FEATURE

My Patient Wants to Friend Me on Facebook!

You sign into Facebook and there it is: the small red circle. **"Who sent me a friend request?"** A small picture next to a name appears as you hover your mouse over the icon, and you realize … **"oh no, my patient wants to friend me."**

BY EMILIE T. PINKHAM, ESQ.

**This is the first article in a four-part series exploring social media and electronic communication challenges for health centers.*

Technology expands our reach both professionally and personally – video conferences connect colleagues on different continents, blog posts are edited in opposite time zones, and family vacation photos are shared across oceans. Although the healthcare industry has often been slower to adopt the latest technology than other industries, many health centers are becoming more comfortable establishing an online presence. This trend is well-timed as patients increasingly expect tech-savvy providers. As each new generation comes of age with increased technological expertise and comfort, the ability to virtually access and connect with healthcare providers will be a foregone conclusion.

In an increasingly connected world– individuals often communicate daily despite never having met IRL (in real life). Not surprisingly, patients, especially younger Millennials who have grown up on social media, may be inclined to reach out to their doctors online. So, what's a health center to do? The answer for many health centers will be to cautiously embrace social media as part of a larger strategy to engage with patients and their communities electronically.

What is Social Media?

Broadly, 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 online. While the scope is ever-expanding, social media 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, ZocDoc) may also be considered social media.

Benefits of Connectivity

For health centers, there are immense benefits to increasing patient engagement through social media. Facebook posts can share information about an upcoming influenza immunization campaign to an entire patient base at once, a tweet can announce the opening of a new facility to an entire community, and a YouTube video could provide patient education around an important health topic. Furthermore, health centers can track and analyze which forms of social media are reaching the most people. A well-constructed social media presence can be an important part of a health center's marketing and patient interaction strategies.

So What's the Problem?

Healthcare providers face a delicate balancing act: a desire to meet patient communication preferences and leverage the benefits of social media coupled with an obligation to keep such communications appropriately documented and secure. Any increased access to protected health information (PHI) comes with a corresponding increase in potential risks and adds to the health center's security burden.

For health centers, common risks associated with social media and electronic communication generally fall into three categories: privacy and security, medical malpractice, and reputation. This first article in the four-part series covers privacy and security risks related to social media use. Future articles will focus on risks related to malpractice liability and professional reputation as well as a closer look at privacy and security issues with other forms of electronic communication (e.g., emailing and texting patients and the use of patient portals).

Social Media Privacy and Security Risks

Privacy and security risks associated with a social media presence should not be understated. 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 you share information with online through a social media site) are able to share that information with a wider audience, with or without your permission. For example, a friend can take a screenshot of your 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 could violate the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which governs the protection and confidential handling of protected health information (PHI).

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 inadvertent, a selfie showing off a new haircut that shows an eight-year-old 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.

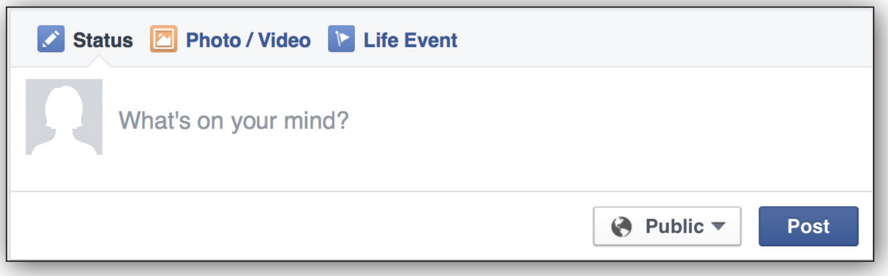
While HIPAA and HITECH (the Health Information Technology for Economic and Clinical Health Act, a law promoting the meaningful use of health information technology) do not directly address the use of social media by a healthcare provider, the posts described in the examples above demonstrate that a health center or its employees could still breach these laws, as well as state privacy laws, by posting information about patients (e.g., comments, photos, video) on social networking websites without the patients' permission. As such, health centers must avoid any unauthorized disclosure of individually identifiable health information in any form on social media.

Of particular importance, 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).

Violations of HIPAA and HITECH can mean large fines for a health center and its employees. In addition, state medical boards may also discipline providers for such behavior with punishments ranging from a simple reprimand to a suspension or revocation of a license.

Strategies to Protect Against Associated Liabilities

Unfortunately, there are no obvious limitations on the use of social media in healthcare and the landscape is quickly evolving, making best practices a moving target and leaving health centers with more questions than answers. Given all the uncertainties related to social media, what practical steps can a health center take to protect against the risks described above and any associated liability?



- Conduct a social media risk analysis to understand how health center staff engage with patients online and learn more about how patients wish to connect with staff.
- 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.
    - 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).
- 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.
- 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 you want to share a patient's story or picture in connection with the health center on social media, be sure to obtain patient authorization first.

- Steer patients away from social media and toward secure methods of communication for discussions about their healthcare. Ensure that any patient portals or other direct electronic communications with patients (patient portals, email, text, instant messaging) are appropriately secure and encrypted – more on this advice in a future article.
- 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.

What's Next?

Digital interaction through social media is not fading from the healthcare landscape. Quite the opposite – as technology improves, the demand for quick, virtual interaction will continue to grow and yet-to-be-developed media will present new challenges to healthcare providers. Technology continues to become more accessible and widely available. Seemingly every day, there are new ways to share information and the type of devices on which to share it continues to expand.

Health centers need to find middle ground between patient expectations of provider accessibility online and the practical risks associated with engaging with patients over social media. This includes the establishment of clear policies and operational procedures for staff, together with a Patient Notice of Privacy Practices, aligned with the standards outlined in HIPAA, HITECH, and state privacy and security requirements to limit a health center's exposure.

But remember, it's not all bad. Social media presents health centers with many opportunities to broaden their reach by engaging with patients and entire communities in a more personal way.

Author's note: We want to hear from you! Do you have a social media "close call," blunder, or success story you would be willing to share? We're looking for real world examples of technology pitfalls, challenging situations, and social media accomplishments related to health centers and providers connecting with patients online (or through electronic means like texting or emailing patients). If we include your story in a future article, all identifiable information will, of course, be removed! ◆

Emilie Pinkham is an Associate at Feldesman Tucker Leifer Fidell LLP. For more information, contact Emilie at: epinkham@ftlf.com.