

Safety and Security Issues with the Use of Social Media¹

Social media impacts us personally and professionally on a daily basis. Most of us could not have envisioned the effect that social media has had upon us within the healthcare sector, including the field of psychiatry. In the coming years, social media use will only increase, potentially causing risk management and legal concerns within your practice. Although there is minimal caselaw of statutory regulations nationally concerning social media, it is anticipated that legal challenges will arise.

There are a multitude of issues when using social media including boundary issues, ethical issues, confidentiality issues, standard of care issues, and privacy issues. This column will address specifically safety and security of patient information with respect to the use of social media.

Social media refers to the use of web-based and mobile technologies to turn communications into an interactive dialog.² Social media is used to connect individuals with each other in an online format. It can take on a variety of forms including electronic mail, *Facebook*, *MySpace*, *Google+*, *LinkedIn*, *Twitter*, *YouTube*, *Skype*, *Foursquare*, blogs and on-line dating sites. The use of social media spans across all ages and all professions, including psychiatry.

A critical issue when accessing or using a social media site when communicating with and about patients, is the degree of privacy and security available within that medium. As you all know, patients are entitled to confidentiality and whichever form of social media outlet you use, it remains of the utmost importance.

The use of social media could potentially expose you to liability under HIPAA privacy laws. Consider if one of your office staff breaches HIPAA when posting information online concerning a patient. For example, your office assistant dealt with a difficult patient and later that day posts on Facebook about his/her interaction with the patient. Although you may not have interacted with the patient directly, may not have been in the office at the time and may not have observed the interaction, this posting could expose you to liability. Not only could a post like this result in a breach of privacy under HIPAA, the Federal Trade Commission could impose liability (FTC may impose liability upon businesses for statements made by their employees on social networking sites even if the company itself had no actual knowledge).³

There are a number of ways privacy could be breached by the use of social media. One such way is with the use of *Skype*. Since the inception of *Skype's* video conferencing in 2006, it is becoming more widely used in healthcare, including within the behavioral health sector.⁴ If using *Skype* in treatment of patients, there are certainly a variety of risk management and legal issues concerning safety and security. First, how are you visualizing the patient and what safety precautions do you have in place in the event that something adverse were to occur? Further, how do you know that it is a secure connection? *Skype* claims to be secure and encrypted; however, it is impossible to verify

that the algorithms are used correctly, completely and at all times. *Skype* has been found to have a number of security issues.⁵

Security issues can also occur with use of other forms of social media, including use of *Facebook* and email. One case involves a Rhode Island physician who was reprimanded by the state licensing board and her privileges were revoked due to posting information online. The physician did not include the patient's name; however, sufficient information was conveyed such that others within the community would be able to identify the patient.⁶ Another case from California involves patient communication with a therapist through a work email account. The California Appeals Court found that the patient's communication with her therapist may lose protection under patient-therapist privilege when there is a transmission from a workplace device.⁷ These cases involve very distinct and separate issues with different forms of social media but are examples of how issues may arise when engaging in online communication.

While this column touches upon some safety and security issues when using social media, it does not constitute an exhaustive list of issues to consider. Social media is a moving target that evolves with every click, post and blog. Engaging in the use of social media should not be entered into lightly and its impact on psychiatry is wide-reaching.

Author Profile: Kristen Lambert, JD, MSW, LICSW is the Vice President of Healthcare Risk Management for AWAC Services, a Member Company of Allied World. She leads risk management services for psychiatrists who are Allied World policy holders and has a background in litigation and clinical social work.

End Notes

1 This information is not intended to be and should not be used as a substitute for legal advice. Rather it is intended to provide general risk management information only. Legal advice should be obtained from qualified counsel to address specific facts and circumstances and to ensure compliance with applicable laws and standards of care.

2 http://en.wikipedia.org/wiki/Social_media. Social Media. September 21, 2011.

3 Overly, Michael, CSO: Security and Risk. Businesses May be Liable for Employee Statements on Social Networking Sites, says new FTC Guidelines
http://blogs.csoonline.com/businesses_may_be_liable_for_employee_statements_on_social_networking_sites_says_new_ftc_guidelines

4 Hoffman, Jan. "When Your Therapist is Only a Click Away." The New York Times. September 23, 2011.

5 <http://en.wikipedia.org/wiki/Skype>. Skype. September 27, 2011.

6 Conaboy, Chelsea. For doctors, social media a tricky case.

http://boston.com/lifestyle/health/articles/2011/04/20/for_doctors_social_media_a_tricky_case. April 20, 2011.

7 Holmes v. Petrovich Development Co., LLC, 191 Cal.App. 4th 1047 (2011).