Publication of MEDICAL MUTUAL / Professionals Advocate®

DOCTORS Rx

Volume 18 No. 2 Winter 2010

A Letter from the Chair of the Board

Dear Colleague:

The ability to communicate outside of the traditional methods of e-mail and Internet sites has evolved to now include social networking sites as a means of exchanging information.

This issue of Doctors RX *will take a look at the ramifications of social networking not only for Physicians, but also their staff and will provide suggestions to reduce the legal risk of utilizing this new form of communication.*

George S. Malouf, Jr., M.D.
Chair of the Board
MEDICAL MUTUAL Liability Insurance Society of Maryland
Professionals Advocate Insurance Company

Why Can't We Be "Friends"?

The Pitfalls of Social Networking for the Practicing Physician

Imagine this scenario: Upon arriving to the office you discover that one of your patients has filed a complaint with the Office for Civil Rights alleging a HIPAA privacy violation. The matter involves some seemingly innocuous posts you had made describing the attributes of a difficult patient. The content of these posts are being investigated to determine if they are descriptive enough to make the patient's identity discernable to the general public. Think it can't happen? Think again.

Online social networking has exploded over the past half-decade. The most popular social networking site, Facebook, was founded a little more than six years ago and in July 2010 boasted 500 million active users.[1] For Physicians, social networking may be beneficial for marketing, patient education and even online collaboration regarding patient care. One need only watch the local news or search quickly online to find examples of new uses of social media sites by Physicians (such as a recent *Baltimore Sun* article regarding social media discounts for new patients), but also tales of abuses of social networking leading to lawsuits, citations for HIPAA violations, professional discipline, even suicide.

Continued on next page

Todd Anderson, Esq.
Attorney with the firm of LeClairRyan in Richmond, Virginia

If social networking is the wave of the future (particularly among those who say "e-mail is for old people"), how can a Physician reap the rewards while managing the potential risk? The answer can be complicated and clouded with legal jargon, but you can go a long way in this area by employing that timeless resource: **common sense.**

Physician Protect Thyself

One would think that individuals would be more guarded with the information they share with the rest of the world and not deviate from common sense behavior. Sadly, this is not always the case. Many individuals continue to believe the Internet affords them a level of anonymity which does not exist. One has only to recall the online blogging of "Dr. Flea" to see the negative ramifications for Physicians. Dr. Flea was the pseudonym of a Boston-area pediatrician who was sued for medical malpractice in the death of a young child. Prior to and during his trial, he posted information on his blog regarding his deposition, meetings with a witness consultant, the plaintiff's case, the plaintiff's attorney and even the jurors. Unfortunately for the Physician, the plaintiff's attorney had been following the blog and questioned him about his online persona during cross-examination. The case settled within 24 hours. Even worse for the Physician, the story made it to the *Boston Globe* so that his patients and colleagues could see what he had done.[2]

With that scenario in mind, consider the cost of an ill-advised blog or post that could effectively create a cloud over eight years of medical school training, internship and residency. Do you really want a patient to see a medical school photograph of you in a compromised position posted to your personal Facebook page? Unlikely to happen? A 2008 University of Florida study published in the *Journal of General Internal Medicine* examined the Facebook status of more than 800 medical school students. In a randomly selected subset of ten individuals, seven included photos of the student drinking alcohol and as many as half the photos suggested what the researchers called "excessive or hazardous drinking."[3] Services now exist to monitor Internet traffic with the goal of protecting your reputation and alerting you to negative comments made about you by others. In the end, however, your

reputation depends largely upon your own actions. Physicians should consider what is posted to their personal sites, whether that site is marked private, and whom one allows to view the information.

Patient Confidentiality

Long before the advent of social networking sites, Physicians faced issues regarding patient confidentiality and the behavior of staff members, issues which can easily turn into lawsuits. In one small community, a patient with HIV alleged he was known personally by a medical office staff member who communicated his condition to a friend, and so on and so on, until the patient arrived at a party to learn everyone knew his diagnosis. This was years before social networking web sites. Imagine how easily a member of your staff "innocently" could "tweet" the presence of her high school classmate in your waiting room. "OMG! Ginny Smith is pregnant! I didn't think

CME Test Questions

Instructions for CME Participation

CME Accreditation Statement — MEDICAL MUTUAL Liability Insurance Society of Maryland, which is affiliated with the Professionals Advocate® Insurance Company, is accredited by the Accreditation Council for Continuing Medical Education (ACCME) to provide continuing medical education for Physicians.

CME Designation Statement — MEDICAL MUTUAL Liability Insurance Society of Maryland designates this enduring material for a maximum of one (1) *AMA PRA Category 1 Credit(s)*.™ Physicians should claim only the credit commensurate with the extent of their participation in the activity.

Instructions—to receive credit, please follow these steps:

1. Read the articles contained in the newsletter and then answer the test questions.
2. Mail or fax your completed answers for grading:

   Med•Lantic Management Services, Inc.
   225 International Circle
   P.O. Box 8016
   Hunt Valley, Maryland 21030
   Attention: Risk Management Services Dept.

   Fax: 410-785-2631

3. One of our goals is to assess the continuing educational needs of our readers so we may enhance the educational effectiveness of the *Doctors RX*. To achieve this goal, we need your help. You must complete the CME evaluation form to receive credit.
4. Completion Deadline: March 25, 2011
5. Upon completion of the test and evaluation form, a certificate of credit will be mailed to you.

1. If utilized with good judgment, social networking has the potential to provide Physicians with which of the following beneficial uses?

   A. Patient education
   B. Online collaboration
   C. Marketing
   D. All of the above

2. Comments posted to a blog, Facebook account, or other social networking site may be brought into evidence in a court proceeding.

   A. True B. False

3. Negative posts on social networks about hospitals or other providers are shielded by the peer review privilege.

   A. True B. False

4. State and federal privacy protections apply equally to disclosures of confidential and protected health information posted on the Internet as they do for other forms of communication.

   A. True B. False

5. Physicians cannot restrict employees from posting on external sites due to freedom of speech.

   A. True B. False

6. Suggested ways to reduce your risk of having to defend against privacy law violations involving Internet use include?

   A. Developing office policy on sharing information online
   B. Educating staff on issues regarding patient confidentiality
   C. Maintaining an anonymous presence online
   D. A and B

7. Many health care organizations have developed social media policy guidelines to educate staff on prohibited posting practices.

   A. True B. False

8. While general medical information may be beneficial to the public, Physicians should be cautious about providing specific advice to patients online because of the potential for inadvertently creating a Physician-Patient relationship.

   A. True B. False

9. Social network sites catering to Physicians maintain patient identifying information but redact that information from postings to protect individual privacy.

   A. True B. False

10. Virginia has adopted a policy which allows litigants and lawyers unfettered access to comb social networks for information related to litigation.

    A. True B. False

CME Evaluation Form

Statement of Educational Purpose

Doctors RX is a newsletter sent twice each year to the Insured Physicians of MEDICAL MUTUAL/Professionals Advocate®. Its mission and educational purpose is to identify current health care related risk management issues and provide Physicians with educational information that will enable them to reduce their malpractice liability risk.

Readers of the newsletter should be able to obtain the following educational objectives:
1) Gain information on topics of particular importance to them as Physicians,
2) Assess the newsletter's value to them as practicing Physicians, and
3) Assess how this information may influence their own practices.

CME Objectives for "Why Can't We Be Friends"?

Educational Objectives: As a result of participating in this enduring material, participants should be better able to:
1) Consider implications for their practice caused by staff use of social networking sites.
2) Evaluate possible uses in litigation of information contained on social networking sites and the ease of "mining" that information.
3) Plan an appropriate social networking policy for the practice.

	Strongly Agree				Strongly Disagree
Part I. Educational Value:	5	4	3	2	1
I learned something new that was important.	❑	❑	❑	❑	❑
I verified some important information.	❑	❑	❑	❑	❑
I plan to seek more information on this topic.	❑	❑	❑	❑	❑
This information is likely to have an impact on my practice.	❑	❑	❑	❑	❑

Part 2. Commitment to Change: What change(s) (if any) do you plan to make in your practice as a result of reading this newsletter?

_____

_____

_____

Part 3. Statement of Completion: I attest to having completed the CME activity.

Signature: _____ Date: _____

Part 4. Identifying Information: Please PRINT legibly or type the following:

Name: _____ Telephone Number: _____

Address: _____

_____

_____

_____

she was married yet." It is fairly obvious that this sort of commentary is problematic; however, simply posting that a patient was seen in your office may be sufficient to raise privacy concerns.

At the time this newsletter went to press, no formal guidelines on social networking for Physicians had been issued by the Virginia, Maryland or D.C. medical boards. The AMA's Council on Ethical and Judicial Affairs is currently at work on ethical guidance that could be presented as a report within the next 12-18 months. Despite the lack of these formal guidelines, the same privacy protections afforded by HIPAA and state privacy laws apply to the Internet as well as other forms of communication. Violations of federal and state privacy laws can result in civil and criminal penalties; therefore, it is important to educate your staff as well as yourself. Make clear what is acceptable and what is not. Have a specific social media policy in place which applies equally to Physicians and staff, and at a bare minimum includes the following:

- Personal responsibility for the content published on blogs, wikis, social networking sites or any other form of user-generated media.
- Prohibitions from disclosing any information that is confidential or proprietary to the practice (including patient information). This also includes information provided by a third party to the practice.
- Agreement to uphold the practice's policy to respect individuals and avoid making any defamatory, disrespectful or harassing statements about other employees, members, partners and affiliates of the practice.
- Disciplinary standards that outline the consequences for conduct in violation of the social media policy, up to and including termination of employment.

Caution against what information is shared online and how some information may hurt patients, the practice, or themselves. Have the employee acknowledge the policy with his or her signature. Repeat that education regularly and with every new hire. Do not wait for the inadvertent disclosure and the subsequent reporting requirements, lawsuit and media inquiries to prompt you to action.

Hospital Relationships

Criticisms of hospital personnel, bureaucracy, communications, etc. are not uncommon, but they often are contained within the office water-cooler setting. When criticisms and dissatisfaction are voiced through a social networking site, however, they become open to the public. A Physician or staff member posts: "Another screw-up with the hospital today. Failed to send pathology on a patient with cancer, now Stage IV. When are they going to get it right!?" Who are this individual's "friends?" Who are the friends of **their** friends? What will be your response to hospital administration when they learn of the post and call your office? Will you be prepared to address in a deposition questions regarding your office's alleged knowledge of ongoing failures in hospital communication which you failed to address or protect against?

Find out the social media policies of the hospitals and ambulatory surgical centers where you regularly send patients to make sure that patient information is being protected there as well. If no such policies exist, you may need to discuss corrective measures.

Suggestions for Social Media Policies

- Use common sense. Think before you post. Confidential information, especially that which relates to patients, must be kept **confidential.**
- Employ a plan.
- Make your social media policy clear and easy to understand. Avoid "legalese."
- Make it clear that your policy applies to both employer-hosted sites as well as external or personal sites.
- Prohibit the transmission of material which is unlawful, profane, threatening, obscene, libelous or hateful as well as any material which might infringe on any patents or copyrights. Statements made by employees often are attributed to the employer, even when the employee is operating on their own.
- Prohibit the transmission of unsolicited promotional materials (i.e. spam) as well as viruses or other files designed to disable or otherwise harm computer hardware or software.
- In order to provide transparency, Physicians and their staff should use their true identity when posting.
- Use disclaimers to identify all opinions as personal and not that of any current or former employer.
- Be clear about the consequences and ensure that they apply equally to Physicians and staff members. Violation of privacy laws can result in civil or criminal penalties to the practice. Employees should understand that they could face varying levels of disciplinary action from the practice, ranging from retraining up to and including termination of employment.

Marketing and Patient Communication

Hospitals, practice groups and individual Physicians continue to find ways to harness the Internet to push content to patients and potential patients. Online social networking is just another tool. As with any online content, Physicians should be cautious about providing specific advice to patients and creating Physician-Patient relationships. General medical information is helpful and beneficial and increases your online footprint, but be cautious about engaging in "discussions" via social networks wherein confidential patient information inadvertently may be disclosed.

Online Collaboration

The curbside consult now has a very long curb. Where once you might ask a colleague in the hallway about a particular case, a quick post can push your questions nationwide to professionals online. While Twitter, Facebook and MySpace get the media hype, social networking sites such as Sermo, Ozmosis and iMedExchange are restricted to Physicians and can be used to share opinions. Be mindful, however, how access to those sites might be used later. It is easy to envision a malpractice attorney asking if you posted any comments about your case to an online forum seeking advice and what you did in response to any such advice. While some sites maintain a privacy policy on how information will be used, it is unclear how social networking sites will respond to a subpoena seeking your particular post and responses to it for use in litigation.

E-Location Software

Not long ago, Physicians were surprised when attorneys used subpoenas for cell phone records to track when and how often they may have been called regarding a change in patient condition. In one lawsuit, cell phone records were cross-referenced with information from an online mapping website to inquire why it took the Physician so long to respond to a call when his home was only minutes from the hospital.

Today, geo-tracking and e-location software allows users to "tag" locations where they have been. Consider a scenario where you are on-call and go out for dinner. You, or maybe even your spouse, use a cell phone to "tag" a local restaurant with the comment, "Loved the wine selection. Of the three house wines, the cabernet is the best!" Later, you are called to the hospital for a patient who has taken a bad turn. How could that comment be used against you in the subsequently filed lawsuit alleging a failure to timely respond to a page or a failure in clinical judgment? Is it likely? Probably not anytime soon, but law schools are generating tech-savvy attorneys just as medical schools generate tech-savvy Physicians. The more adept attorneys become with these tools, the more likely they will be used in litigation.

The New York Bar Association recently decided it is ethical for lawyers to comb social networking sites to collect information on opposing parties involved in lawsuits, so long as the information is accessible to **all** members of the network. The underlying assumption by

plaintiff attorneys seeking such access is that these new avenues of research may prove to be fertile ground for acquiring damaging information.

Suggestions

Who are your "friends"?

You do not send all your patients your personal holiday card with a photo of you and your family around the fireplace. Likewise, patients do not need access to your family vacation photos posted on your Facebook page. Consider maintaining separate personal and business online presences.

Who are "friends" of your "friends"?

If you want something kept confidential, sharing it on the Internet with your college roommate may not be the way to go. One of the most troubling things about Internet content is that you cannot control how someone might use that information after it is "out there." True, that same concern exists for information shared in a private conversation, but when blasted to any number of individuals who may have access to your social networking page, you really cannot expect that problems with your partners or hospital administration will not make it to individuals you would prefer not hear your "unvarnished" opinions.

Have a plan

As with HIPAA and other laws regarding workplace discrimination, your staff should be educated on your policy for social networking. While some businesses block access to social networking sites from office computers, trying to stop someone from "tweeting" from their personal phone while at work may be futile. What you can do, however, is educate your staff that it is unprofessional, unacceptable and possibly illegal to post about patients, hospitals and other Physicians or other staff members. Getting that message across may prevent a situation like those discussed above.

Use common sense

Confidential patient information, criticisms of colleagues or hospitals, information about mergers, terminations, or litigation – none of this is information which should be broadcast to the public, some because it is illegal to do so, and some simply because it just is not a good idea. If you would not shout something to everyone in the room at a party, why would you do the online equivalent? Think before you post. Let common sense be your guide.

References

1 http://www.facebook.com/press/info.php?statistics

2 http://www.boston.com/news/local/articles/2007/05/31/blogger_unmasked_court_case_upended/

3 http://news.ufl.edu/2008/07/10/facebook/

Doctors RX

Elizabeth A. Svoysky, J.D., *Editor*
Assistant Vice President - Risk Management

Dr. George S. Malouf, Jr., M.D., *Chair of the Board*
MEDICAL MUTUAL Liability Insurance Society of Maryland
Professionals Advocate® Insurance Company

Numbers you should know!

Home Office Switchboard	410-785-0050
Toll Free	800-492-0193
Incident/Claim/ Lawsuit Reporting	800-492-0193
Risk Management Seminar Info	ext. 215 or 204
Risk Management Questions	ext. 224 or 169
Main Fax	410-785-2631
Claims Department Fax	410-785-1670
Web Site	www.weinsuredocs.com

Coming Soon:
Risk Management Education Programs for 2011!

The 2010 risk management education program, *Risk Management Protection for the Unpredictable*, has successfully concluded. We would like to thank the thousands of Physicians in Maryland and Virginia who participated and made 2010 one of our most successful programs ever.

MEDICAL MUTUAL/Professionals Advocate will be mailing brochures for our new risk management education programs in February 2011. We look forward to seeing you at one of these future programs.

Register online! It's easy, quick and secure.
www.weinsuredocs.com

Publication of MEDICAL MUTUAL/Professionals Advocate®

DOCTORS Rx

Volume 18 No. 2 Winter 2010

MEDICAL MUTUAL Liability Insurance Society of Maryland
Professionals Advocate® Insurance Company
Home Office: Box 8016, 225 International Circle
Hunt Valley, MD 21030 • 410-785-0050 • 800-492-0193