physician connection
Professional SOLUTIONS
PROFESSIONAL SOLUTIONS INSURANCE COMPANY BRINGS YOU PRACTICAL TIPS FOR AVOIDING A MALPRACTICE ALLEGATION ISSUE 1 • 2011

Physician Practices & Social Networking

Do the Risks Outweigh the Benefits?

INSIDE THIS ISSUE:

Social Networking (SN) has become a cultural phenomenon. Sites such as Twitter, MySpace, Facebook, YouTube, and LinkedIn are well recognized, with Facebook alone having over 500 million active users.[1] What's more, advances in mobile technology have resulted in the meteoric rise of texting and instant messaging for personal and professional communication, including the ability to easily take and send photo and video attachments.

More hospitals and practices are recognizing the potential of SN, as well. As of October 3, 2010, 830 hospitals were using SN tools, including over 600 with Facebook pages.[2] Renowned medical centers like the Mayo Clinic and Henry Ford were frontrunners in successfully using Twitter and Facebook as electronic forms of word-of-mouth advertising.[3] Physician participation in SN on general and physician-specific SN sites (e.g., Sermo, Ozmosis, DoctorsHangout, and IMedExchange, etc.) is also increasing in popularity.

These sites are limited to healthcare providers and are more secure than general sites, something that is extremely important. As online technology and SN continue to evolve, there is the potential for unknown risks that may adversely impact a physician's professional liability.

Protection of Patient Health Information

The most significant concern about SN is the lack of security offered both by sites and electronic devices. The duty to protect patient confidentiality is inherent in the physician-patient relationship and the hospital-patient relationship and extends to all employees and staff. That duty applies to patient health information (PHI) in any format—whether through spoken gossip, a misplaced chart, an overheard hallway consultation, a lost laptop, in a chat room, a Tweet or a Facebook posting.

In addition, users of SN routinely share detailed information about their daily lives and activities, and hit the SEND button without much forethought about the ramifications. Once posted, the information or photo can't be taken back or deleted. Also, consider that despite signing confidentiality agreements, some employees still inappropriately send out patient information they feel is interesting to share. Here are two recent breaches involving unauthorized photography of a patient and subsequent posting on a SN site:

- A patient who was treated in a Hawaiian hospital after a shark attack is now suing the hospital in which he was treated for HIPAA and privacy violations after a member of the ED staff photographed his severely bitten leg and circulated the photos on the Internet.[4]
- In a California case, emergency responders and hospital personnel were accused of photographing a dying 60-year-old man who had been stabbed 16 times in the neck by his convalescent home roommate, and posting the photo on Facebook.[5]

As HIPAA and the Health Information Technology for Economic and Clinical Health (HITECH) Act increase penalties for such PHI breaches, there are serious monetary repercussions for the practice or physician employer,

Continued on Page 2

Continued from Page 1

potential disciplinary actions (including dismissal) against the involved employee, as well as loss of patient trust and bad physician-patient relations. (See "Civil Money Penalties" table below.)

Civil Money Penalties under HIPAA Privacy and HITECH

The Department of Health and Human Services Office of Civil Rights (OCR) may impose a penalty on a covered entity for a failure to comply with a requirement of the Privacy Rule. Penalties will vary significantly depending on factors such as the date of the violation, whether the covered entity knew or should have known of the failure to comply, or whether the covered entity's failure to comply was due to willful neglect. Penalties may not exceed a calendar-year cap for multiple violations of the same requirement.

Practices need to update their confidentiality policies and HIPAA training programs annually to address how a patient's right to confidentiality can be breached by new technology and devices in addition to more traditional scenarios. Practice policies should address staff access to SN sites during working hours, including whether access via the practice's computer system or an e-device for personal or practice-related purposes is permissible. Training efforts should be documented. As with all other office policies, staff should initial the policy after review.

To add to the risk potential, most patients, family members, vendors and other visitors come to the office or hospital with smartphones or PDAs capable of capturing confidential patient information. For this reason, many hospitals and practices are banning these devices in patient areas in an attempt to protect patient privacy. (See enclosed Sample Policy Statement "Use of Cell Phones, Smartphones, PDAs, Laptops and Other Similar Electronic Devices.")

Data and Identity Theft/Viruses

Because the Internet is far from adequately regulated or secure, there is a significant risk of breaching patient confidentiality when information is stored online. Unfortunately, these sites have become easy prey for hackers, scammers and phishers in the business of identity theft, fraud and other cybercrimes. Malicious software and code can be planted into victim computers that allow passwords for any account on that computer to be stolen. The thieves can then change the user's passwords to hijack SN accounts and then move on to friends of the victim. Over 3,000 such hijackings were reported to the FBI's Internet Crime Complaint Center between 2006 and 2009.

Cellphones, smartphones, PDAs and other electronic devices present potential risk to practice and patient information security when used for e-communications and SN in the office. SN sites could become portals for illegal access into other databases or additional PHI. Getting access to patient records is especially valued by hackers because they often include complete demographic information, including Social Security Numbers. Consequently, not only could patient information be breached and stolen, the entire system could be incapacitated by a virus. That's why it's important to put in place technology risk audits, firewalls and security scans and to routinely monitor the system's protection.

Professional versus Personal Posts and "Friending"

Most physicians have a desire to keep their personal and professional lives separate. Yet, many frequent online chat rooms, social networking sites, or they maintain blogs where they identify themselves as physicians. It is important that physicians ask themselves whether any postings could adversely affect their professional relationships. Researchers at the University of Pennsylvania recently studied 271 medical blogs[6] and found:

- Individual patients were described in 114 (42.1%) blogs.
- Patients were portrayed positively in 43 blogs (15.9%) and negatively in 48 blogs (17.7%).
- Of blogs that described interactions with individual patients, 45 (16.6%) included sufficient information for patients to identify their doctors or themselves.
- Three blogs showed recognizable photographic images of patients.
- Healthcare products were promoted, either by images or descriptions, in 31 (11.4%) blogs.

The study concluded that blogs are: *a growing part of the public face of the health professions and provide an opportunity for physicians and nurses to share knowledge and experiences gleaned from patient cases. They also risk*

CIVIL MONEY PENALTIES

	For violations occurring prior to 2/18/2009	For violations occurring on or after 2/18/2009
Penalty Amount	Up to $100 per violation	$100 to $50,000 or more per violation
Calendar Year Cap	$25,000	$1,500,000

Source: OCR website, www/hhs/gov/ocr/privacy/hipaa/understanding/summary/index.html

revealing confidential information or, in their tone or content, risk reflecting poorly on the blog authors and their professions. The health professions should assume some responsibility for helping authors and readers negotiate these challenges.[7]

Some practice and risk management experts recommend that a physician or other healthcare professional interested in SN have two separate pages—one personal and one professional. Some even go so far as saying a physician's personal account should be devoid of any mention of the physician's professional status.

Moreover, accepting patients' invitations to be "friends" or asking patients to be your "friend" is not recommended as it blurs the patient's distinction between physician and patient and jeopardizes the efficacy of the therapeutic process. It may be a good idea to develop a standard response in this area. For example, tell patients that you make it your policy not to "friend" current or former patients out of respect for the physician-patient relationship and to safeguard the patient's confidentiality. Some physicians also develop a social media policy that addresses the professional use of all types of social media by the physician and practice with patients. This policy could be incorporated into the practice's new patient practice information booklet.

If a physician elects to have a profile on one or more SN sites, privacy settings will require extreme care and regular attention. Even when privacy settings are in place, the protection may not be sufficient. The privacy settings on these sites were never intended to guarantee the level of security and privacy required for PHI.

It is essential to keep online discussions free of patient-specific information if there is a chance that the patient's identity could be gleaned from the facts presented. Some physicians use physician-specific SN sites to get advice on a particular case. Consider these to be online hallway consultations and make sure no patient-specific information is exchanged that could jeopardize the patient's identity or privacy.

To reference the American Medical Association's policy on the use of social media, go to www.ama-assn.org/ama/pub/meeting/professionalism-social-media.shtml

Medical Advice

It is not prudent to use the Internet for any specific discussions with patients about their condition or treatment, unless the site is known to be secure. Various health systems have set up password-protected and encrypted communication sites for general dissemination of patient information or dedicated patient portals for specific patient-physician online communication.

Outside of such systems, security cannot be assumed, and it is best to avoid communicating anything that could be construed as medical advice. Even a seemingly innocent comment could be interpreted by a patient as medical advice and could come back to haunt you.

In addition, responding to a patient's specific medical questions or requests for medical advice should be documented, just as they would with telephone calls between a physician and patient. Should the patient have ill effects from following online medical advice and subsequently file a malpractice claim, the defense would be jeopardized. The old adage of

SAMPLE POLICY STATEMENT

Use of Cell Phones, Smartphones, PDAs, Laptops and Other Electronic Devices

To Our Patients:

The physicians and staff of XYZ Medical Associates are dedicated to safeguarding the privacy of our patients and protecting the health information exchanged during their care and treatment. As such, the use of cell phones, smartphones, PDAs, laptops and all other electronic devices is not allowed in the reception area, waiting areas or patient care areas of this practice. This is a policy followed by all XYZ staff, and we expect our patients and their families to comply with it, as well.

These devices are permitted ONLY in the main hallway of this building outside the reception area. If there are special circumstances that require your use of an electronic device while in our practice, please see our office manager. Thank you.

Sincerely,
Drs. X, Y and Z

Continued on Page 4

"if it's not in the record, it didn't happen" would apply.

If you choose to communicate with patients in this fashion it is imperative that you spell it out in advance how often you will be online and be vigilant about maintaining that schedule. Once a physician commits to online patient communication, he or she must check back frequently to continue the conversation string. If a patient posts pertinent and time-critical information related to treatment and the physician isn't able to respond in a timely fashion, it could lead to an allegation of delayed treatment or diagnosis. It's also important to advise patients about other ways to reach you during office hours, after hours and in emergency situations. These should be addressed via a practice email or SN policy.

For all of these reasons, it is best to avoid giving medical advice online. Instead, recommend the patient call your office or schedule an appointment to continue the discussion.

SAMPLE POLICY COMPONENTS

Components of a Social Networking Policy

When developing a social networking policy for inclusion in your practice privacy policy, consider the following:

- ☑ **Will the practice have its own professional page on a SN site such as Facebook, LinkedIn, YouTube, Twitter, Blogspot or similar online forums?**
- ☑ **Will the practice policy prohibit the use of electronic devices that could be used to inappropriately text, photograph or video patients, their protected health information, staff or patient areas during normal working hours?**
- ☑ **Will the practice ban access to social networking sites by the physician, staff, patients, visitors and vendors during working hours?**
- ☑ **Will the practice allow staff and employees to access SN sites for personal purposes during designated breaks on the practice premises?**
- ☑ **Will the practice routinely discuss how HIPAA regulations can be breached by SN postings by staff, practice patients and their families?**
- ☑ **Will the practice provide information to patients and their families about the practice's commitment to the protection of patient information?**

For guidance on each component, please refer to the separate insert.

Questions?

If you have any questions you'd like our **Connection** *experts to answer, please e-mail them to riskmanagement@psicinsurance.com*

Be Vigilant to Avoid the Risks

Although the risks inherent with SN may outweigh the benefits in many situations, there are ways to mitigate those risks and still protect your patients' confidentiality and privacy and yourself from professional liability. Navigate wisely and be vigilant to avoid the dangers that lie within. Regardless, it is best to proceed with caution—just because you can't see the SN content doesn't mean it's gone for good.

[1] Facebook Press Room. Statistics – People on Facebook. Accessed October 2, 2010, at: www.Facebook.com/press/info.php?statistics

[2] Bennett, E. Hospital Social Networking List as of 10/3/2010. Accessed October 6, 2010, at: http://ebennett.org/hsnl/

[3] Yee, CM. Mayo turns to social media to reach out to potential patients. April 29, 2009. Star Tribune. Available at: www.startribune.com/business/43644522.html

[4] HIPAA News, Shark Attack Victim Suing Hospital for HIPAA Violations. Sept. 22, 2010. Available online at: http://hipaanews.net/archives/2010/09/22/shark-attack-victim-suing-hospital-for-hipaa-violations/

[5] Cawley-Jean, N. Why is it so hard for hospital staff to follow HIPAA rules when using social media? August 12, 2010. www.wellsphere.com/general-medicine-article/why-is-it-so-hard-for-hospital-staff-to-follow-hipaa-rules-when-using-social-media/1195050

[6] Lagu, T, Kaufman, EJ, Asch, DA, & Armstrong, K. (2008). Content of Weblogs Written by Health Professionals. J Gen Intern Med 2008 October 23(10): 1642-1646.

[7] Ibid.

Professional SOLUTIONS INSURANCE COMPANY

Send all inquiries, address changes and correspondence to:
Physician Connection, P.O. Box 9118, Des Moines, IA 50306
Toll-Free 1-888-336-2642
Internet – www.psicinsurance.com
Email – riskmanagement@psicinsurance.com