

Issue Brief:

Managing Online Patient Engagement

October 2018



NATIONAL ASSOCIATION OF
Community Health Centers

7501 Wisconsin Avenue
Suite 1100W

Bethesda, MD 20814

Phone 301.347.0400

www.nachc.com

Managing Online Patient Engagement

An integral component of health center practice operations is patient engagement. Whether patient engagement is done over the phone, in person at the health center, via patient portals or online, health centers need to be prepared to provide a positive patient experience. However, managing patient expectations about online engagement can present challenges. Health care has gone digital and health center patients want to engage around their health care online. Social media platforms provide individuals with a community whereby they can share and access health information, learn more about a given provider, and provide feedback regarding their patient experiences at the click of a button. As social media options continue to grow, the number of patients who use the internet to discuss health information will also likely continue to grow. As a result, health centers face a delicate balancing act: a desire to meet patient communication preferences and leverage the benefits of social media versus the health center's risk management obligations to keep such communications secure, appropriately documented, and useful to the health center enterprise. For health centers, the common risks associated with social media and electronic communication generally fall into three categories: (1) privacy and security, (2) medical malpractice, and (3) reputation.

This Issue Brief:

- Addresses the key ways that health centers can benefit from using social media to increase patient engagement;
- Discusses the associated risks surrounding patient online engagement; and
- Provides strategies that health centers can apply to protect against associated liabilities.

I. Benefits of Online Patient Engagement

Health centers are becoming increasingly aware of the power of social media. The horror stories about the impact of a patient's negative review or the recklessness of an employee's online behavior are enough to make an absolute ban on engaging on social media look rather appealing. Nevertheless, health centers should examine the benefits of connecting with patients online:

■ Keeping Up with The Times:

Using social media platforms to connect is now ubiquitous in our society. A recent Pew Research Center survey found that some form of social media is used by:

- 88% of individuals between the ages of 18-29 years old;
- 78% of individuals between the ages of 30-49 years old;
- 64% of individuals between the ages of 50-64 years old; and
- 37% of individuals who are 65 years and older.¹

The ease and convenience of online engagement has developed an expectation of increased transparency between the patient and all of the patient's providers. In the 21st century, nearly every professional and business maintains some presence online—a dedicated website, Facebook page, LinkedIn profile, *etc.* Even if the health center does not have a large online presence, it is more likely than not that its patients spend a significant amount of time online. In fact, patients may go online to find out more about the health center, including scouring through patients' reviews on providers. Just like searching online for a local restaurant, it is a common practice to use the internet to search for potential health care providers nearby. As a result, cultivating a robust and positive online presence can be a valuable tool for health centers that are seeking to wield influence.

The term “social media” is used to describe websites, applications, and other electronic platforms that enable users to create and share content such as pictures, personal messages, videos, ideas, news stories, and other information. While the scope is ever-expanding, this includes social networking websites such as Facebook, Twitter, Instagram, LinkedIn, Pinterest, and YouTube, as well as a multitude of blogs and other sites that have user-generated content. Online review sites (*e.g.*, Yelp, Healthgrades, RateMDs, and ZocDoc) may also be considered social media.

■ Improving Patient-Provider Relationships:

Education

Patients are increasingly seeking health information on the internet to make health decisions. Often, the information floating around has not been properly managed for updates or is just simply inaccurate. As a result, many patients are self-diagnosing their conditions without ever seeing a provider and solely at the guidance of patient-based chat forums. To combat these issues, health centers can use online platforms to disseminate health education to their patients. The fact that the information stems from a health care provider rather than a patient-led forum not only provides patients with access to up-to-date and accurate information, but also has the additional benefit of increasing the platform's visibility. By doing this, a health center can shape the reputation it has within its community as an organization that cares about the quality of information its patients are accessing and thus increase trust and patient engagement with the health center itself.

¹ “Social Media Use in 2018.” Pew Research Center, Washington, D.C. (March 1, 2018) <http://www.pewinternet.org/2018/03/01/social-media-use-in-2018/>.

Improved Services and Accountability

It is natural to balk at the idea of monitoring patient online reviews, especially when there is so little control over what patients post and, as discussed later in this Issue Brief, in light of legal consequences, how a health center may respond is restricted. It is, however, still important to regularly review and consider patient complaints and reviews. Honest reviews can be helpful feedback that a health center can use to collect more detailed information about its patients, improve services, and let patients know that the health center is listening to their concerns.

■ **Strategic Marketing:**

A well-constructed social media presence can be an important part of a health center's marketing strategies. Health centers can use available data and analytics from social media websites to track and analyze which forms of social media are reaching the most people and tailor its strategies accordingly. Further, social media is not just good for encouraging new patients to join a health center practice, it is also good for recruiting providers, staff, medical students, residents, volunteers, board members, and others, as those people may also be using social media to learn more about the health center.

II. Risks Associated with Online Patient Engagement

As with any powerful tool, online patient engagement can be harnessed for good but it can also expose the health center to a number of risks, especially regarding maintaining compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations.

1. HIPAA Implications

HIPAA (and related legislation such as (the Health Information Technology for Economic and Clinical Health (HITECH) Act, a law promoting the meaningful use of health information technology) and their implementing regulations govern the privacy and security of protected health information (PHI), including electronic protected health information (ePHI). Of particular importance to the discussion of online patient engagement is the HIPAA Privacy Rule which prohibits the use or disclosure of PHI outside of certain exceptions.²

Although HIPAA does not specifically regulate the use of social media, health centers could unintentionally run afoul of the HIPAA Privacy Rule by posting PHI about patients (e.g., comments, photos, video) without the patients' permission. Violations of HIPAA can mean civil and criminal penalties for a health center and its employees. In addition, state medical boards may also discipline providers for privacy violations with punishments ranging from a simple reprimand to a suspension or revocation of a license.

A. HIPAA Privacy Risks

Most posts on social media are public or semi-public; most are not secure or otherwise encrypted. Even if the post is intended to be private, it's easy to mistakenly post a message publicly. Further, any followers (*i.e.*, any person the

² Health centers should also be familiar with the HIPAA Security Rule which contains the technical, physical, and administrative safeguards that health centers must implement to safeguard and protect PHI, as well as any state laws and regulations regarding the privacy and security of patient information in their individual jurisdictions.

“Protected Health Information” means individually identifiable health information that is:

- (i) Transmitted by electronic media;
- (ii) Maintained in electronic media; or
- (iii) Transmitted or maintained in any other form or medium.

“Individually identifiable health information” is information that is a subset of health information, including demographic information collected from an individual; and:

- (i) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
- (ii) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
 - a. That identifies the individual; or
 - b. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

“Electronic protected health information” means individually identifiable health information that is transmitted by electronic media and/or maintained in electronic media.

user shares information with online through a social media site) can share that information with a wider audience, with or without the user’s permission. For example, a friend can take a screenshot of a “private” post (*i.e.*, make a copy of the information by taking a picture) and share it from his or her personal social media account. Also consider this scenario: a patient posts a status update on the health center’s Facebook page (or “tags” the health center from the patient’s personal page) regarding a confirmed positive pregnancy test. Any health center response to the post acknowledging that the individual is a patient of the health center could violate the HIPAA Privacy Rule and state law counterparts.

Instead of responding to the specific comment of a patient on social media, health centers should consider developing a standard message directing patients to a more appropriate venue for health concerns.

In addition to concerns about the risks associated with the maintenance of the health center’s own social media presence, health centers should also be aware of the possibility of improper disclosures on the personal accounts of health center employees. For example, a health center employee who posts a photo posing with her patient who has recently recovered from cancer or, even more inadvertently, a photo showing off a new haircut that shows a patient in the background, has created exposures. Posts do not have to be made from the health center or during work hours to be problematic: an employee posting at home on a personal account may still pose a risk to the health center if the information shared includes PHI or otherwise identifies a patient. As such, health centers and their staff members must avoid any unauthorized disclosure of PHI in any form on social media. Particularly, health centers should remember that photographs of patients that can identify them (usually photographs that include facial features) are considered individually identifiable health information. As such, any information posted on social media concerning past or current patients must be de-identified (*i.e.*, all individually identifiable information must be removed).

Any health center response to patients’ online comments could violate the HIPAA Privacy Rule and state law counterparts. Health centers should, however, still let patients know that the health center is invested in addressing patient concerns. One way to do this is by developing a standard response message such as the following:

“In accordance with laws about patient confidentiality, it is XYZ Health Center’s policy to refrain from responding to any comments made on this platform. We invite patients, their families, and members of our community to direct any concerns or requests for information about XYZ Health Center to us directly by contacting us at XXX-XXX-XXXX or concerns@xyzhealthcenter.org.”

B. Strategies to Protect Against HIPAA Privacy Risks

Unfortunately, the use of social media in the health care industry is a quickly evolving landscape, making best practices a moving target. There are, however, practical steps that a health center can take to protect against the risks associated with online patient engagement.

- Conduct a **risk analysis** to understand how health center staff currently engage with patients online. Consider conducting an informal survey about patient comfort with technology and interest in electronic messaging.
- Establish and update **clear social media policies** regarding the health center's online presence and staff interaction with patients online, as well as organizational standards regarding PHI and social media use:
 - Set appropriate limits on the ways in which staff may interact with patients online and the scope of those interactions (e.g., declining friend requests from patients);
 - Discourage staff from using personal accounts to connect with the health center or health center patients (e.g., responding to a patient question on the health center's business page or profile from a personal account);
 - Encourage providers and staff to use enhanced privacy settings on personal social media accounts to prevent patients from finding these accounts;
 - Urge staff to “pause before they post” and consider whether content is appropriate to share before the post goes online and becomes permanent; and
 - Outline how information is posted on the health center's business pages (e.g., which staff members are authorized to post and who approves posts).
- **Inform patients** about how best to communicate electronically with their provider (e.g., not posting questions about personal conditions to social media) and the risks of using social media to contact the health center about medical concerns. If a provider wants to share a patient's story or picture in connection with the health center on social media, be sure to obtain patient HIPAA-compliant authorization first.
- Steer patients away from social media and toward **secure methods of communication** for discussions about their health care. Provide clear examples that illustrate when a question can be resolved through a secure message on a patient portal and which common scenarios are more likely to require an in-person visit and/or physical exam.
- **Train employees** on the potential risks of online communications with patients and provide the tools to respond to common patient behaviors (e.g., not turning to Facebook to vent about a particularly difficult patient interaction, because even without mentioning the patient by name, there could be sufficient information to identify the individual). Encourage staff to use the highest privacy settings on personal accounts and review website privacy policies and terms of use when new versions are available.
- Develop a clear internal **process for reporting** unauthorized disclosures of PHI, including inappropriate use of social media in connection with the health center or health center patients. Where appropriate, ensure compliance with HIPAA's breach notification rules and their state law counterparts.

2. Potential Malpractice Claims

A. Health Center Social Media Accounts

There are two main areas of concern when it comes to social media, technology, and medical malpractice:

- Committing an act that constitutes potential malpractice; and
- The impact of social media use on a potential or pending malpractice proceeding

With some social media websites that offer aid in identifying symptoms or crowdsourcing health advice, many patients expect the convenience of instant communication when it comes to their health care providers. As a result, patients may find it convenient to reach out to providers (or health centers) with medical questions through public channels on social media, even if the health center has a patient portal or other secure means of communication set up for this purpose. Or, a patient may reach out to a provider with whom (s)he does not have an established relationship for medical advice due to that provider's expertise or social media presence. A provider's response to this question could establish a treatment relationship, making the provider accountable for the advice.

Whether or not a provider owes a "duty of care" to a patient depends, in part, on whether (or not) a provider-patient relationship has been established. If a provider owes a duty of care to a patient and (s)he fails to diagnose, treat or otherwise care for that patient, the provider could face a malpractice action.

Online interactions between patients and the health center's social media pages complicate this question by creating uncertainty around when and how such a relationship begins and what type of activity constitutes establishing a provider/patient relationship. Unfortunately, there are few clear legal lines defining when an interaction on social media establishes (or clearly does not establish) a provider-patient relationship. Health centers, however, can and should explain to patients how to communicate with providers safely and securely, providing examples of when it is appropriate, or not, to use certain channels. In addition, the

Successful malpractice claims must prove the following elements:

1. A provider-patient relationship was established and therefore, the provider owed the patient a *duty of care*—a duty to provide reasonable care, as appropriate for the situation and the expertise of the provider (e.g., a medical assistant is not held to the same standard as a physician, but would be expected to call a physician into the room if necessary).
2. One or more of the provider's actions or inaction violated (in legal terms, "breached") the duty of care, which means that the provider deviated from the professional standard of care and failed to provide appropriate care to the patient.
3. The provider's breach (the actions falling short of the standard of care) *caused or contributed* to some sort of harm to the patient, like a worsened condition due to improper or missed diagnosis.
4. The patient sustained *damages* (further injury, monetary harm e.g., medical costs, etc.) because of the provider's breach.

health center's social media presence should include disclaimers that comments do not constitute medical advice and that patients should call with questions or to make appointments (or for emergencies, call 911).

If patients routinely post questions publicly that are more appropriate for an exam room, the health center may want to increase moderation of these pages or accounts and consider setting up a standard message directing patients to a more appropriate venue for health concerns, as discussed above.

B. Provider's Personal Social Media Accounts

Health care providers' personal use of social media can pose a malpractice risk as well. Any posts published around the same time when the alleged malpractice occurred may

be directly relevant and problematic. An example would be a provider posting a status that (s)he is nervous, but excited, about performing a new procedure the next day.

Even posts that have nothing to do with the facts and circumstances of a malpractice claim (or medicine in general) could be used to paint a provider in a negative light. The more personal information the provider shares, the more posts plaintiff's counsel has to choose from in establishing the provider's character and defining the theme of the case.

C. Strategies to Protect Against Potential Malpractice Claims

- **Do not give medical advice online.** It is best to avoid giving out any clinical advice online so as not to inadvertently establish a provider-patient relationship or engage in the improper practice of medicine. If unsure of whether a post or message could be problematic, use disclaimers to clearly state that the content is not meant as individual medical advice and encourage the recipient(s) to consult their primary care providers or other appropriate medical professional.
- **Redirect patient inquiries.** If a patient posts a clinical question on social media, direct him or her to more appropriate channels like messaging in a secure patient portal or calling the health center. Given the question, it may be most appropriate for the patient to schedule a visit so that a health professional can examine him or her and answer questions in person.
- **Avoid posting about work on social media.** Social media is a prime location for many people to share (and vent) about their experiences in real time. Though it may be tempting to post about a particularly frustrating patient or unique diagnosis, it is best not to do so. Even if it is posted anonymously or the names are changed or the facts are altered slightly, these posts and comments could inadvertently identify patients (leading to a potential HIPAA violation) or could be used against the health center if the health center or its providers are involved in malpractice proceedings.

- **Control who can view providers' profiles and accounts.** Providers should keep personal and professional accounts separate and should use the highest possible security settings on both. It is also a good idea for providers to routinely go through their "friends" or followers to make sure they know with whom they are sharing information. Security settings on social media platforms change from time to time so they may also need to routinely adjust what and with whom they are sharing online.
- **Providers should think before they post.** Everyone should use discretion when posting messages or pictures online; once posted, the information is public, it is linked to the health center or provider's name, and it is more or less permanent. Even if it is deleted, the information is likely to be archived and accessible somewhere. Providers should consider what articles, blog posts, and videos they are commenting on or sharing. If someone tags them in a picture (*i.e.*, identifies them as a person in the photograph, linking their account(s) to the picture), consider "removing the tag" if it is not a picture they would want to post themselves.

If the health center or its providers are involved in a pending malpractice action, there are additional precautions to consider:

- **Do not delete past posts.** If there are posts that may shed a negative light on a certain provider or a particular incident, deleting them can make the situation worse by suggesting that the provider or the organization has something to hide. Further, once a health center reasonably anticipates or becomes aware of litigation, it must implement a "litigation hold" to preserve all forms of information relevant to the litigation, including electronic posts.
- **Do not post about possible, pending, or even closed legal matters on social media.** If a provider is involved in a malpractice action, the mantra should be "anything I post or share can be used against me." Particularly while a claim is pending, the best practice is to assume everyone can see everything the provider posts online so it is important to be especially vigilant.

- **Lock down profile(s).** If providers have not done so already, they should consider enhancing security on their profiles (or, as appropriate, deleting them) for the duration of the proceeding.
- **Do not “friend” or newly connect with anyone connected to the pending case.** This includes the provider’s attorney and their staff, opposing counsel and their staff, the individual who sued the provider, *etc.* While the provider’s attorney will want to see their social media profiles and may ask to see pictures and comments the provider has posted, the provider should not share the provider’s account log in information and password with the provider’s attorney. If the malpractice claim leads to a more formal proceeding (like a trial), the provider should not make any attempt to connect with judges and jurors or even search for them on social media (the latter could result in an accidental invitation or connection).

3. Reputational Harm

There are many online threats to an individual’s and an organization’s reputation. *Internal* threats originate from the organization itself; the reputational damage may be unintentional:

- A quick-tempered staff member posts a disparaging comment about work on a personal Facebook page, which lists the health center as his/her employer;
- An employee mistakenly tweets inappropriately from the corporate account instead of his/her personal account; or
- An employee inadvertently shares an internal communication describing a politically polarizing situation and the email is then widely circulated online.

When threats stem from *external* sources, such as patients, competitors, community members, former employees, or even total strangers, they are more likely to be deliberately harmful:

- A disgruntled former employee intentionally leaks embarrassing information on the health center’s Facebook page;
- A competitor trying to downplay the success of a particular clinician writes fake reviews to hurt the health center’s business;
- So-called “trolls” attack individuals and organizations for fun with the explicit intention of ruining innocent (and not-so-innocent) reputations; or
- Hackers obtain network credentials and seize control of the health center’s social media accounts, going on a rampage against its reputation.

While each of these external sources represent a threat, disgruntled patients likely represent the most likely risk for reputational harm to health centers and their providers.

A. Patient Comments

Patient comments are a category of their own. Whether or not the allegations are true, or are even written by actual patients, negative reviews can color public perception of a health center or a provider. In a perfect world, honest reviews would help patients make informed choices about health care and help health centers improve services. However, the internet is far from perfect: online reviews are rarely verified and feedback may not be reflective of the community served as a whole. Like many businesses, health centers and their providers are struggling with the increasing consequences of online patient reviews and complaints, both formally on traditional review sites and informally on social media sites.

Freedom of speech protections extend online: both the speech of the reviewer and the host (*e.g.*, the website) are protected. These protections not only safeguard a reviewer who is posting accurate, but perhaps unpopular, statements or unverifiable opinions, but also a private website removing posts (*i.e.*, the website has the right to *not* be represented by a reviewer’s speech).

This area of law is evolving. For example, in late 2016, Congress passed the Consumer Review Fairness Act, which prohibits “non-disparagement clauses” (provisions that prohibit or punish negative reviews by consumers) from websites’ Terms of Service (the rules by which a user must agree to abide in order to use the website). Although the law confers on consumers the “freedom to Yelp,” it does nothing to ban “strategic lawsuits against public participation,” which censors public speech by invoking the court system to intimidate authors of negative reviews. An example of a strategic lawsuit against public participation would be if a patient posts a negative online review about her last doctor’s visit. Shortly after, the patient receives a letter from the doctor’s attorney threatening legal action unless she removes her negative online review.

Many times, reviews are not even based on whether a provider is objectively “good,” but on tangential issues or interactions: a patient did not like the recommended course of treatment even though it was clinically appropriate or, a patient had a bad experience in the waiting room, which is unrelated to the provider’s competency. On its own website, a health center can moderate content, limiting the impact of negative comments and false information. But reviews posted to third party sites are, for the most part, beyond reach and, in many cases, these reviews exist whether or not a provider or a practice actively sets up a profile.

While there are broad protections for freedom of speech, there are limits, particularly where there is a substantial likelihood of significant harm that outweighs the restriction on individual liberty. Included in such limits are defamation laws that protect individuals, organizations, and even products, from false or unsupported statements resulting in harm to a reputation and/or financial interests. According to Black’s Law Dictionary:

- **Defamation:** the act of harming the reputation of another by making a false statement to a third person; a false written or oral statement that damages another’s reputation.
- **Libel:** a defamatory statement expressed in a *fixed medium*, especially writing, but also a picture, sign, or electronic broadcast.

- **Slander:** a defamatory statement expressed in a *transitory form*, especially speech.

Broadly speaking, in order to prevail on a defamation claim, the health center must prove that a statement was *false* and caused *harm*. Depending on the situation, there may also be requirements to show either a malicious intent to harm another’s reputation or unusual carelessness, such as insufficient research into a statement’s truthfulness. Often, the most difficult part is showing that a statement is factually incorrect. Statements of opinion are typically not defamatory but can nonetheless be harmful.

B. Strategies to Protect Against Reputational Harm

- **Cultivate the health center’s online presence.** The best defense is a good offense: while it can be tempting to disengage, creating an online presence is exactly what health centers should be doing. Take advantage of platforms where the health center can control the message, like the health center’s website and social media accounts, to highlight accomplishments and unique contributions to the community. Fostering a strong online presence with positive, accurate stories can help counteract negative comments to build (or rebuild) a good reputation.
- **Fill out online profiles.** There are dozens, possibly hundreds, of websites that rate providers and practice groups. More often than not, the profiles on these pages are blank, sparsely populated, or factually incorrect. Where possible, edit these profiles and correct false information.
- **Leverage search engine capacity.** There are strategies to influence where health centers and providers appear in search engine results, but sheer volume also helps; an abundance of positive press and activity can push the outlier negative comments down in the search results.

- **Review the Terms of Service.** Nearly every website has a defined set of rules users must follow. These rules have titles like “Terms of Service,” “Community Standards,” and “Posting Guidelines.” Look for pages explaining how to report inappropriate comments and “flag” posts for removal. If the comment or post violates the rules, the moderator should remove it from the website.
- **Escalation.** Some comments may not be technical violations, but it is always worth reporting to the website and essentially “asking for the manager.” For example, perhaps one comment does not rise to the level of a violation, but one particular user repeatedly commenting about the health center or its providers with misleading information suggests a problematic pattern of behavior to be monitored.
- **Obtain a Court Order.** With strong evidence, the health center may be able to obtain a court order declaring certain content defamatory. Generally speaking, websites respond promptly to such requests and, if not, search engines like Google can remove the links from search results so the content is more difficult to find.
- **Pursue a Civil Action.** Health centers can try to bring a civil case in court; however, this is a novel approach and, even if the underlying facts have merit, many websites are reluctant to identify users, making it difficult to sue unless the offender is known.
- **Monitor Accounts.** If patients are complaining online about services, logistics, or a specific provider address these fixable problems.
- **Retain Strong Privacy Settings.** Providers should enable dual authentication, change passwords regularly, and limit the number of people with access to their account(s).

III. Conclusion

Health centers are tasked with finding and maintaining a middle ground between patient expectations of provider accessibility online and the practical risks associated with engaging with patients over social media. To that end, this issue brief offers information on the common pitfalls and risk areas that providers and health centers should be aware of when contemplating how best to strategically move forward with utilizing social media in a manner that enhances the overall patient experience.

The laws governing the various elements of social media use are ever-changing. Health centers and providers should work with their local legal counsel to ensure that they are staying current with applicable requirements and best practices.

Additional Resources

- 1, HIPAA Journal, “HIPAA Compliance Checklist 2017-2018,” (<https://www.hipaajournal.com/hipaa-compliance-checklist/>).
2. HIPAA Journal, “Social Media Rules,” March 12, 2018 (<https://www.hipaajournal.com/hipaa-social-media/>)

Acknowledgements

Molly Evans and L’Kel Little

Feldesman Tucker Leifer Fidell

April Lewis and Marisol Murphy-Ballantyne

National Association of Community Health Centers