Don't Post That! Protecting Patient Privacy in the Age of Social Media

Spencer Hamer, JD, and Chloe Ghoogassian, Esq.

Urgent message: Using social media platforms helps your community get to know your urgent care center. But be sure that you protect your patients' privacy when doing so.

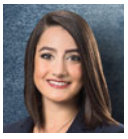
Introduction

Social media has great utility for urgent care centers, providing invaluable opportunities to connect with the local community and offering a host of educational tools for providers and patients. The explosion of myriad social media platforms, however, has created a variety of new channels for exposure of confidential patient medical information, resulting in traps for the unwary. Predictably, the rising use of social media in the health-care environment has led to lawsuits and regulatory scrutiny. Urgent care operators must understand the unique health-care-related legal risks posed by social media and develop an action plan for mitigating these risks.

The Expansive Reach of HIPAA

The U.S. Health Insurance Portability and Accountability Act (HIPAA) regulates use and disclosure of protected health information (PHI). PHI is defined under HIPAA as "individually identifiable health information transmitted or maintained in any form or medium, whether in electronic or other form." HIPAA, as modified by the Health Information Technology for Economic and Clinical Health (HITECH) Act, governs the use and disclosure of PHI by health-care providers, including urgent care centers. State laws also prohibit such disclosures.

HIPAA authorizes heavy fines and potential criminal charges for the unlawful disclosure—whether orally, on paper, or electronically—of PHI. To comply with HIPAA's Privacy Rule, information concerning patients must be "de-identified": All personal identifying information and any revealing references must be removed. Inadvertent breaches of the rule can result in corrective action, hefty fines, and investigations by the U.S. Department of Health and Human Services (HHS). In addition, HIPAA breaches can result in reputational damage and loss of business.



Spencer Hamer, JD, is a partner working in the Irvine, California office of the law firm of Michelman & Robinson, specializing in labor and employment matters for health-care clients. **Chloe Ghoogassian, Esq.,** is a health-care attorney in Los Angeles, California.

Social Media and Patient Privacy

Use of social media potentially violates HIPAA when posts, blogs, tweets, photos, videos, or other information concerning a patient is posted to a social networking site. Even a well-intentioned provider can be responsible for a violation, by using ineffective safeguards against disclosing PHI. Even a single unauthorized PHI disclosure may be sufficient to generate an HHS investigation.

For example, in 2013, an administrative employee at a university medical center accessed, took a screenshot of, and posted a patient's medical records to a Facebook group, mocking the woman's diagnosis. The story went viral, and the hospital suffered substantial reputational harm. Ultimately, a private lawsuit brought by the patient was dropped, and the hospital avoided civil liability, after the judge determined that the employee's actions were outside the scope of her employment as defined by the hospital's social media policy.

HIPAA violations can also occur when health-care providers attempt to share success stories. In a well-publicized case, a nursing student took a picture of a 3-year-old patient who had cancer and posted it on her personal Facebook page, with a caption praising the young boy's bravery. Despite her admirable intentions, the post was a HIPAA violation, and the student was expelled from nursing school for unauthorized disclosure of PHI—the patient's face and his diagnosis.

Problems can also arise when conflict occurs between patients and providers. In one case, a nursing assistant used Snapchat to record and share a video of a partially undressed nursing-home resident who was "giving [the nursing assistant]

a hard time getting changed." Another Snapchat user reported the video to her employer; the nursing assistant was fired, and criminal charges were filed against her.

Negative patient reviews are another common source of violations. For example, a California dentist accused by a patient of misdiagnosis in a one-star Yelp! rating responded to the review by defending his diagnosis, but he disclosed PHI in the process. The patient reported him to HHS, which warned the dentist that responses to negative reviews must not disclose PHI. Even if a patient publicly discloses her PHI, a provider can violate HIPAA by referring to the information in response to the initial disclosure.

Urgent Care Best Practices

In the rapidly expanding and competitive urgent care industry, establishing a brand and engaging the community are critical to success, and social media is an integral part of this strategy. Employees in new and expanding centers, however, are often hired without being fully apprised of the legal risks presented by social media, while also being tasked with using social media to promote the center and connect with the local community. Given the speed with which a single social media post can transform into a potential HIPAA violation, centers must develop and implement a strategy to protect PHI from inadvertent disclosure.

Hiring

Ask potential hires about their experience in handling PHI. If they have minimal to none, that may not exclude them from being hired, but you will at least know the level of experience you are dealing with and can tailor the amount of training accordingly. Employees with substantial knowledge of PHI may be able to separate themselves from other candidates. Talk about social media use in the center, and gauge the level of familiarity the applicant has with PHI protocol. Develop hypothetical questions related to PHI disclosure through social media, and see whether the applicant can spot the issues.

Training

Training on PHI, including a review of how the center uses social media, and how inappropriate use of social media can result in HIPAA violations, should begin in the orientation process. For example, employees should know the identifiers specified by the HIPAA regulations that can result in a violation. They should be informed that seemingly private communications can illegally disclose PHI, and they should be provided with examples of how PHI breaches can occur on social media. In addition, employees who interact with the public on social media should be given specific instructions on how to use various platforms. For example, they should be advised that responses to negative reviews must not contain PHI. The center's social media policy should also be reviewed for compliance with the growing body of state and federal laws, including recent decisions of the National Labor Relations Board, regarding employee rights related to social media in the workplace.

"Use of social media potentially violates HIPAA when posts, blogs, tweets, photos, videos, or other information concerning a patient is posted to a social networking site."

Employees should not be given access to any of the center's social media passwords until training has been completed and documented. Employees should receive regular follow-up training on HIPAA requirements, with social media remaining a key area of focus.

Written Policies

In conjunction with their HIPAA training, all employees should receive written policies on the use of social media, both in the employee handbook and as stand-alone documents. These policies should be saved in the employees' personnel files.

Monitoring

A well-trained employee should be designated to regularly monitor social media sites used by the center, and to review and respond to information posted about the center on the internet. Work with your information technology department to set up procedures that will maximize your ability to monitor all relevant posts.

Employee Feedback

Bring your employees into the conversation about best practices. Make social media a regular topic in meetings, review breaches that are reported in the news, and survey employees for their opinions on how to prevent breaches.

Terminations

When employees leave the center, a review must be immediately conducted to determine whether they had access to social media passwords. Your information technology department should ensure that former employees can no longer post anything on the center's social media platforms.

Conclusion

Though the world of social media presents substantial risk regarding PHI, the good news is that with careful preparation and consistent practices, urgent care centers can proactively manage this risk. ■