

THE ROZOVSKY GROUP, INC.



NEWSLETTER



Volume Five - Number Nine

September 2009

Should Healthcare Facilities Use Social Networking?

by Fay A. Rozovsky, JD, MPH and Joshua I. Rozovsky, MS

There was a time when “fast paced” sound bites came from the radio. The background noise was a cacophony of teletype machines and news directors shouting orders about news copy. A generation or two ago it was the likes of Walter Winchell who powered rapid delivery of “news” to a national hungry for information.

The telecommunications innovations of the 21st Century have changed all that. The public no longer “waits” for the news hour or idle chitchat in a gossip column. Today, it is the public who are crowding out the ranks of the “fifth estate” - the media. They do it by publishing news and observations of their own on blogs and other facets of “Web 2.0”. Some have become the eyes and ears of the “mainstream” media too, joining the ranks of “iReporters” who file their own commentary, videos, and photos electronically. Although news anchors may caution that “what you are about to see did not originate from our news teams,” the fact that it is on television or a website provides an air of credibility to such information.

Some “news” items are staged for the purpose of gathering attention. Sites like YouTube contain all manner of “information” and news. Some of the content is accurate and may be helpful, oftentimes emanating from well-respected sources embracing the new medium. At other times user-generated sites are replete with sophomoric pranks and gags that could be harmful to the intended “butt” of the joke. Compromising pictures can be found with relative ease on media-sharing sites on the Internet.

Sometimes user-generated content including blogs contain less than accurate

information. Content may include images of those who did not provide an authorization for their likeness or their information to be hoisted to a website or a blog.

The explosion in telecommunication possibilities includes social networking sites. A few years ago no one knew the terms “tweet” or “twitter.” Another novel term has arisen too, call “friending” another person. The term “Web 2.0” is often used to describe the various resources available for web-based “social” networking and other types of interactive online resources where the website content is created by its users rather than by a single editor or publisher. But just how “social” is the network? Does it have a business application? Should healthcare facilities use the blogs, the iReports, the websites, and all the innovative social networking sources to promote quality, safe, patient care? In other words, should healthcare facilities allow themselves to be “friended” or “linked in?” Should healthcare organizations send out “tweets” and if so, to whom?

Social Networking Examples in Healthcare.

There are numerous examples of social networking concerns in the healthcare field. Some involve so-called “bragging rights” about the latest sexual conquest or compromising photographs. Other bragging behavior has involved medical students discussing their exploits in the area of substance abuse or alcohol intoxication.

This is not a matter of conjecture. Indeed, a recent study published in the *Journal of the American Medical Association* described the results of a survey done among institutional members of the Association of American Medical Colleges.¹ The survey had a sixty percent response rate. It demonstrated that some 38% reported medical students posting sexually suggestive material and 39% reported students depicting intoxication on a website.²

Breaching patient confidentiality via social networking is yet another area of risk concern. In the study noted above, 13% reported patient privacy violations by medical students.³

A fundamental concept in social networking is communication based on trusting relationships. But what if the relationships are false? In New York, Attorney General Andrew Cuomo filed a lawsuit against a social networking website, alleging that consumers who visited the social networking site were essentially tricked into providing their personal email accounts that were then used to send

out millions of promotional emails. It was alleged that consumers were led to believe that the promotional material was coming from personal contacts when in fact the information was actually from spam emailers.⁴

Third-party “applications” added by users into social networking sites may also expose the organization and users to malware. The IT security firm Sophos’ 2009 threat report highlights the increasing risk of social networking as a vector for phishing attacks, and malware distribution.⁵

One can envisage how “friending” someone who is nothing more than a thief can lead to dissemination of important personal information and resulting identity theft. It can also occur as a result of so-called malware or “bots” penetrating a social networking site and accessing personal information and passwords. In the case of patients, the result could be identity theft or access to sensitive personal information including financial and health information that may have been posted in what were thought to be “private” areas of a user’s profile or page.

Yet another risk for patients is the degree of information hoisted to a social networking site. A person who chronicles on his social networking site his slow, painful recovery from a total right knee replacement may be broadcasting to would-be thieves that his house is empty. Similarly, a person with the best of intentions “tweets” to a host of concerned people that “Joan should be released from the hospital in five days.” What the “Tweeter” may not realize is that such information serves as a “green light” for a home burglary at Joan’s apartment.⁶

A facility that communicates with potential or current patients via a social networking tool must ensure that protected health information is not discussed using the network. It should be remembered that the identity of the online user may not be secure, and communications with that person via social networking tools may, in effect, be public.

The point is that trying to be “social” and communicative can have negative consequences. Web 2.0 and social networking are not foolproof. Like other types of “e” tools, the ability to safeguard communication is limited and users must exercise caution.

Can Social Networking Sites Help Prevent Risks?

Although some have little appetite for using social networking to “prevent” risks, Web 2.0 resources offer a rich resource for those in healthcare facilities. Human resources, credentialing, and security professionals may find pertinent information that can help identify those who *may* pose a risk of harm to patients or healthcare facility personnel. In a study conducted by CareerBuilder.com, an online job-search site, found 45% of employers used social networking searches on online applicants, with 53% of the rejections based on the “candidate post[ing] provocative or inappropriate photographs or information” and 44% of candidates rejected for “content about them drinking or using drugs.”⁷

Two hypothetical examples demonstrate what many see as the “upside” of social networking in the healthcare field.

Professionalism – Difficult at times to define, an important concept in healthcare professional credentialing is “professionalism.” A reference may be asked, “Does the applicant demonstrate attributes of professionalism consistent with his or her profession?” The reference responds, “Most of the time. But I suggest that you check the applicant’s blog for further information.” A check of the applicant’s blog reveals a photograph of the applicant in a suggestive pose. The tag line beneath the photo is filled with sexual innuendo and foul language. Further searches reveal additional “exhibits” suggesting a pattern of unsavory behavior by the applicant. The blog and other sites on the Internet refer to the individual as a medical specialist. Concerned that the specialist may lack professionalism, the Credentials Committee insisted on additional information. When told of the reason why he needed to provide more information, the applicant suddenly withdrew his application.

Will the Real RN Please Stand Up – A 45 year-old registered nurse applies for a job with a long term care facility. The applicant states that he worked in Idaho in 2008, Alaska in 2007, and Indiana in 2006. The name provided on the application is John Thomas Ruane. He provides the names of three individuals to serve as references. In doing so, the applicant signs a release authorizing the references to supply requested information. He also signed paperwork required under the Fair Credit Act to authorize the facility to complete other aspects of a background check. One of the references responds saying, “I have known J.T. Ruaneiz for several years. We worked together overseas and more recently a few years ago. He is fun-loving most of the time. Sometimes he has a short fuse.” Concerned that the surname was spelled differently and the passing indication of potential anger issues, HR decided to delve more fully into the

background of the applicant. Running a detailed criminal background check and following up on information supplied by another reference taken from a Web 2.0 applications, it is determined that J.T. Ruaneiz is also known as J.T. Ruane and J.T. Runanney. Mr. J.T. Ruanney had a string of convictions for assault, the most recent of which was in 2002 in Illinois. Under applicable state law, a person with a history of crimes against the person is precluded from working with vulnerable adults.

Should social networking be used as a tool in credentialing? Should such information be used as part of the hiring process? How much credence should be placed on social networking information? What if the information was posted as part of a prank, or by a computer criminal (cracker)? Suppose the information cannot be corroborated?

There are other questions to ask about such practices. What if the information found on social networking sites *is* accurate? For example, in the “professionalism case” did it help to identify a care provider whose behavior did not fit the culture of the organization? Would the situation have been different if the care provider had manifest a pattern of posting derogatory statements about patients, fellow care providers, or particular religious or racial groups?

From a risk management standpoint, using social networking as a vetting tool requires legal advice and a comprehensive plan for purposes of credentialing and employment screening. A haphazard approach would not suffice, especially if it could be demonstrated that certain individuals were selectively singled out for such scrutiny without a rational basis for such action.

A delicate balance is in order when using social networking data to scrutinize would-be employees or applicants in the credentialing process. It would be difficult to justify using unrelated information found on a social networking site as the basis to cast doubt on an individual in terms of professionalism or the ability to carry out employment responsibilities.

Furthermore, corporate use of some social networking sites for the purposes of pre-employment screening may violate the terms of use of the site, with potential civil and criminal penalties.

Knowledge is a Burden.

A principle often impressed upon healthcare risk management professionals by a leader in the field is that knowledge is a burden.⁸ Why is this statement significant? If a person or a healthcare institution has seen information on a social networking site that impacts safety, patient care, or the well-being of staff, then that individual or facility cannot deny such knowledge. If the individual is in a position that requires him or her to take action based on such knowledge and if he or she fails to do so resulting in foreseeable injury or death, then the foundation may be set for a claim of negligence.

Having a “knowledge burden” carries with it considerable responsibility. It imposes an obligation to take appropriate action. Depending upon a person’s work within a healthcare organization, this responsibility may involve notifying a supervisor or someone higher up in the chain of authority.

Social networking data has created something of an irony. A decade ago such a responsibility may not have existed. Medical students and others did not have Web 2.0 vehicles at their disposal through which they could post compromising photographs, lewd or suggestive remarks or private patient information. Today, the data left online may be accessible “forever.” It may be cut and pasted to a different social networking location leaving a trail of embarrassing or unprofessional commentary that may haunt an individual throughout his or her career.

While the information online may help to curtail risk prone behaviors, it also creates another liability exposure: the consequences of failing to taking reasonable, prudent, and appropriate action when one knew or ought to have known that such a response was required in the circumstances. In essence, Web 2.0 is the latest version of the adage, “knowledge is a burden.”

Social networking may also allow employers to learn more about prospective employee’s other activities, politics, interests, and intimate relationships. While the viewer may characterize such information as evidence of “unprofessional conduct,” it may constitute the exercise of free speech. That the viewer disagrees with such communication should not serve as a pretext for inappropriate or discriminatory action. This is especially important with information discovered through social networking that involves individuals who are part of a protected class under state or Federal law. A similar line of reasoning would follow with respect to job action or credentialing action taken against a provider or professional based on use of social networking data.

Risk Management Strategies for Healthcare Use of Social Networking.

Social networking use in the healthcare field presents a good opportunity for enterprise risk management (ERM). Some practical ERM style strategies include:

1. Identify Permissible Uses for Social Networking in the Healthcare Organization.

Assemble an enterprise risk management-style team to develop a list of permissible uses of social networking resources for the healthcare organization. Consider including the Compliance Officer, the Chief Privacy Officer, and representatives from security, credentialing and risk management.

2. Complete a Vulnerability Analysis.

Ask the ERM team to complete a social networking vulnerability analysis for the organization. Include in this evaluation privacy and data breach, botnets, trojans, viruses, worms, and other malware penetrating or crippling functionality of the healthcare organization IT system. Set priorities for process improvements based on the results of the social networking vulnerability analysis.

3. Develop A Social Networking Policy and Procedure.

Ask the ERM team to help develop a social networking policy and procedure for the organization that includes key components such as:

- Access authority.
- Use authority.
- Setting privacy thresholds on social network sites.
- Limits on information and photographic images that may be posted on and disseminated through social networking sites by employees or agents of the healthcare organization.
- Logs.
- Communication of Web 2.0 information in the organization.
- Reporting of impermissible use.
- Reporting inaccurate information found in a social network setting.

4. Identify Permissible Social Networking Users.

Establish a list of users within the healthcare organization who may have access through the healthcare organization IT system to various social networking sources. Review the list on a regular basis and

disseminate updated user information that can be expected with employee turnover in a healthcare organization.

5. Implement Enterprise Level Social Networking Access Permission Documents.

Develop appropriate notification in the medical staff bylaws and credentialing applications about the use of social networking sources as part of the verification process. Work with legal counsel to include in credentialing and recredentialing applications permission statements for accessing and using social network information. Take a similar approach with respect to employment applications. Make certain that the social networking sites that the healthcare organization intends to access for screening purposes permit data to be used for such purposes. Given the frequency of change in privacy policies and terms of use among social networking sites, check to see if a restrictive “term of use” can be relinquished by a person who voluntarily posts his or her information to a social networking location, Ask legal counsel to design a practical notification and permission process that is consistent with applicable federal and state employment law. Work with legal counsel to develop a framework for corroborating information gleaned from social networking resources as a prelude to using such data in any credentialing or pre-employment review process.

6. Implement Appropriate Information Technology Safeguards.

Look to IT and HIM colleagues as a resource for designing and implementing effective information technology requirements for use of social networking information in the healthcare organization. Consider respected external resources such as HIMSS, AHIMA, and SANS. Include in the safeguard measures a framework to address possible e-Discovery of social networking transactions and data under applicable state and Federal law.

7. Institute Enterprise-Wide Education on Social Networking.

Provide enterprise-wide education on the proper use of social networking information. Include those at the board level, senior management and line management as well as members of the medical staff. Encompass in education programs medical students, medical residents, students doing practicums and agency personnel.

8. Test and Monitor for Social Networking Compliance.

Ask IT colleagues to implement a process for testing for compliance with the social networking policy of the healthcare organization. Include in this process monitoring and, if necessary, use of external sources to fulfill this part of the process.

9. Take Prompt Action on Social Networking Non-Compliance.

Follow the requirements of recent FTC⁹ and DHSS¹⁰ regulations dealing with data breaches that may stem from protected patient information being disseminated from the healthcare organization to social networking sites.

10. Provide Patient and Family Warnings on Social Networking.

Offer cautionary warnings to patients and families about posting personal health information on social networking sites. Go further, offering suggested “do’s” and “don’t’s” about what should and should not be mentioned, including data about sensitive diagnostic information, anticipated time that a person will be out of his or her home, and comprising photographs. Incorporate this information in a statement or brochure on “Social Networking Etiquette for Patients and Families.” Recognize that such a document should address taking and posting on a website unauthorized photographs of staff, medical or nursing students.

Conclusion.

Social networking is a growing trend in the evolution of telecommunications. Although some may see it as a waning fad, others realize the power of Web 2.0 tools in commerce and the healthcare industry.

Social networking is a work progress. As it evolves, it will be necessary to adjust processes, systems, policies, and procedures for the effective and legitimate use of this technology in the healthcare field. Education is essential for users of the technology, including patients and family members.

An essential component will include readiness to address non-compliant practices. Liability risk exposures do exist from inappropriate practices in social networking. However, like other emerging technologies, the risks can be identified and treated effectively, especially if healthcare organizations take advantage of enterprise risk management strategies.

If you would like assistance with developing an enterprise risk management program, please contact us at (860) 242-1302.

¹ K.C. Chretien, S.R. Greysen, J.-P. Chretien, and T. Kind, "Online Posting of Unprofessional Content by Medical Students," JAMA 302(12): 1209-1315 September 23/30, 2009.

² Id.

³ Id.

⁴ Press Release, "Attorney General Cuomo Announces Legal Action Against Social Networking Site That Raided Email Address Books, Stole Identities, And Spammed Millions Of Americans," July 9 2009, accessed at: http://www.oag.state.ny.us/media_center/2009/july/july9a_09.html

⁵ "Web 2.0 Woe: 2009 Sophos Threat Report" July 22, 2009, from <http://www.sophos.com/pressoffice/news/articles/2009/07/threat-report.html>

⁶ "Random Burglary or Twitter Consequence?" retrieved from AllBusiness.com, St. Louis Dispatch. July 19, 2009 from <http://www.allbusiness.com/technology/software-services-applications-online-security/12571572-1.html>

⁷ "Forty-five percent of Employers Use Social Netorking Sites to Research Job Candidates." August 19, 2009, accessed from http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?id=pr519&sd=8%2f19%2f2009&ed=12%2f31%2f2009&siteid=cbpr&sc_cmp1=cb_pr519_&cbRecursionCnt=1&bsid=76ef5b042d8c4c86bb29b600faeb6bd2-307700958-R1-4

⁸ The statement is ascribed to Ellen Barton, a Past President of the American Society for Healthcare Risk Management and the person for whom the ASHRM Module Education Certificate Program is named.

⁹ Health Breach Notification Rule, Final Rule, Federal Register 74(163): 42739-4277, August 25, 2009.

¹⁰ Breach Notification for Unsecured Protected Health Information; Interim Final Rule, Federal Register 74(162) 42739-4277, August 24, 2009.