Guidelines for Ethical and Professional Use of Social Media in a Hand Surgery Practice

Scott D. Lifchez, MD, Desirae M. McKee, MD, Raymond B. Raven III, MD, Adam B. Shafritz, MD, Jonathan L. Tueting, MD

In growing numbers, patients are using social media platforms as resources to obtain health information and report their experiences in the health care setting. More physicians are making use of these platforms as a means to reach prospective and existing patients, to share information with each other, and to educate the public. In this ever-expanding online dialogue, questions have arisen regarding appropriate conduct of the physician during these interactions. The purpose of this article is to review the laws that govern online communication as they pertain to physician presence in this forum and to discuss appropriate ethical and professional behavior in this setting.

Key words Social media, online, heathcare, blog, physician Web presence.

An ever-increasing number of Americans are obtaining health information via the Internet. Frequently, this information comes from social media outlets, interactive Web sites where the users can obtain information and also post information about health conditions. Rozental et al[1] reported that nearly 40% of surveyed patients in their practice use social media sites regularly. These patients tended to be younger, to have higher levels of education, and to own computers.

Many providers now have a presence in one or more social media outlets. Such outlets can be used to post practice information that may be of interest to patients, to be contacted by patients or prospective patients, and to provide general medical information from a reliable source. Franko[2] reported that there are over 400 orthopedic profiles just on Twitter.

In this review, we discuss the federal privacy and communications laws as they apply to a physician's use of social media. We review the existing guidelines from state and professional medical organizations regarding appropriate behavior online. Finally, we present concepts regarding professional online physician conduct when interacting with patients and other physicians.

From the Department of Plastic Surgery, Johns Hopkins Bayview Medical Center, Baltimore, MD; Department of Orthopedic Surgery, Texas Tech University, Lubbock, TX; Orthopaedic Surgery Specialists, Burbank, CA; Department of Orthopaedics & Rehabilitation, University of Vermont, Burlington, VT; and Department of Orthopedics and Rehabilitation, University of Wisconsin, Madison, WI.

Received for publication August 18, 2012; accepted October 5, 2012.

This article was written as part of an initiative of the Ethics and Professionalism Committee of the American Society for Surgery of the Hand by the ASSH Social Media Task Force.

No benefits in any form have been received or will be received related directly or indirectly to the subject of this article.

Corresponding author: Scott D. Lifchez, MD, Department of Plastic Surgery, Johns Hopkins Bayview Medical Center, 4940 Eastern Avenue, Room A520, Baltimore, MD 21224; e-mail: Slifche1@jhmi.edu.

0363-5023/12/37A12-0038$36.00/0
http://dx.doi.org/10.1016/j.jhsa.2012.10.002

LEGAL CONSIDERATIONS

Several federal statutes govern transmission of patient information and communication of all forms over the Internet and other broadcast media. The Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health (HITECH), and Communications Decency Act (CDA) statutes all have content within them relevant to use of social media in a physician's practice.

Health Insurance Portability and Accountability Act

The HIPAA of 1996[3] addressed 2 major issues with respect to patients' health care. Specific provisions addressed a patient's right to retain access to information despite changing jobs. Other provisions addressed a patient's right to confidentiality with respect to health information. The law introduced the term *protected health information* (PHI) and set forth rules as to how this information must be protected. HIPAA is enforced

TABLE 1. Safe Harbor Standard for De-identification of Patient Information

All of the following information must be removed:

1. Names
2. All geographical subdivisions smaller than a state
3. All elements of dates (except year) for dates directly related to the individual
4. Telephone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social Security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints
17. Full-face photographic images and any comparable images, and any other unique identifying number, characteristic, or code, except as permitted for re-identification purposes provided certain conditions are met. In addition to the removal of the above-stated identifiers, the covered entity may not have actual knowledge that the remaining information could be used alone or in combination with any other information to identify an individual who is subject of the information.

Adapted from the Office for Civil Rights. Summary of the HIPAA privacy rule. Available at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf. Accessed August 17, 2012.

by the Office of Civil Rights (OCR) within the Department of Health and Human Services (DHHS).

A doctor or health care practice can use PHI for the purposes of providing care to a patient and conducting business relevant to that patient's care (eg, billing an insurance carrier). Using this information as part of the doctor's Facebook page or other social media outlet without the patient's consent is prohibited by this law.

There are 2 ways to include patient information in a social media outlet that are acceptable within HIPAA. A patient may sign a consent form allowing the doctor to include the patient's PHI in a social media outlet. Alternatively, the information can be "de-identified" and then would be acceptable for use.

The "safe harbor" method is the most thorough way to ensure that all identifying information has been removed (Table 1). For the purposes of hand surgeons, x-rays scrubbed for identifying information can meet the safe harbor criteria. Photographs, even of hands, can potentially be problematic if there are sufficiently identifying marks on the hand (such as tattoos).

TABLE 2. New Penalties for HIPAA Violations Under HITECH

1. Up to $100 per violation in which the person did not know and could not have known with due diligence that he or she was committing a HIPAA violation, up to $25,000 per year
2. Up to $1000 per violation in which the person did not known but could have known with due diligence that he or she was committing a violation, up to $100,000 per year
3. Up to $10,000 per violation in which the violation was caused by willful neglect, up to $250,000 per year
4. Recurrent violation due to failure to correct or address violations above can result in $50,000 for each violation, up to $1,500,000 per year

Adapted from Federal Register. Rules and regulations. Vol. 74, No. 209. Friday, October 30, 2009. Available at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/enfifr.pdf. Accessed August 16, 2012.

Health Information Technology for Economic and Clinical Health Act

The HITECH Act[4] is part of the American Recovery and Reinvestment Act of 2009. HITECH primarily addresses security and privacy concerns related to the electronic transmission of health information.

The HITECH Act also included provisions regarding the enforcement of HIPAA (Table 2). The law specifically states that collections of fines from enforcement of HIPAA violations will become a part of the OCR's budget. All of this has led to a more proactive enforcement of HIPAA. OCR does not need to wait for a complaint to be filed; it can investigate without cause and apply penalties for any violations it encounters. An occurrence can be defined as each e-mail, transmitted document, or other release of PHI. As such, a hospital or even a practice can incur the maximum penalty per year very quickly. For the most egregious offenses, recurrent violations can be fined up to $1.5 million per year.

The Communications Decency Act

Where HIPAA protects patient information, the CDA regulates content transmitted via Internet, whether or not it involves a specific patient's information. CDA was introduced as Title V of the Telecommunications Act of 1996 as an attempt to regulate obscenity in cyberspace.