You Saw What, Where, About Whom? Improper Use and Disclosures of Protected Health Information Through Social Media

Patrick D. Souter
Gray Reed & McGraw PC
Dallas, TX

The use of social networking applications to exchange personal and professional information has become commonplace today. While many believe that societal acceptance lies primarily with high school- and college-age groups, in reality, all ages have embraced this technology as a way to interact with others on a regular basis. Social networking applications, or "social media," provide immediate transmissions of text, documents, or data that result in an element of convenience that traditional communications do not provide. However, the attractiveness of this convenience comes with a significant price. Familiarity and acceptance result in the failure to recognize that social media is not a secure method of communication. As we move away from the traditional ways of sharing information, the social media user's recognition of what is and what is not acceptable for publication may become blurred. This failure to recognize that certain information is confidential, private, or otherwise restricted from publication may result in its improper dissemination. This issue is especially important when attempting to comply with the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, and other federal and state laws, rules, and regulations that govern confidentiality, privacy, and security.

Social Media

The term "social media" encompasses an array of sites and services, each with a different niche purpose. The term is defined as "forms of electronic communication (as Websites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (as videos)."[1] Generally, there are six types of recognized social media: social networks, bookmarking sites, social news, media sharing, microblogging, and blog comments and forums.[2] Common social media portals include Facebook, Twitter, Instagram, LinkedIn, Tumblr, and YouTube.[3] Through these sites, the user may comment on different matters, post audio and video content, share information from other users, and otherwise communicate with an array of individuals and entities that wish to receive such information.

How Health Care Providers Commonly Use Social Media

With the growth of social media as an acceptable method of communication, health care providers have witnessed an increasing use of social media in the following areas:[4]

- Allowing for conversation and interaction between providers and patients in an individual or group format;
- Marketing of health care services, offering general health information and data creation to determine performance levels;
- Determining website-driven metrics related to the aforementioned marketing efforts;
- Engaging "e-patients," defined as patients who are significantly engaged in electronic technology in everyday life;
- Promoting wellness initiatives, such as health information and dietary and exercise content;
- Professional collaboration to allow for communication between health care providers;
- Consumer, patient, and professional education, such as social media platforms, applications, and mechanisms, that allow for ease in communication with individuals and entities;
- Clinical trial recruitment by health care providers and research organizations; and
- Workforce recruitment through professional networking platforms such as LinkedIn.

In each of these areas, there may be possible exposure of Protected Health Information[5] (PHI) regarding a patient or the patient's health care.

Concerns for Health Care Providers Related to Social Media

Health care providers and those who store, process, use, or otherwise maintain PHI have specific responsibilities when dealing with PHI due to the providers' position and relationship with patients and patients' records.[6] As previously mentioned, social media has become so commonplace that health care providers must be cognizant of what is posted, and where and how the information was obtained. Social media postings commonly occur on networks or other types of electronic communities, resulting in mass disclosure and significant damages due to the number of individuals who have access to the post. Medical boards are becoming more diligent in investigating information and images that health care providers have posted on social media that may be considered unprofessional conduct.[7] These include inappropriate actions such as posting patients' photos without permission, providing false or misleading information on clinical trials, posting inaccurate information regarding a health care provider's qualifications, or using social media to contact patients through inappropriate means.[8]

In numerous recent instances, providers and employees of providers have utilized personal social media portals to post inappropriate information or images that may result in liability. These instances include the following:

- A paramedic who treated a sexual assault victim posted information about the assault on his MySpace page. While the paramedic did not disclose the victim's identity, sufficient information was disclosed to allow for the patient's identification;[9]
- An Emergency Department (ED) physician in Rhode Island was fired, hospital privileges revoked, and reprimanded by the Rhode Island Board of Licensure and Discipline for posting personal information about a patient on the physician's Facebook page. The physician did not disclose the patient's identity, but sufficient information could be obtained from the posting to identify the patient through the nature of the patient's injury;[10]
- A hospital employee working as an ED technician recently was discovered to allegedly have posted comments on her Twitter account regarding patients and their PHI, such as specifics regarding their medical care and X-rays; and[11]
- The nurses of a Fargo, ND-based health care facility provided each other shift-change information via the nurses' personal Facebook accounts so they could prepare for their upcoming shift. While they did not use specific patient names, sufficient information was provided that allowed for discovery of the patient's identity.[12]

In addition to the risks of disclosing PHI, general commentary on blogs or personal social media sites regarding a patient or a facility may not necessarily be illegal, but may cast a negative light on providers. A St. Louis OB-GYN posted her frustration with a patient on her personal Facebook account without identifying the patient's name or sufficient facts to identify the patient. Other providers responded how they would have dealt with the patient in less-than-flattering terms. These comments were then redistributed across social media and caused a wave of negative press.[13]

How a Health Care Provider Can Address Social Media Concerns

A health care provider must be proactive in addressing the concerns created by social media use. While creating a social media policy is a good first step, it is just that—a first step. The policy must provide the framework for social media use. Education and training on the social media policy and on the laws, rules, and regulations related to the use of such mediums and information must be established. The health care provider also must establish risk-mitigation strategies that require constant review, testing, and corrective actions related to social media. As previously noted, health care providers may be subject to board action, in addition to liability related to HIPAA and associated concerns, due to social media usage that may be considered unprofessional conduct. To assist providers with this issue, the Federation of State Medical Boards has published guidance on policy guidelines and appropriate social media use.[14] In addition, the Healthcare Information and Management Systems Society has published privacy and security considerations including sample policies as well as privacy and security considerations for health care providers.[15]

The social media policy itself must address dual aspects of disclosure where a health care provider may encounter social media issues. First, the health care provider may utilize approved content through an official social media portal recognizing the restrictions imposed by law on such disclosures. A social media policy must set forth the individuals who have the authority to approve the content and where the content is posted. An example may be posting information or responding to a patient question on a social media portal. It is imperative that the information disclosed not reveal any information that is to be maintained in a private and secure setting. Second, the health care provider may have to address the unauthorized posting of PHI at the workplace or outside of the workplace on the employee's personal time. In those instances, the individual, while arguably a representative of the health care provider, generally does not have the authority to post the information. The social media policy should prohibit unauthorized individuals from posting any information regarding health care providers no matter if through the provider's social media portal or the individual's portal. The reasoning behind this restriction is that those comments are based on information obtained in the individual's capacity as an employee. An employee commenting on a post, even if created by the patient, may still result in an inappropriate disclosure that leads to liability.

Employee education and training on social media policies is imperative to safeguard against improper disclosures. Many providers believe that HIPAA training is sufficient to provide the appropriate baseline guidance, but this training falls short of what is needed to address all social media concerns. While HIPAA training focuses on security and privacy standards, social media training also should address issues such as confidentiality, restrictions on what is said and the method the message is conveyed, and the particular standards related to social media sites. A health care provider also should ensure that information presented is not considered to create a physician-patient relationship or be construed as providing medical advice in an inappropriate format.

Finally, risk mitigation should be considered mandatory when utilizing social media. "Risk mitigation" may be described "as the systematic reduction in the extent of exposure to a risk and/or the likelihood of its occurrence."[16] Risk mitigation is not only creating a social media policy and providing appropriate training. It also is a series of checks and balances to ensure that inappropriate material has not been made available to the public by efforts of the health care provider as well as ensuring that third parties have not

been able to improperly access such information. Risk mitigation provides for additional compliance initiatives to not only ensure that improper disclosures have been minimized but also that other legal and regulatory issues have been addressed. These additional risks include HIPAA, HITECH Act, intellectual property, copyright and trademark infringement, and the inappropriate use of a person's likeness. Risk mitigation techniques include the following:[17]

- Performing a risk assessment on social media uses to determine prevalent risks. Such risk assessment should include input from health care providers' employees and contractors as well as third-party vendors that may have access or otherwise participate in social media activities;
- Developing an all-encompassing risk-based social media strategy in conjunction with social media policy development. The policy and strategy should work together in establishing goals and objectives for the provider's utilization of social media; and
- Defining what type of online reputation and brand the health care provider wishes to convey and then developing a strategy to monitor it. This allows for simultaneous review of social media content to ensure that inappropriate uses of social media have not occurred while ensuring that the message conveyed is consistent with the provider's desired reputation and branding.

The health care provider must be prepared and execute on any issues that arise through the risk-assessment process. By not doing so, the provider not only opens itself up to liability but also sends the message to stakeholders in the risk-assessment process, such as employees and patients, that it does not intend to follow its social media policy or ensure low risk in utilizing social media. Failure to follow standard operating procedures is the equivalent of not having any procedures at all.

Conclusion

Social media has become entrenched in society and is universally accepted as part of everyday life. However, such customary use may cause a user to oftentimes forget what laws, rules, and regulations may apply to a particular area of communication. Health care communications involving PHI is an area that creates traps that may result in substantial penalties. The creation of a social media policy is only the first step in the process of ensuring compliance. Employee training and risk assessment with appropriate standard operating procedures for compliance are mandatory in addressing social media usage. In numerous cases, not only have rogue employees posted something inappropriate but health care providers themselves have violated confidentiality, privacy, security, and other legal requirements faced by all industries, not just those in health care. The continued diligence in monitoring and responding to social media usage should be on the same level as other areas of compliance.

Practice Groups Staff

Trinita Robinson
Vice President of Practice Groups
(202) 833-6943
trobinson@healthlawyers.org

Magdalena Wencel
Senior Manager of Practice Groups
(202) 833-0769
mwencel@healthlawyers.org

K.J. Forest
Senior Manager, Practice Groups Distance Learning
(202) 833-0782
kforest@healthlawyers.org

Brian Davis
Senior Manager, Practice Groups
Communications and Publications
(202) 833-6951
bdavis@healthlawyers.org

Arnaud Gelb
Practice Groups Distance Learning Administrator
(202) 833-0761
agelb@healthlawyers.org

Crystal Taylor
Practice Groups Activities Coordinator
(202) 833-0763
ctaylor@healthlawyers.org

Dominique Sawyer
Practice Groups Distance Learning Certification Coordinator
(202) 833-0765
dsawyer@healthlawyers.org

Matthew Ausloos
Practice Groups Communications and Publications Coordinator
(202) 833-6952
mausloos@healthlawyers.org

Jasmine Santana
Practice Groups Editorial Assistant
(202) 833-6955
jsantana@healthlawyers.org

Graphic Design Staff

Mary Boutsikaris
Creative Director
(202) 833-0764
mboutsik@healthlawyers.org

Ana Tobin
Graphic Designer/Coordinator
(202) 833-0781
atobin@healthlawyers.org

1 Merriam-Webster Dictionary, *available at* www.merriam-webster.com/dictionary/social%20media.
2 Grahl, T., *The 6 Types of Social Media*, Out:think Author Marketing, *available at* www.outthinkgroup.com/tips/the-6-types-of-social-media.
3 These social media portals may allow for multiple types of social media platforms.
4 Healthcare Information and Management Systems Society Privacy and Security Committee, Social Media in Healthcare: Privacy and Security Considerations, at pp. 3-4, *available at* http://himss.files.cms-plus.com/HIMSSorg/Content/files/Social_Media_Healthcare_WP_Final.pdf. (Hereinafter, HIMSS, Social Media in Healthcare).
5 45 C.F.R. § 160.103
6 Perkins, N.L. and Theis, A.R., *HIPAA and Social Networking Sites: A Legal Minefield for Employers*, AAOE Executive Update, Jan. 2011, *available at* www.aao.org/yo/newsletter/201201/article02.cfm. (Hereinafter, Perkins and Theis, *HIPAA and Social Networking Sites*).
7 Adams, D., *Medical boards keep a wary eye on doctors' social media posts*, amednews.com, Jan. 28, 2013, *available at* www.amednews.com/article/20130128/profession/130129957/7/.
8 *Id.*
9 Perkins and Theis, *HIPAA and Social Networking Sites*, *supra* note 6.
10 Harris, S.M., *How to Avoid Data Breaches, HIPAA Violations When Posting Patients' Protected Health Information Online*, The Hospitalist, June 2014, *available at* www.the-hospitalist.org/article/how-to-avoid-data-breaches-hipaa-violations-when-posting-patients-protected-health-information-online/2/. (Hereinafter, Harris, *How to Avoid*).
11 Murray, R., *Police Chief's Daughter Fired From Hospital After Tweets Go Viral*, Good Morning America, Sept. 25, 2014, *available at* http://abcnews.go.com/US/police-chiefs-daughter-fired-hospital-tweets-viral/story?id=25758122.
12 Dimick, C., *Privacy Policies for Social Media*, Journal of AHIMA, Jan. 6, 2010, *available at* http://journal.ahima.org/2010/01/06/social-media-policies/.
13 Harris, *How to Avoid*, *supra* note10.
14 Federation of State Med. Bds., Model Policy Guidelines for the Appropriate Use of Social Media and Social Networking in Medical Practice, *available at* www.fsmb.org/Media/Default/PDF/FSMB/Advocacy/pub-social-media-guidelines.pdf.
15 HIMSS, Social Media in Healthcare, *supra* note 4, at 21-27.
16 *Id.* at 13.
17 *Id.* at 15-18.

Physician Organizations Practice Group Leadership

Julie E. Kass, Chair
OberlKaler
Baltimore, MD
(410) 347-7314
jekass@ober.com

Nancy P. Gillette, Vice Chair – Publications
Ohio State Medical Association
Hilliard, OH
(614) 527-6767
gillette@osma.org

Rick L Hindmand, Vice Chair – Educational Programs
McDonald Hopkins LLC
Chicago, IL
(312) 642-2203
rhindmand@mcdonaldhopkins.com

Alyson M. Leone, Vice Chair – Membership
Wilentz Goldman & Spitzer PA
Woodbridge, NJ
(732) 726-7474
aleone@wilentz.com

David T. Lewis, Vice Chair – Strategic Activities
Miller & Martin PLLC
Nashville, TN
(615) 744-8605
dlewis@millermartin.com

Daniel F. Shay, Vice Chair – Research and Website
Alice G. Gosfield & Associates PC
Philadelphia, PA
(215) 735-2384
dshay@gosfield.com

Ashley Thomas, Social Media Coordinator
Presence Health
Chicago, IL
(816) 582-3303
ashley.thomas@presencehealth.org