of individuals with whom they are connected, to create custom lists, and then tag posts as being viewable only by those lists. The feature was

[15] Facebook, too, uses hashtags, but this is a relatively recent development, having only become part of Facebook in 2013. In addition, due to Facebook's privacy settings, users can only view posts with hashtags that they would otherwise be able to see. Thus, a user might be able to see a post set to be viewable to the general public with "#HealthReform" from the Centers for Medicare and Medicaid Services (CMS), but would not see a post by a user with whom they are not friends complaining about how complex health reform seems to be.

[16] There are, certainly, other networks that still exist, including the once-vaunted MySpace. However, these networks are not as popular, and therefore are beyond the scope of this chapter.

popular and useful enough that Facebook ultimately developed its own similar feature of customizable friend lists.

Pinterest, on the other hand, represents a far less interactive social media site. Instead, it functions more like an online scrapbook, or a collection of website bookmarks. A user may find a particular website or image online, and "pin" it to their account or "board" Users can connect to each other and "re-pin" what they find on other users' boards. With respect to physicians, Pinterest will likely only be relevant in a few ways. First, it demonstrates another medium by which information can be rapidly disseminated among people. A Pinterest user could, for example, pin an article about the nutritional value of certain foods, written by a physician at a local practice, which is then re-pinned by other individuals who might decide to call the practice for an appointment. In this sense, Pinterest is simply another avenue by which marketing may occur.

LinkedIn represents another platform for social media, chiefly in a networking context. LinkedIn profiles usually include resume information, a picture or two, and some message board functions. With respect to physician-patient relationships, it is not much more useful than an online Yellow Pages. Unless a patient has their own LinkedIn account, they are unlikely to see much more than basic demographic information about the physician. However, maintaining a LinkedIn profile can be helpful for physician-to-physician contacts, and can still be useful in maintaining the physician's own online presence and ensuring that information about oneself is correct.

Instagram lies within the realm of less interactive, less private social media sites. The site itself is a photo-sharing website (and smartphone application) that allows users to take pictures with a smartphone or other device and upload them to their own account. Users can post captions and alter pictures slightly, and add a caption to the photo itself.[17] In addition, users can comment on each others' photos and can connect to each other without requiring approval. As a result, Instagram offers far less control over who can see a user's content. Users can delete pictures that they post, but cannot limit who can view them, offering even less privacy options than Twitter. Instagram can also automatically connect to sites such as Facebook and Twitter (as well as others). Thus a user can post a picture on Instagram, and have it instantly populate to Facebook, Twitter, and the other sites to which Instagram can connect. Physicians are far less likely to use Instagram themselves for marketing and promotional purposes, but they may use Instagram as a window through which to peek into patients' lives. However, they should also understand that the window is a two-way window and that if they peer into a patient's life, the patient can peer back into theirs. Similarly, understanding Instagram can help physicians develop effective office policies for managing office staff to prevent (or at least control the scope of) improper disclosures of patient information.

[17] Users can add what are known as "filters," which automatically alter the color balance, sharpness, etc. of a photograph, can add borders, and can slightly retouch photos. The application does not allow them to drastically alter photos, such as cutting and pasting additional images into the photo, although users can use other applications to do so, and then upload a photo on Instagram.

__.2.5 Reputation and Review Websites.

Public review-based websites, such as Yelp and Google Pages, present an additional hurdle for physicians and physician practices' management of their online presences. These websites serve as outlets for the public to rate and comment on the physician practice. Much of what they discuss is oriented around the patient's perception of their own experiences. Angie Hicks, founder of the review site Angie's List, has commented that physicians have challenged her review site's validity, claiming that patients are not smart enough to effectively review the physician, while the American Medical Association has cautioned that anonymous reviews of physicians online should be "taken with a grain of salt."[18] However, while physicians may find these review sites unfair (given the potential belief in the patient's inability to necessarily recognize the quality of the *care* they receive as distinct from the quality of the *experience* at the practice), they are now a fact of life.

In general, the review websites are interactive, permitting the patient (and sometimes individuals who are not patients) to post comments and reviews of the practice, without oversight prior to posting. There is often no way for other users of the site to know whether the individual posting the review is actually a patient. These sites usually offer a mechanism by which the business can challenge a user's comments. Some sites also permit users (including patients) to connect to each other and send messages directly to each other.

For example, the review website Yelp permits users to add each other as friends, track their friends' reviews, and send messages to other users -- even ones they have not added as friends. Users will see that their friend has added a new review or visited a new location. Even when there is no existing entry for a given business, users of the website are invited to create a new entry for the business, which will allow other users to then comment on the business after them. Thus, if there is no existing entry for Smith County Gastroenterology Associates, a user can create one themselves, write a review, and other users will then be able to write their own reviews of Smith County Gastroenterology Associates -- all without the business' own oversight.

Even Medicare is climbing on the review site bandwagon, in a manner of speaking.[19] While it is not a true social media outlet, nor a site where users can write reviews, Medicare's Physician Compare site permits users to look at physicians and physician practices in comparison with other Medicare-participating physicians, based on information submitted to Medicare by the physicians themselves. Physician Compare draws its data from the Medicare online provider enrollment system (PECOS), the

[18] Lieber, Ron, "The Web Is Awash in Reviews, but Not for Doctors. Here's Why," New York Times, March 9, 2012. http://www.nytimes.com/2012/03/10/your-money/why-the-web-lacks-authoritative-reviews-of-doctors.html?pagewanted=all&_r=0.

[19] Other review sites which lack a social component include Healthgrades and RateMDs.com. Neither of these sites allow users to network the way social media sites do, and thus are beyond the purview of this chapter.

Physician Quality Reporting System, and eventually the Value Based Purchasing Program.[20] However, as stated above, Physician Compare does not permit patients themselves to comment about a practice, nor does it allow physicians to alter the information in the system.[21]

__.3 The Legal Issues.

Social media usage presents a potential minefield of legal issues. The nuances of social media can increase the complexity of these matters. Because the Internet itself permits information to be spread so rapidly, the social media context can introduce hurdles and considerations not applicable in the offline environment. Thus, the legalities of issues such as privacy and confidentiality, malpractice concerns, and defamation all become trickier when filtered through the prism of the Internet. With a better understanding of the nature of social media sites in general, as discussed above, this section examines the legal issues that physician practices face in the social media context.

__.3.1 Privacy and Confidentiality.

Patient privacy is a constant concern for physician practices, both in terms of compliance with state laws, and with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its related regulations. Social media, however, introduces new pressures. For example, some physicians have used social media to live-tweet surgeries.[22] This generates publicity for the institution live-tweeting the surgeries, and can create the impression that such places are forward-thinking and technologically oriented. While it is almost certain that the patients in these instances gave appropriate consent to the publicization of their surgeries (such as a HIPAA-compliant authorization), physicians' impulses to use social media as a marketing platform must be tempered with an understanding of the risks involved with respect to maintaining appropriate patient privacy and confidentiality. In addition to the usual issues that physician practices must address in relation to the privacy and security of patient PHI, both the physicians' own use of social media outlets for publicity, and the practice staff's personal use of social media each require different considerations and policies.

To the extent that a physician practice maintains a social media presence on sites such as Facebook and Twitter, the practice will need to ensure that it effectively polices its account to eliminate, or at least minimize, improper PHI disclosures. Generally speaking,

---

[20] Shay, Daniel, "Highest and Best Use Revisited," Health Law Handbook, 2013 ed., Alice G. Gosfield, editor, pp. 309-344.

[21] Physicians may update and correct their PECOS enrollment information, and have the ability to challenge information submitted to PQRS. For more information, see Shay, Daniel, "PQRS and its Penumbra," Health Law Handbook, 2012 ed., Alice G. Gosfield, editor, pp. 87-119.

[22] UCLA Live Tweets Brain Surgery, http://newsroom.ucla.edu/portal/ucla/ucla-live-tweets-surgery-to-implant-246356.aspx; Live Tweeting of Open Heart Surgery; https://dev.twitter.com/media/twitter-moments/social-good/open-heart.

practice communications over social media networks which contain PHI are likely to be considered "unsecured protected health information," as that term is defined under HIPAA.[23]

Since posts on social media websites lack encryption, any PHI that is improperly disclosed within the social media context will implicate both the HIPAA Privacy Rule, and the Breach Notification Rule.[24] Given how information is broadcast and spread on social media sites, such improper disclosures may result in serious fines.[25]

If, for example, a patient inquires about the results of recent diagnostic testing on the practice's Twitter account, there is no way the practice can reply without breaching the Privacy Rule under HIPAA (and thereby implicating the Breach Notification Rule). The reply itself will either be visible to the entire Internet, or to all of the users the practice has approved to follow it under Twitter; all of this is because Twitter does not allow the practice to limit which individual followers on Twitter can view the results. However, on a site such as Google Plus, the practice could reply solely to the patient alone. If the patient had given consent to be contacted using such a medium, there would be no HIPAA violation. On a site like Facebook, the user might have simply sent a private message to the practice, to which the practice can privately respond, again eliminating the possibility of a wider disclosure of PHI. Even seemingly innocuous communications, such as confirming appointment times, will likely at least constitute an improper disclosure of PHI under HIPAA, if they are visible to anyone beyond the patient themselves.

Similar issues arise with respect to the personal social media accounts of practice employees and agents. Physicians and other practice employees must therefore be trained in -- and remain vigilant about -- appropriate uses of social media and the posting of PHI to social media sites. Interactions with patients using private accounts can still result in an improper PHI disclosure, just as with a practice's interactions via "official" practice social media accounts. The scenario described above where the patient inquires as to test results could occur on a practice employee's personal account, just as it might on the practice's business account.

While it may seem hard to fathom, employees may even willfully post PHI. Consider the example of a recent news story involving a physician posting photographs of an

---

[23] 45 C.F.R. § 164.402. "Unsecured protected health information" is defined as PHI "that is not rendered unusable, unreadable, or indecipherable to unaauthorized persons through the use of a technology or methodology specified by the Secretary [of Health and Human Services]." In practice, this means PHI which has not been encrypted in accordance with guidance published by HHS, available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html.

[24] 45 C.F.R. §§ 164.500, et seq., and 164.400, et seq., respectively.

[25] See, Gosfield, Alice G., and Daniel Shay, "HIPAA Again: Confronting the Updated Privacy and Security Rules," Family Practice Management, May/June, 2013, pp. 18-22.

intoxicated patient in an emergency room.[26] Such incidents can expose the practice to HIPAA penalties, and can require expensive and time consuming damage control efforts, such as determining the full scope of the disclosure, attempting to eliminate as many outlets of the disclosure as possible, and the inevitable legal expenses for consulting with counsel and interacting with federal and/or state authorities.

The more likely scenario, however, is that of an inadvertent disclosure of PHI over an employee's personal social media account. For example, multiple employees at a practice might discuss a patient's case over social media with each other. Even if those employees do not use the patient's name, depending on the patient's condition and/or other particulars of the case, and depending on the privacy controls offered by the particular social media site and employed by each of the employees, the discussion itself may constitute an improper disclosure. A discussion of a patient with a relatively common condition, which does not reference the patient's name, age, locale, etc., will likely be permissible, provided that both employees are involved in the patient's care.

By contrast, changing even just a few elements of that hypothetical can create an improper HIPAA disclosure, such as if the patient has a unique or extremely rare condition, or is of particularly advanced age, or the discussion includes a sufficient number and type of patient identifiers to cause it to prevent the discussion from effectively being "de-identified."[27] For example, consider the case of an emergency department physician who discussed a patient's case over social media, whose post did not include the patient's name, but did include enough information that others in the community could identify the patient, resulting in an improper disclosure under HIPAA and a $500 fine by the Rhode Island Board of Medicine.[28]

Even something as simple as an employee posting a photograph of a gift brought by a patient -- which happens to be sitting on top of a daily appointment sheet containing patient names, phone numbers, and medical record numbers (an actual event on which I was consulted) -- is an improper disclosure under the HIPAA Privacy Rule, and could constitute a breach under the Breach Notification Rule. In each of these cases, the physician practice will have to conduct a risk analysis for breach purposes -- including determining the scope of the disclosure itself, how to mitigate the potential harm caused by the disclosure, and consult with legal counsel, all of which will cost time and money. Depending on how the disclosure itself was made and the specific sites used, the analysis may change. A single post limited only to Facebook or Twitter, posted at odd hours where other users are unlikely to have seen it, and which is promptly deleted, will pose less of a risk than an Instagram photo which automatically is posted on both Facebook

---

[26] Abramson, Alana, "Chicago Doctor Accused of Posting Photos of Intoxicated Patient," via Good Morning America, August 20, 2013. http://abcnews.go.com/US/chicago-doctor-sued-photographing-hospitalized-intoxicated-woman/story?id=20003303.

[27] 45 C.F.R. § 164.514.

[28] Conaboy, Chelsea, "For Doctors, Social Media A Tricky Case," Boston Globe, April 20, 2011. http://www.boston.com/lifestyle/health/articles/2011/04/20/for_doctors_social_media_a_tricky_case/?page=full.

and Twitter, and where the photo is retweeted by other users. Other considerations will include the number of "likes" or comments a post received before the post was deleted, the user's own privacy settings, the total number of social media connections (e.g., how many "friends" the user has on Facebook, and how many "followers" the user has on Twitter and Instagram), all will come into play in determining the scope and harm of the disclosure, and whether it constitutes a breach. By contrast, if the photo is "retweeted" on Twitter, and/or if the user has no privacy settings activated on Twitter (and therefore anyone on the internet can see their account), then there is effectively no way to know how many people saw the photo, and thus, the disclosure must be presumed to have been a breach.

Disclosure alone is a problem, but can potentially be mitigated. The real question is whether the disclosure rises to the level of a breach and whether the disclosure implicates the administrative headaches imposed by the Breach Notification Rule. Determining whether a breach has, in fact, occurred does not end merely because the disclosed information was not encrypted. The practice must conduct a full risk assessment.

This generally requires that the practice consider four factors: (1) the nature and extent of the PHI involved, including the type of PHI and the likelihood of re-identification; (2) the unauthorized person(s) who used the PHI or to whom the disclosure was made; (3) whether the PHI was actually acquired or viewed; and, (4) the extent to which the risk to the PHI has been mitigated. Naturally, any such risk analysis depends heavily on the facts of the disclosure incident. For example, if PHI is disclosed on Facebook, what privacy controls does the disclosing account have in place; are posts visible only by friends, by friends of friends, or by the general public? If the account is only visible to friends, how many friends could have seen the post? How many likes did the post receive? How many comments did the post receive? How visible was the PHI when posted to Facebook? If the PHI was in a picture, could a user have seen the PHI clearly when posted to Facebook?[29] These questions will all be relevant in analyzing how far the disclosure is likely to have spread, and whether it rises to the level of a reportable breach.

__.3.2 Malpractice Concerns.

Interaction with patients over social media networks can facilitate physician-patient communication by offering a more convenient and faster way for patients to contact the physician. Social media can also offer a mechanism by which physicians may rapidly disseminate educational information to patients as well as the general public. However, such interactions can expose physicians to malpractice risk, depending on both the nature of their communications, and the relationships between physicians and the individuals to whom they connect on social media sites.

[29] Facebook does re-size the photos posted by its users, so one should not necessarily assume that a picture taken with a 3 megapixel cell phone will necessarily be perfectly clear when re-sized to fit Facebook's requirements.

Within the social media context, where a physician must rely solely on the information a patient types, the normal risks of malpractice can increase significantly if a physician provides advice or diagnoses to patients online. With respect to such interactions, a threshold issue in determining the risk of malpractice exposure is whether a physician-patient relationship exists in the first place; if no such relationship can be shown to exist, then a malpractice claim against the physician will fail. The danger with social media, however, is that even minimal interaction can potentially establish such a relationship.

Due to the potential risks, many physicians are currently unwilling to interact with patients directly using social media. Online interaction with a patient can lack critical information, such as an opportunity to observe the patient's behavior, tone of voice, and body language, not to mention a lack of first-hand observation of symptoms and the ability to physically interact with the patient, such as through palpation or other physical manipulation. For example, a QuantiaMD survey conducted in August, 2011 found that, while physicians were interested in using a secure online environment for activities such as offering patients educational resources, monitoring patient health and/or behavior, and growing and/or maintaining their practices, over 40% of the physicians surveyed stated that they were not interested in diagnosing or treating patients online. One physician surveyed stated "There is no substitute, clinically, for actually seeing and examining the patient." Another physician simply predicted that such online use would lead to "Lawsuits, lawsuits, lawsuits."[30]

However, there is currently a dearth of established case law on medical malpractice occurring on social media websites.[31] This is no doubt due in part to the youth of the medium itself, and the fact that many medical malpractice cases settle before going to trial. However, although the cases have not directly addressed circumstances similar to an online interaction between an individual seeking treatment and a physician, courts have held that other minimal contacts with individuals can form the basis for the establishment of a physician-patient relationship.

The Ohio Supreme Court has stated generally that, "The physician-patient relationship arises out of an express or implied contract which imposes on the physician an obligation to utilize the requisite degree of care and skill during the course of the relationship. The relationship is a consensual one and is created when the physician performs professional services which another persona accepts for the purpose of medical treatment."[32] The

---

[30] Modahl, Mary, Lea Tompsett, and Tracey Moorhead, Doctors, Patients, & Social Media, September, 2011, p. 7. http://www.quantiamd.com/q-qcp/doctorspatientsocialmedia.pdf.

[31] There are, however, law review and other journal articles on this and related concepts. See, for example, Terry, Nicolas, P., "Physicians and Patients Who 'Friend' or 'Tweet': Constructing a Legal Framework for Social Networking in a Highly Regulated Domain," 43 Ind. L. Rev. 285; Bailey, Regina A., J.A., M.D., LL.M, "Cybermedicine: What You Need to Know," Health Lawyer, Vol. 23, No. 6, p.13, August, 2011; McCann, Michael A., "Message Deleted? Resolving Physician-Patient E-mail Through Contract Law," 5 Yale J. L. & Tech. 3, 2002-2003; Spradley, Paul, "Telemedicine: The Law Is the Limit," 14 Tul. J. Tech. & Intell. Prop. 307, Fall, 2011.

[32] Lownsbury et al. v Van Buren et al., 762 N.E.2d. 354, (Ohio, 2002), at 358.

Court further stated, "A physician-patient relationship, and thus a duty of care, may arise from whatever circumstances evince the physician's consent to act for the patient's medical benefit."[33] Although the case addressed a fact pattern involving whether an attending physician at a teaching hospital had a duty to a patient treated by a resident whom the attending physician was contractually obligated to supervise, the Court's language could easily be applied to the social media setting to impute a physician-patient relationship where a physician offers diagnosis or other medical advice to an individual with whom they otherwise have no treating relationship.

The Court of Appeals in Washington state held that "Physical contact with [a] patient is not an absolute prerequisite," in establishing a physician-patient duty.[34] The case involved a patient who had died of diabetic ketoacidosis. The patient had been a sailor on a fishing trawler located in the Bering Strait. When the patient became ill, the ship's purser and designated medical officer used a ship-to-shore telephone to call physicians working for a company that was contracted to provide ship-to-shore medical services to the company that owned the ship. At court, the physicians argued that they had no duty to the patient because they did not speak to, advise, or examine the patient. However, the record showed that the physicians, acting under their contract, had provided the purser with care instructions and advice for three days prior to the patient's death, including recommending hydration, running an intravenous line, and putting the patient on a 24-hour watch with valium administered every six hours.[35]

Similarly, the New York Supreme Court addressed a case in which a physician provided a telephone consultation to an emergency room physician assistant to treat a patient who had presented with an eye injury. The physician who received the call never personally saw the patient, and only provided advice to the physician assistant on the phone. In ruling on whether this telephone call could establish a physician-patient relationship, the Court stated, "...a doctor-patient relationship can be established by a telephone call...when such a call 'affirmatively advis[es] a prospective patient as to a course of treatment' and it is foreseeable that the patient would rely on the advice."[36] The Court further stated that the question of whether a physician's advice offered a sufficient basis on which to determine that a physician-patient relationship had been established is a matter for the jury to decide.[37]

When such minimal contacts as a telephone interaction can create an implied contract between patient and physician, it is easy to envision circumstances online where a

---

[33] Lownsbury et al. v Van Buren et al., 762 N.E.2d. 354, (Ohio, 2002), at 360.

[34] Lam v. Global Medical Systems, Inc., P.S., 111 P.3d. 1258 (Wash. App. Div. 1, 2005), at 1261.

[35] Lam v. Global Medical Systems, Inc., P.S., 111 P.3d. 1258 (Wash. App. Div. 1, 2005), at 1261.

[36] Cogswell v. Chapman, 249 A.D.2d. 865 (N.Y. Sup. Ct. App. Div. 3rd. Dept., 1998), at 866.

[37] Cogswell v. Chapman, 249 A.D.2d. 865 (N.Y. Sup. Ct. App. Div. 3rd. Dept., 1998), at 866.

physician establishes a physician-patient relationship with an individual who contacts them online asking for advice or treatment recommendations. Consider a scenario where a follower of a physician practice's Twitter account does not yet have an established relationship with the physician, and tweets a question to the practice about particular symptoms, such as shortness of breath and back pain. Depending on the content of the physician's response, a physician-patient relationship could be established. If the physician, for example, cites to a WebMD article and provides general information on the symptoms, it is possible a jury would find that no physician-patient relationship has been established. By contrast, if the physician responds that it could be a heart attack and recommends taking aspirin and going to an emergency room immediately, a physician-patient relationship may have been established.

With existing patients, the analysis will be more complex, given that the duty likely can be shown to exist. The question then becomes a fact-specific inquiry into whether the physician's response met the applicable standard of care, and if not, whether the failure to adhere to such standard was a proximate cause of the patient's harm.

__.3.3 Defamation

Whereas malpractice risks within the social media context arise from physician-patient interactions, defamation concerns derive more from the independent actions of patients online -- specifically, the posting of negative statements and reviews in various online fora. A patient can just as easily complain on Facebook about a physician or physician practice as they can on Yelp or Google Pages. This begs the question of what recourse physicians have to respond to such complaints, particularly when they are unfounded.

If the patient has posted to the practice's own Facebook Page, for example, it is a simple enough matter to delete the offending post. However, if the patient comments on their own Profile, the physician has no ability to remove it (and may be wholly unaware of it). Online review sites represent an additional wrinkle. An excellent discussion of this issue, particularly with respect to lawsuits against the review sites themselves, appears in the 2013 edition of this Handbook, in Todd A. Rodriguez, Esq.'s chapter.[38] In broad strokes, it is extremely difficult to succeed in a lawsuit against a website such as Yelp for acts of defamation by the site's users. Review sites of this sort are usually protected by federal statute, as well as common law.

Lawsuits brought against users who post reviews, rather than the review sites themselves, on the other hand, represents a relatively new area lacking in court decisions. However, physicians have begun to file such cases against individual reviewers. For example, in Chicago, a plastic surgeon sued a patient over negative reviews posted by former patients on Yelp. [39] In California, another plastic surgeon sued seeking damages and injunctive

---

[38] Rodriguez, Todd A., "The Virtual Realities of Online Professional Reputation Management," Health Law Handbook, 2013 ed., Alice G. Gosfield, editor, pp. 345-368.

[39] Pirillo, Chris, "Doctor Suing Patients Over Negative Yelp Reviews," http://chris.pirillo.com/doctor-suing-patients-over-negative-yelp-reviews/.

relief against at least 12 online reviewers, only a few of whom could be positively identified, on sites including Yelp and DoctorScorecard.com.[40] Most of these cases against patients and individuals have not been successful; as of this writing, there have been no lawsuits won on the grounds that the statements themselves were knowingly false.

Another risk for physician practices looking to challenge bad reviews in a legal arena are so-called "Anti-SLAPP" laws. Many jurisdictions employ protections designed to prevent "strategic lawsuits against public participation" (or "SLAPPs"). These laws are designed to prevent businesses from stifling public comment about them, often by requiring that the business repay the individual they may sue for defamation, if the business loses the case.[41] In practical terms, this would mean that a physician who sues a patient who has posted a negative online review would need to carefully consider whether doing so is worthwhile, balancing the prospect of a lost lawsuit (and the need to both pay for the physician's own expenses in the lawsuit and the patient's expenses) against the actual and potential harm the patient's review may cause.

__.4 Practical Guidance

Shooting the social media rapids can prove a challenge for physician practices. Nevertheless, social media is now a fact of life with which such practices must contend, even if they maintain no social media presence on their own behalf. Patients and others will still discuss the practice online, and employees will undoubtedly have and use social media accounts, often across multiple sites. Thus, it is imperative for physician practices to develop mechanisms to both direct employee usage of social media, and to manage and maintain their own online presence.

__.4.1 General Guidance

The first step a physician practice should take is to establish clear and firm policies regarding the use of social media by practice employees both on and off the job.[42] For official practice social media accounts, practices should generally limit the number of people who can post using the account itself. This will prevent inappropriate messages

---

[40] Klien, Gary, "Greenbrae Plastic Surgeon Sues Online Critics," July 5, 2010, http://www.marinij.com/marinnews/ci_15444079.

[41] For further discussion of Anti-SLAPP laws, see Lee, Sean D., "'I Hate My Doctor': Reputation, Defamation, and Physician-Review Websites," 23 Health Matrix 573, Fall, 2013; Randazza, Marc C., "The Need for a Unified and Cohesive National Anti-SLAPP Law," 91 Or. L. Rev. 627, 2012; Richards, Robert D., "A SLAPP in the Facebook: Assessing the Impact of Strategic Lawsuits Against Public Participation on Social Networks, Blogs and Consumer Gripe Sites," 21 DePaul J. Art, Tech. & Intell. Propl. L. 221, Spring, 2011; www.anti-slapp.org.

[42] For additional resources and further discussions about social media in the health care industry in general, and developing company policies in specific, see Goldman, Daniel S., "Managing the Risks of Social Media in Healthcare," Health Law Handbook, Alice G. Gosfield, editor, 2012 ed., pp. 285-316.

from being posted in the practice's own name. The fewer people who can access the account, the less likelihood there is of an error.

For personal usage, practice policies should limit the time employees may spend on social media during work hours.[43] However, there are limits to how a practice's policies regarding employee social media usage may reach, particularly with respect to the content of employees' posts. The National Labor Relations Act[44] (NLRA) protects certain employee rights, including rights to organize and engage in "concerted activities for the purpose of...mutual aid or protection."[45] The National Labor Relations Board (NLRB) has published guidance on how the NLRA applies to the degree to which employers may control their employees' activity on social media sites.[46] The NLRB has further provided examples of how it has applied the NLRA to employer social media policies in specific cases.[47]

In cases where the policies were found to be unlawful -- and termination of employees was therefore found to be unlawful -- the activities prohibited by the employer's policy were usually too broadly defined and could therefore include "concerted activity." For example, an ambulance service was found to maintain an unlawful policy which prohibited employees from making disparaging comments online when discussing the company or the employee's superiors, coworkers, and/or competitors, because it was too ambiguous and could include "concerted activity" such as protesting or holding a picket sign complaining about a superior.[48] This case, as well as others in the same guidance, show that it is essential that physician practice employers who seek to control the content -- rather than merely the timing -- of employee social media posts must tailor any such

---

[43] Physician practices may be tempted to absolutely prohibit the use of social media sites during work hours, but unless it physically blocks those sites from its own network and monitors employees' online activity, they will have difficulty enforcing such rules. Moreover, given the ubiquity of smartphones, even a bathroom break can be an opportunity for an employee to post on a social media site.

[44] 29 USCA § 151, et seq.

[45] 29 USCA § 157.

[46] http://www.nlrb.gov/news-outreach/fact-sheets/nlrb-and-social-media.

[47] Memorandum OM 11-74, Re: Reporting of the Acting General Counsel Concerning Social Media Cases, August 18, 2011.

[48] Memorandum OM 11-74, Re: Reporting of the Acting General Counsel Concerning Social Media Cases, August 18, 2011, pp. 5-6. By contrast, an employer that provided emergency and nonemergency medical transportation to municipal, residential, commercial, and industrial customers was found not to have unlawfully discharged an employee for posting to a Senator's Facebook "wall" (or "timeline") that the employer was the cheapest service in town, paid employees $2 less than the national average, had only two trucks for an entire county, referenced an incident in which a crew responding to a cardiac arrest call did not know how to perform CPR, and that the state had awarded a contract to the employer solely to save money. The employee was found to have not engaged in "concerted activity," although the employer's policies -- if any -- were not addressed. Still, the case proves illustrative with respect to what would not be subject to protection under the NLRA. Id., at pp. 15-16.

policies to explicitly permit "concerted activity" under the NLRA, or to only exclude activity that would not otherwise be protected (e.g., impermissible HIPAA disclosures).[49]

Generational differences will also likely be highlighted by the use of social media, and will need to be taken into account by physician practices, both with respect to practice employees (and both professional and non-professional employees), and with respect to patients themselves. Users of social media tend to be younger.[50] Thus, younger people, particularly those who have grown up with social media as a simple fact of life, are less wary about the use of social media and are, perhaps, more comfortable with "broadcasting" their lives. By contrast, those who grew up before the advent of social media came of age in a world where life was simply conducted in a more private manner.

These generational differences may lead younger patients to feel "shut out" of their physicians' lives (particularly if the physicians themselves are also younger), when the patients are accustomed to more open access to the lives of their contemporaries. Similarly, younger employees may not think twice about the implications of their social media interactions or how such activities could harm their employer. At the same time, older patients may not be as comfortable using social media, and may therefore miss much of a physician practice's social media presence -- including marketing and educational information. Older physicians and practice employees may be far less likely to engage in improper use of social media sites, but may be disinclined to capitalize on the beneficial aspects of social media.

With respect to physicians' own social media presences, some degree of management is advisable. Several physician organizations have published policies stating that strict separation between the physician's professional and personal life online is the ideal approach. In other words, physicians should have two identities online: a public one, and a private one. For example, the American Academy of Family Physicians (AAFP) states,

> "We recommend that physicians not accept patient friend requests in their personal social networks. This not only protects the physician from exposure to litigation but maintains the boundary needed for a professional physician-patient relationship. Facebook, in particular, offers a way to keep this boundary intact by the use of a business page."[51]

---

[49] For further discussion of the NLRB and social media policies, see Goldman, Daniel S., "Managing the Risks of Social Media in Healthcare," Health Law Handbook, Alice G. Gosfield, editor, 2012 ed., pp. 285-316.

[50] See, Brenner, Joanna, "Pew Internet: Social Networking (full detail)," August 5, 2013, http://pewinternet.org/Commentary/2012/March/Pew-Internet-Social-Networking-full-detail.aspx.

[51] "Social Media for Family Physicians: Guidelines and Resources for Success," American Academy of Family Practitioners, http://www.aafp.org/dam/AAFP/documents/about_site/SocialMediaFamPhys.pdf , p.8.

Similarly, the American Medical Association (AMA) takes the position that physicians should "maintain appropriate boundaries of the patient-physician relationship in accordance with professional ethical guidelines, just as they would in any other context," but also states that "to maintain appropriate professional boundaries, physicians should consider separating personal and professional content online."[52]

However, in an article published in the Journal of the American Medical Association in August, 2013, doctors challenged the AMA's position, arguing that is operationally infeasible to separate a physician's professional and private lives in a social media setting. Moreover, the authors argued that it could be harmful to physicians to maintain two separate online identities, and could erode trust between a patient and physician if the physician appeared to be "hiding something" from the patient. Instead, the article suggested that the AMA's position on social media should focus more on whether the content posted is appropriate for a physician to post in a public space. This would require no separation of identity, nor adoption of a new approach to behavior online (such as maintaining two separate accounts, one for work and one for personal use).[53]

Other professional societies have taken a different approach as well, and the issue continues to develop. The American College of Physicians (ACP) adopts a more flexible approach than the AAFP and AMA. The ACP recommends that standards for physician behavior be consistent across multiple mediums, stating:

> "Physicians who use online media, such as social networks, blogs, and video sites, should be aware of the potential to blur social and professional boundaries. They therefore must be careful to extend standards for maintaining professional relationships and confidentiality form the clinic to the online setting. Physicians must remain cognizant of the privacy settings for secure messaging and recording of patient-physician interactions, as well as online networks and media and should maintain a professional demeanor in accounts that could be viewed by patients or the public."[54]

Meanwhile, the American Osteopathic Association currently has no official policy position on social media sites used by physicians, but indicates that it is in the process of establishing one.[55]

---

[52] American Medical Association, Ethical Rule 9.124, "Professionalism in the Use of Social Media," http://www.ama-assn.org/ama/pub/physician-resources/medical-ethics/code-medical-ethics/opinion9124.page.

[53] "JAMA Viewpoint Calls for Revising Physician Social Media Guidance," iHealthBeat, August 14, 2013, http://www.ihealthbeat.org/articles/2013/8/14/jama-viewpoint-calls-for-revising-physician-social-media-guidance.

[54] American College of Physicians Ethics Manual, 6th Ed., http://www.acponline.org/running_practice/ethics/manual/manual6th.htm.

[55] AOA Policy Compendium, 2013, Policy H352-A/13, p. 182.

In practice, the choices for physicians may not be quite as stark as those advocated by the AMA. For physicians who feel most comfortable maintaining separate personal and public social media accounts, this may be the simplest approach. However, for physicians who find such an approach unrealistic, it may be more appropriate for them to adopt a different mindset when operating in the social media sphere. Relationships online can be approached in a manner similar to how offline relationships are conducted. In this regard, the ACP position seems the most feasible: if a physician would establish a friendship with a patient in an offline context, the physician should feel free to "friend" the patient in the social media context; if not, then the physician should not "friend" them.

The online context itself may come into play as well. It may be easier to maintain a more "public" vs. "private" distinction on a site like Facebook, where a business can establish its own Page, while physicians keep their Profiles private. The physician would not necessarily need to treat the Profile as a "separate identity," as if the physician were a masked superhero. If a patient were to discover the physician's Profile or private account, the physician could simply redirect them to their public Page. In essence, this would be no different from the physician refusing to give out their home phone number to a patient.

However, more public services like Twitter or Instagram present a different problem. Since neither service distinguishes between "public" and "private" accounts, physicians may prefer to maintain two separate accounts. If not, they should recognize the public nature of the medium, and hew towards caution in what they post. It would likely be counter-productive at least for a physician to counsel a patient to stop smoking, only to post a picture of themselves smoking a cigarette on Instagram. Even on a site with robust privacy controls, physicians should be aware of the difficulty in controlling information once it has been posted; there is nothing to stop another user with access to the physician's account from copying and pasting a screenshot from the physician's account or otherwise sharing the image itself in a more public medium.

It is also helpful to understand the different functions and functionality of social media sites, particularly with respect to privacy features. Knowing what options are available for a user's privacy may help craft more effective social media policies. For Facebook, Google Plus, and other sites with similar capabilities, patients who are added to a physician or practice employee's "friends" list may be able to be segregated to a particular list of friends with customized privacy settings, such as a "Patients" list that can only see certain types of posts. For sites like Twitter, it may simply be easier to keep one's profile private altogether, or to establish two accounts (or only use the practice's account for public postings). Understanding the differences in the sites can be particularly helpful for managing issues such as the complexity of a PHI disclosure on a Facebook account which is linked to Instagram and Twitter accounts.

__.4.2 Avoiding HIPAA Concerns

Information on social media sites can spread rapidly. To craft effective HIPAA policies that can address the reality of employees use of social media sites, physician practices must understand how information flows on the various social media sites, as well as how the flow of such information can be restricted using privacy features. With this information in mind, practices can develop effective policies regarding social media and HIPAA, and engage in meaningful education of practice employees.

All practice employees -- including physicians -- should be educated on HIPAA in the social media context. This should include repeated reminders of what actually constitutes PHI, using examples. It is not enough to inform practice employees that names, birth dates, and unique medical conditions all can constitute PHI; this information must be put into the social media context.

Consider a simple photograph. Social media users frequently post photographs, including from their own workplace. It might seem obvious in a general discussion that a photograph of a patient would constitute PHI, but it may help to illustrate, for example, that there is fundamentally no difference for HIPAA purposes between a picture taken of a sleeping patient unbeknownst to them, and a picture posed with a smiling, friendly patient. Posting either online would constitute a violation of the HIPAA Privacy Rule. The patient's implicit consent does not constitute an authorization to disclose their PHI. Similarly, even seemingly innocuous photographs may contain PHI in the background, such as documentation or visible computer screens with patient information. One exercise that might be helpful in training would be to create a "Find the PHI" game using photographs from within the practice itself.[56]

These examples can also be posted online to help illustrate how fast a disclosure of this sort can spread and be viewed. Such an exercise can also be used to show how interaction between employees can lead to disclosures. An exemplar photo could be posted, followed by an example of another employee disclosing further information in the discussion, or re-posting the photo or other information. The benefit of such exercises is that they provide concrete, real-life examples of how disclosures can happen, rather than an abstract general discussion of why it is a HIPAA violation to post such information online. When employees can see in person how their actions might jeopardize the confidentiality of patient information, they may be more likely to internalize practice policies surrounding social media use.

__.4.3 Avoiding Malpractice Concerns

Perhaps the simplest way for physicians to avoid or at least minimize malpractice exposure in the social media context is to simply not engage patients directly in any clinical sense on social media networks. In other words, physicians should not respond

[56] Such photographs should be taken strictly for the purposes of HIPAA education, and should not be used outside of that context. They should also not contain any actual patients or real life PHI, but rather example PHI referring to fictional patients.

directly to patient inquiries about clinical or potential clinical matters directly through social media sites.

Consider the following real-life example from a physician who maintains an active Twitter account and posts general wellness information. The physician was contacted by another twitter user. The user inquired as to whether certain symptoms (discomfort and chest pressure) were indicative of a heart attack or indigestion. The physician replied "If movement, deep breath, swallowing makes pain worse or better, it is NOT a heart attack."[57] While other information posted to the account is general, the tweet in question could be viewed as diagnosis and medical advice, upon which the tweeting user might rely, possibly to their detriment. This is risky behavior for the physician.

The Doctors Company, one of the leading medical malpractice insurance companies in the country, suggests that social media sites like Twitter, Facebook, etc. are "not appropriate for doctor-patient communications because they are too informal and lack an atmosphere of professionalism--making it easy to lapse into casual conversation and inadvertently cross the boundary between personal and professional relationships."[58] The company further advises doctors not to discuss individual patients, provide medical advice, or respond to clinical questions from patients or otherwise practice medicine on such sites. In addition, doctors are reminded to presume that anything they say or post is in the public domain and is likely retained in a permanent record that can be discovered in a lawsuit.[59]

It may not be necessary for physicians to completely avoid social media interaction with patients, although some caution is advisable. With established patients, physicians should generally not respond directly to clinical inquiries, except – at most – to state medical facts, cite respected sources of information, or otherwise offer educational information. For example, there is likely little risk posed to the physician if a patient posts on a physician's Twitter account asking about which foods are most likely to trigger migraines, the physician could cite to a WebMD entry, or a JAMA article on the subject, or simply offer a general answer. By contrast, if the patient asks a clinical question about their own health, such as sending a picture of a wound and saying "Does this look infected?" the physician should avoid online diagnosis, and direct the patient to either schedule an appointment, call an emergency department, or at least call the physician on the phone or contact them via email or a secure patient portal.[60] The goal in such an

[57] https://twitter.com/RMichlerMD/status/304298604531699712. The physician's account has, as of this writing, 263 followers, while the user who wrote the initial question about the symptoms has a total of 179 followers, meaning that this advice could be seen in the twitter feeds of at least 442 people. Moreover, neither account is currently private, so the message can be seen by anyone with a functional web browser.

[58] Troxel, M.D., David B., "Electronic Medical Record and Social Media Malpractice Risks," The Doctor's Advocate, Third Quarter, 2010, pp. 2, 6, p. 6.

[59] Troxel, M.D., David B., "Electronic Medical Record and Social Media Malpractice Risks," The Doctor's Advocate, Third Quarter, 2010, p. 6.

[60] The phone offers an additional protection for physicians in that it is confidential, and does not leave a permanent electronic record available online.

interaction is to avoid harm, since it could be argued that a duty has already been established by virtue of the existing physician-patient relationship.

For individuals who have not become patients, physicians face a more difficult challenge. One purpose of social media is to encourage such patients to come to the physician's practice. Accordingly, physicians have some incentive to interact with such patients. However, physicians should take all steps necessary to avoid establishing a physician-patient relationship with such individuals, prior to them actually visiting the office itself. Therefore, physicians should not answer any clinical questions posed by such individuals, or even engage in telephone consultations. Rather, they should suggest that these individuals set up an appointment to become a patient, and remind them that they do not provide medical treatment online or over the phone. In this scenario, the goal is to avoid establishing a duty to the individual in the first place.

In either scenario, both physicians and those office personnel who have access to practice social media accounts should be trained in how to respond to such inquiries, and the office's policies should clearly state how to communicate online with both patients and non-patients.

__.4.4 Avoiding Reputational Harm

It should come as no surprise that bad reviews online leave physicians angry. Understandably, they may therefore take it as a personal affront when a patient posts a bad review of them online. A patient may not realize that, in spite of an unsatisfactory clinical outcome, the physician performed their part to the best of their abilities and in keeping with the standards of medical practice. In such a scenario, it will be essential that the physician evaluate the review as dispassionately as possible. A physician should be cautious in crafting any response to the review, if he or she chooses to respond at all.

If the site in question has a private messaging feature, the physician should consider responding privately, using public responses only as a last resort. [61] A private response should be acknowledge the patient's complaint, but in a way which does not create an admission against interest that can be used in a potential malpractice suit in the future. A telephone call or in-person meeting with the patient may therefore be better, rather than creating an electronic written record of the discussion. With respect to public responses, the substance of the response should only reference the physician's standard protocols, rather than including any kind of specifics regarding the patient's complaint; discussing the specifics of a patient's treatment or procedure could breach the physician's duty of confidentiality.

---

[61] Goldman, Eric, "How Doctors Should Respond to Negative Online Reviews," Forbes, November 21, 2013, http://www.forbes.com/sites/ericgoldman/2013/11/21/how-doctors-should-respond-to-negative-online-reviews/.

If the physician responds at all, the response itself should also be courteous. A harshly worded or vehement response denying the information contained in the review, or a response which conveys indifference can harm the practice. A better approach is to encourage the patient to contact the practice directly over the phone or email, to help resolve their concerns. Such an approach will avoid potential malpractice exposure that admitting actual wrongdoing might create, will avoid an inadvertent violations of patient confidentiality, and will create a public appearance that the practice is willing to work with patients who have complaints. This is essential, because responses left by the practice on sites where patients can post reviews become part of the practice's public face, just as much as the practice's own website. Thus, the practice must ensure that it does not appear rude or dismissive of the patient's concerns.

Instead of attempting to directly respond to -- or worse, sue for -- negative reviews, some advocate accentuating the positive. For example, physician and social media blogger Kevin Pho, M.D. recommends encouraging that physicians provide clear instructions to patients on how to rate the physician positively on websites.[62] Others cite to the impact that multiple reviews may have on a physician's rating, as compared to a lone negative review. Moreover, in some instances, patients themselves will defend the physician, rather than the physician needing to become involved at all.[63]

False reviews, reviews from non-patients, or defamatory reviews provide a more difficult case. First, the practice may not always be able to tell whether the individual who posted is actually a patient. Website user names may not track to patient records. These can be first-name-last-initial user names, email addresses, or wholly made-up user names like "Scoob4938" or "HealthyGuy18." The practice will have to carefully weigh the potential damage that the review may cause against the cost and effort that will be required to identify the user.[64] Such a process would no doubt prove expensive, and would then only be worthwhile if the practice thought it could both bear the cost of litigation, and recoup its expenses from the individual. Moreover, if the state in which the physician is considering filing a lawsuit is one with an Anti-SLAPP statute, the physician will need to seriously consider the chance of succeeding on the merits of the case. It may, therefore, be cheaper to ignore the problem.

Depending on the site, a better approach may be for the practice to use built-in site tools to challenge an allegedly false review and ask that it be removed. Moreover, not every

---

[62] Pho, Kevin, M.D., "Dealing with a Negative Online Review on a Physician Rating Site," May 3, 2011, http://www.kevinmd.com/blog/2011/05/dealing-negative-online-review-physician-rating-site.html.

[63] Goldman, Eric, "How Doctors Should Respond to Negative Online Reviews," Forbes, November 21, 2013, http://www.forbes.com/sites/ericgoldman/2013/11/21/how-doctors-should-respond-to-negative-online-reviews/.

[64] Tracking down such a user may not be a simple task, either. Depending on the site in question, the user's name may be a false identity, or the user's account could be registered to an otherwise anonymous email address. Even if the practice could track down the user from an internet protocol address, this still may not provide an actual identity and/or street address, but rather the location from which the account was created or the review was posted.

false review necessarily needs to be challenged. Some may be obviously fake, or so poorly written as to be nearly illegible. These reviews are more likely to be ignored by other potential viewers of the site. By contrast, a well-written, thought-through review will be more likely to be taken seriously, and therefore should be taken seriously by the reviewed physician.

__.5 Conclusion

Social media usage should be accepted as a fact of life for the foreseeable future. As more and more individuals gain access to -- and take advantage of -- the Internet, more will be drawn to social media sites. While much current discussion about the American health care industry focuses on the Baby Boomers, physicians must also begin to orient themselves towards the demographic reality that today's younger patients are the health care consumers of tomorrow -- and today. With the passage of the Affordable Care Act, the number of covered individuals below age 26 is estimated to have risen by approximately 3 million between September 2010 and December 2011.[65] That number will likely only increase as more Americans obtain health care coverage through Federal and state exchanges. As these individuals gain greater access to the health care marketplace, they will likely seek to interact with physicians and physician practices through social media.

Rather than balk at the prospect of maintaining a social media presence, physician practices should embrace the potential opportunity to reach a wider audience. Moreover, merely because a physician practice decides to forego creating social media pages for itself, that does not mean that it can afford to ignore social media altogether; practice employees will still likely use social media, and there is nothing to stop other individuals from discussing (or even impersonating) the practice in the social media context. Physician practices must therefore develop carefully designed social media policies to control employee behavior. Such policies must be drafted narrowly enough to avoid being found unlawful under the NLRA, but broadly enough to effectively control for HIPAA disclosures and minimize malpractice risk.

Even physicians who choose not to establish their own social media presence must still monitor their online reputations. Reputation management must also be considered when creating practice social media policies. Likewise, physician practices must consider whether and how to engage with social media users who post negative reviews or comments. Suing for defamation, while perhaps emotionally satisfying, may prove ultimately fruitless -- or even costly in the case of Anti-SLAPP jurisdictions -- and may harm the practice's reputation. Alternative approaches may be preferable. In their development of such social media policies and strategies, legal guidance is essential. Physician practices must understand both their legal risks in the social media context, as well as the limits they face in how they may respond.

---

[65] Zimlich, Rachel, "Number of Insured Young Adults Increased Significantly After ACA," Medical Economics, February 26, 2013, http://medicaleconomics.modernmedicine.com/medical-economics/news/user-defined-tags/primary-care-physicians/number-insured-young-adults-increas.