LEGAL BRIEFS

Amy L. Hader, JD
Evan D. Brown, JD

Patient Privacy and Social Media

Healthcare providers using social media must remain mindful of professional boundaries and patients' privacy rights. Facebook and other online postings must comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), applicable facility policy, state law, and AANA's Code of Ethics.

Keywords: Confidentiality, Facebook, Health Insurance Portability and Accountability Act of 1996 (HIPAA), Internet, privacy.

Exponential growth in our society's use of social networking platforms and applications presents ongoing privacy and liability concerns for healthcare providers and facilities alike. Social media sites such as Facebook offer users the ability to connect electronically with friends and colleagues all over the world. Facebook alone has more than 400 million active users.[1] The number of Facebook users over the age of 35 doubled in 2007 from the previous year.[2]

Healthcare providers using social media must remain mindful of professional boundaries and their patients' privacy rights. Talking with your friends or spouse about work is not necessarily an invasion of your patients' privacy, but when patient-identifying information is discussed, breaches of confidentiality may occur (Figure). Posting work-related information online presents additional challenges and heightens the risk of confidentiality breaches and allegations of unprofessional conduct.

CRNAs using Facebook and other social media must be careful and ensure that all postings and information sharing complies with the Health Insurance Portability and Accountability Act of 1996 (HIPAA),[3] applicable facility policies, state common law and regulatory protections for patient confidentiality, and the AANA's Code of Ethics. Confidentiality breaches and other errors in judgment by practitioners using social media can result in civil liability to patients, job loss, disciplinary action by state licensing boards, and even criminal investigations and sanctions.

HIPAA and the Privacy Rule

HIPAA's Privacy Rule addresses the use and disclosure of patients' protected health information and establishes ground floor privacy protections for certain health information.[4] The Privacy Rule applies to health plans, healthcare clearinghouses, and to any healthcare provider who electronically transmits health information in connection with certain transactions, including both institutional providers (eg, hospitals) and individ-

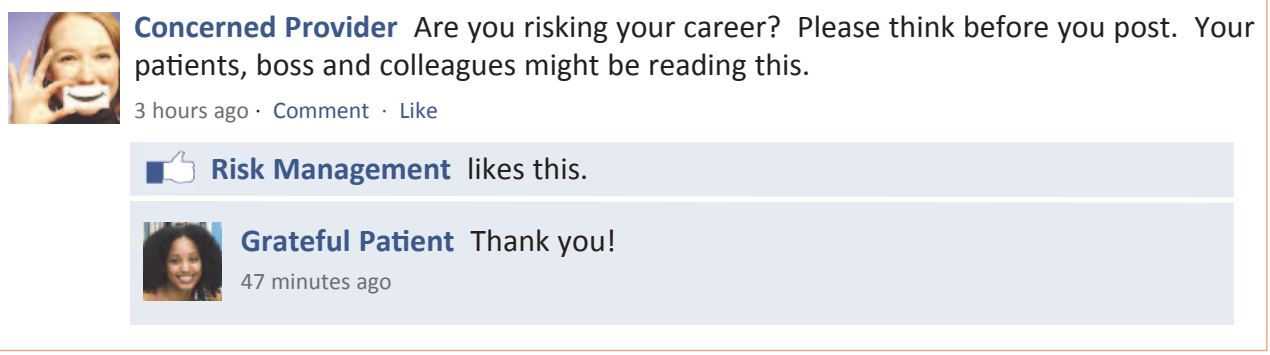

Figure. Facebook Post

ual practitioners such as physicians, dentists, CRNAs, and other practitioners who furnish, bill, or receive payment for healthcare. Healthcare plans, clearinghouses, and providers covered by HIPAA are called "covered entities" in the rule. The Privacy Rule standards also extend to "business associates" who perform certain functions or activities on behalf of or for a covered entity.[5]

The Privacy Rule protects all individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper or oral. Individually identifiable health information is information that relates to the individual's past, present, or future physical or mental health or condition, the provision of healthcare to that individual, or the payment for the provision of healthcare to the individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual.[6] This includes information in the medical record; conversations between practitioners, nurses and other providers; information in health insurers' computer systems; and billing information held by facilities. Such information is referred to as "protected health information" or "PHI" in the Privacy Rule and in practice. PHI includes many common identifiers such as name, address, birth date, social security number, and full face or comparable images and other unique identifying characteristics that could reasonably be used to identify an individual.[6,7]

The Privacy Rule requires covered entities to guard against misuse of individuals' identifiable health information and limit sharing of PHI. While permissible uses and disclosures of PHI include those made for purposes of treatment, payment and healthcare operations, reasonable care must be taken to avoid disclosures incidental to disclosures made for treatment purposes (ie, one should not have patient-specific conversations with coworkers in nonprivate areas).[8] It is never permissible to "snoop" in patient records out of curiosity.

The US Department of Health & Human Services' Office of Civil Rights (OCR) is responsible for enforcing HIPAA. OCR's investigations are complaint driven. In response to complaints received, OCR conducts an investigation and, if it finds that a HIPAA violation occurred, may require corrective action and/or a resolution agreement. If a covered entity is unable to resolve a breach in a satisfactory manner, OCR may impose civil monetary penalties. OCR may also refer matters to the US Department of Justice for criminal investigations. Covered entities and their corporate directors, employees, and officers face criminal fines of up to $50,000 and up to 1 year in prison for "knowingly" obtaining or disclosing PHI in violation of the Privacy Rule.[9] Providers found to have violated HIPAA may also be excluded from participating in Medicare.

The US Department of Health & Human Services publishes case examples of completed health information investigations. In one reported case, a nurse and an orderly discussed a patient's HIV/AIDS status within earshot of other patients without making reasonable efforts to prevent the disclosure. Both employees were placed on leave once their hospital learned of the incident. The orderly ultimately resigned, while the nurse received a write-up in her personnel file, 1 year probation, referral for peer review, and further HIPAA training.[10] In another case, a nurse practitioner was referred for discipline to her state licensing board after improperly accessing her ex-husband's medical records that were housed by the multihospital healthcare system where the nurse practitioner held privileges.[10]

Recent news stories highlight the risk to healthcare providers' careers when HIPAA violations go beyond the waiting room and traditional snooping activities into an online community. Two nurses in Wisconsin are being investigated by the Federal Bureau of Investigation (FBI) for possible federal violations after a photograph of an x-ray image showing a sexual device lodged in a patient's rectum was posted and discussed on one of the nurse's Facebook pages. A local sheriff's investigation determined that 2 nurses had photographed the x-ray and at least one posted it online. The nurses were fired for violating company policy and, in addition to the FBI investigation, may also face discipline from their state licensing board.[11]

Emergency personnel responding to incidents must also be mindful of privacy restrictions. An astonishing error of judgment by a treatment provider was reported in New York City last summer. An emergency medical technician who responded to a call on Staten Island took a picture of a murder victim at a crime scene with his cell phone and posted it on his Facebook page. The emergency medical technician was fired by his hospital and is facing official misconduct charges in state criminal court.[12] A recent California decision also highlights this concern. A California Court of Appeal held that the online distribution of photos of a car accident victim's mutilated corpse gave rise to a cause of action by the surviving family members for invasion of privacy and intentional infliction of emotional distress.[13]

All hospitals and healthcare facilities have (or should have by now) HIPAA policies in place. In addition to the risk of an OCR and possible criminal investigation, employees and other providers who violate HIPAA may face discipline and possible termination according to the terms of their facilities' policies.

State Level Privacy Protections

While HIPAA protects patients' identifiable health information, it does not create a private right of action for patients. In other words, patients cannot sue providers directly for HIPAA violations, and complaints must be resolved via OCR and individual facilities. State law, however, does provide theories of liability and means of recovery to aggrieved patients. State practice acts may also authorize state licensing boards to discipline providers for confidentiality breaches and unprofessional conduct.

Based on a strong public policy in favor of protecting the confidentiality of patient medical information, many states recognize a common law right to privacy for patients. Providers who breach their duty of confidentiality by disclosing confidential patient information may be liable to the patient for injuries sustained as a result of the disclosure.

In New York, a court held that the publication of a picture of a patient's silhouette receiving treatment constitutes a breach of the physician-patient privilege.[14] The court specifically held that the fact that a patient received treatment is equally as confidential as the nature of the treatment. The patient was HIV-positive and was receiving treatment in a hospital's infectious disease unit. The patient reluctantly consented to the silhouette photograph taken from a back angle but was not told the purpose of the photograph. Two days after receiving treatment, the photograph appeared on the front page of a local newspaper as part of an article titled "Aura of urgency cloaks [University of Rochester's] research on AIDS." The patient sued his physician, the hospital and the newspaper, alleging that he was identifiable and that the publication strongly implies he has AIDS. The court found that healthcare patients' rights to the privacy of their medical information are rooted in the clear public policy of the state prohibiting healthcare providers and institutions from disclosing information discovered in attending the patient.[15] The court also held that damages would not be limited to economic losses suffered by the patient (ie, could include reputational and emotional damages).

In 1994, an Ohio court found that a treating physician may be liable to a patient after the physician's nurse disclosed a patient's pregnancy to the patient's mother over the phone.[16] Similarly, in Oregon, a patient was awarded damages after a provider disclosed the patient's suicide attempt to an individual who in turn disclosed that information to the patient's mother's colleagues and professional adversaries.[17]

In limited states, courts will recognize a tort action under the malpractice statute for breach of patient confidentiality, finding that the standard of care includes a duty to maintain the confidentiality of the practitioner-patient relationship. In Washington, for example, a court held that a treating physician who called a patient's ex-husband, who was also a physician, to discuss the patient's use of prescription pain medications, could be liable under Washington's malpractice statute to the patient for damages resulting from his unauthorized disclosure.[18]

In addition to breaches of confidentiality claims, providers who betray patient confidences may also face civil claims for negligent and/or intentional infliction of emotional distress and invasion of privacy. In Illinois, a court recently found a phlebotomist could be liable under common law rights of privacy and for negligent and intentional infliction of emotional distress for the damages caused to a patient after the phlebotomist revealed the patient's pregnancy to the patient's sister at a bar on the weekend.[19] The same court found that the phlebotomist's hospital employer was not liable to the patient for the phlebotomist's disclosure because the phlebotomist was not acting within the scope of her employment when the breach occurred.

Liability for invasion of privacy may attach for publication of confidential information when such publication would be highly offensive to a reasonable person and is not of legitimate concern to the public. While disclosure to one or a few persons does not generally constitute "publication" for purposes of determining whether someone is liable to another for invasion of privacy, providers have been found liable for such actions as (1) displaying before and after pictures of a patient's plastic surgery pictures without the patient's express consent for the display,[20] and (2) negligence in mailing an insurance claim form disclosing a patient's treatment for chronic alcoholism to the patient's husband's employer.[21] A Facebook or other online posting would more than likely constitute publication for purposes of determining liability for invasion of privacy.[22]

Breaches of patient confidentiality may also result in discipline by state boards of nursing under the applicable practice act. Many nurse practice acts contain provisions authorizing the board of nursing to discipline licensees for breaches of patient confidentiality. In Illinois, for example, CRNAs may be disciplined for "willfully or negligently violating the confidentiality between nurse and patient except as required by law."[23] Florida nurses may be disciplined for "violating the confidentiality of information or knowledge concerning a patient."[24] Violations of patient confidentiality may be reviewed under a nurse practice act's prohibition of "unprofessional conduct" in those states that do not specifically list breach of patient confidences as grounds for discipline.

Institutional Policies

Most, if not all, healthcare facilities have HIPAA policies in place that

apply to their employees and independent contractors alike. A conventional HIPAA policy will apply to online violations in the same manner as it applies to more traditional written and oral violations. Some facilities are beginning to address the "Facebook issue" by developing and adopting social media policies that specifically address their employees and providers' online activities, both in and outside of work. Some employers block employee access to social media sites on company computers, while others encourage employee use of social networks, likely to foster the development of community and in hopes of generating free press, goodwill, and product endorsements.[25] Some hospitals and healthcare facilities are even asking employees to connect their online profiles to their employer's site and, in turn, may be monitoring employees' online postings outside of working hours.[25]

CRNAs should become familiar with their facilities' policies concerning patient confidentiality, unprofessional conduct and, if applicable, use of social media. It is possible that you work at a facility with a social media policy giving your facility the right to discipline or fire you based on your online activities outside of work. Work-related postings that are not patient-specific may still raise eyebrows in your facilities' risk management office. For example, a seemingly innocent status update about a long day at work due to understaffing may have consequences in the healthcare industry that do not exist in other industries.

Many companies are also checking the online profiles of potential new hires. Unacceptable online content may prohibit applicants from landing their next dream job.

AANA's Code of Ethics

In addition to applicable regulations and facility policies, CRNAs must adhere to the AANA's Code of Ethics or risk disciplinary action up to suspension or revocation of membership in AANA. The AANA's Code of Ethics[26] provides in relevant part:

> **1 Responsibility to Patients**
> Certified Registered Nurse Anesthetists (CRNAs) preserve human dignity, respect the moral and legal rights of health consumers, and support the safety and well being of the patient under their care.
>
> 1.6 The CRNA maintains confidentiality of patient information except in those rare events where accepted nursing practice demands otherwise.
>
> 1.8 The CRNA does not exploit nor abuse his or her relationship of trust and confidence with the patient or the patient's dependence on the CRNA.

To Post, or Not to Post?

Given the rules and examples above and the often-cited strong public policy in favor of protecting patient confidentiality, it is easy to see how a healthcare provider who posts work-related information online in a Facebook status update, a "tweet," or a discussion blog could unwittingly become ensnared in a disciplinary investigation at work, a federal investigation of a possible HIPAA violation, a disciplinary investigation by the state licensing board, and a civil lawsuit filed by an aggrieved patient.

We are not suggesting that healthcare providers shy away from common online networking applications. These new media tools and technology serve important social and professional purposes in today's society. But please, for your sake and the sake of the profession, stop and think before you post. Conventional advice in the business world says not to post it if you would not want your boss to read it. We agree, and would add your patients, your state board of nursing, and your AANA colleagues to the list of potential readers you should keep in mind.

REFERENCES

1. Facebook Press Room. http://www.facebook.com/press/info.php?statistics. Accessed June 1, 2010.
2. Hof RD. Facebook's New Wrinkles. *Bus Week*. August 20, 2007(4047):38.
3. Health Insurance Portability and Accountability Act of 1996. Pub. L. 104-191 (Aug. 21, 1996).
4. Privacy Act; implementation. *Fed Regist*. 2000;65(250):82462-82829.
5. Health Information Technology for Economic and Clinical Health Act §13404. 42 USC §17934(a) (2009).
6. Privacy Act; definitions. *Code Fed Regul*. 45CFR §160.103(2006).
7. Privacy Act; requirements relating to uses and disclosures of protected health information. *Code Fed Regul*. 45 CFR §164.514(b)(2)(i) (2009).
8. Individually identifiable health information; privacy standards. *Fed. Regist*. 2002; 67(157):53193-53195.
9. 42 USC. §1320d-6 (2010); US Department of Justice June 1, 2005 Memorandum Opinion for The General Counsel Department of Health and Human Services and the Senior Counsel to the Deputy Attorney General. http://www.justice.gov/olc/hipaa_final.htm. Accessed May 17, 2010.
10. US Department of Health & Human Services, Health Information Privacy, All Case Examples. http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/allcases.html. Accessed May 17, 2010.
11. Facebook firings show privacy concerns with social networking sites. *Healthcare Risk Manage*. May 2009;31:49-52.
12. New York Local News (CBS). NY EMT accused of posting corpse photo on Facebook. June 5, 2009. http://wcbstv.com/local/corpse.photo.facebook.2.1031531.html. Accessed May 18, 2010.
13. *Catsouras v Dept. of the California Highway Patrol*, __ Cal. Rptr.3d __, 2010 WL 337335 (Cal. Ct. App. 4th Dist. Jan. 29, 2010).
14. *Anderson v Strong Memorial Hospital*, 531 N.Y.S.2d 735 (N.Y. Sup. Ct. 1988).
15. *Anderson*, citing *Doe v Roe*, 400 N.Y.S.2d 668 (N.Y. Sup. Ct. 1977).
16. *Hobbs v Lopez*, 645 N.E.2d 1261 (Ohio App. 1994).
17. *Doe v Portland Health Centers*, 782 P.2d 446 (Or. App. 1990).
18. *Berger v Sonneland*, 1 P.3d 1187 (Wash. App. 2000).
19. *Bagent v Blessing Care Corp.*, 862 N.E.2d 985 (Ill. 2007).
20. *Vassiliades v Garfinckel's, Brooks Brothers, et al.*, 492 A.2d 580 (D.C. App. 1985).
21. *Herman v Kratche*, 2006 WL 3240680 (Ohio App. 2006).
22. See, eg, *Peterson v Moldofsky*, No. 07-2603, 2005 WL 3126229 (D.Kan. Sept. 29. 2009).

23. Ill Comp Stat ch 225, §65/70-5(b)(25) (2007).
24. Fla. Admin. Code §64B9-8.005(7)(2009).
25. Klich-Heartt EI, Prion S. Social Networking and HIPAA: Ethical Concerns for Nurses. *Nurse Leader.* April 2010;56-58.
26. American Association of Nurse Anesthetists, Code of Ethics for the Certified Registered Nurse Anesthetist. 2005. http://www.aana.com/codeofethics. aspx. Accessed June 14, 2010.

AUTHORS

Amy L. Hader, JD, is a professional practice specialist at the American Association of Nurse Anesthetists, Park Ridge, Illinois.

Evan D. Brown, JD, is an attorney in the Chicago, Illinois, office of Hinshaw & Culbertson, LLP, where he practices technology and intellectual property law. Brown is also a social media enthusiast. He writes the Internet cases blog (http://internetcases.com), and you can find him on Twitter at http://twitter.com/internetcases.