Social Media in Healthcare:
Privacy and Security Considerations
By
The HIMSS Privacy and Security Committee

"Social Media" in Healthcare

Introduction

The growing use of new technologies, applications and platforms, such as "social media," is creating new opportunities for healthcare organizations but is also raising privacy and security challenges.

Increasingly, healthcare organizations will need to adapt old policies and procedures, as well as privacy and security protocols to cover these new channels of communicating and sharing data. This paper will explain these social media technologies and platforms, the challenges that arise, and provide strategies as to how these can be used effectively, while protecting the healthcare organization from risk and respecting a patient's individual privacy. Two generic policy examples will also be provided.

Definition of Social Media

"Social media" is the process of people using online tools and platforms to share content and information through conversation and communication. Social media is typically used by individuals and organizations for the following purposes:

- Deliver pre-developed content - individuals or organizations may have existing information, data or other types of communications that they want to deliver to users, customers and/or associates for which social media mechanisms might be more engaging or expedient than, say, sending an email or posting on a website. Social media mechanisms provide a convenient channel to many individuals/customers and allow for dialog and interaction. Some examples of information or content include:
    - Personal communication
    - Factual/educational
    - Opinion
    - Entertainment
    - Marketing (for example, brand awareness, managing Google "rankings" and web hits, selling products)

- Engage population in discussion - organizations can facilitate brand awareness/ customer satisfaction, and/or connect with individuals or business partners by simply engaging them in interactive dialog through social media such as:
    - Collaboration
    - Reviews
    - Opinions
- Manage communications - social media can offer individuals and organizations a convenient, organized way to consolidate and manage their communications with:
    - Friends, family
    - Customers

Platforms/Applications/Examples

There are many commercially available platforms and applications for use by the general public and by organizations. Table 1 provides some examples and discussion of their function and common uses.

Type	Function	Example(s)	Common Uses
Blog (shortened version of the term "web-log")	Allows users to generate and post their own content, which they can share with anyone Content can be posted on a website or on specialized blog posting sites	• Individual blog • News blog • Organizational blog	• Share opinion, like an op-ed piece • Generate discussion on a topic • Establish subject matter expertise • Facilitate brand awareness
Social Networking Site	Allows users to create a personal profile, connect with others, exchange messages, and join common-interest user groups/sites	• Facebook • MySpace • Google+ • Doximity (for physicians)	• Network with preselected group of friends/acquaintances • Share personal information, pictures, news events, etc. • Messaging • Business pages
Short Networking/Blog Site	A networking/blog site that allows users to communicate with each other and share information through short messages	• Twitter (messages are called "tweets" and are 140 characters or less)	• Post personal or business-related news announcements • Express opinion or observation • Provide links to websites and/or other

			information sources
Media Sharing Platform	Allows users to view and share videos and other media with a global audience	• YouTube	• Share videos • Share marketing-related information • Post information, interviews, news bites, etc.
Podcast	Allows users to access a type of digital media consisting of files (either audio or video) to which they subscribe and download through web syndication	• Various platforms/ applications	• Short videos • Interviews • Marketing-related materials • Repurposed web content (such as summary of a white paper)
Business Networking Site	Allows users to network and message, used mainly for professional networking	• LinkedIn	• Share business-related personal information • Professional networking
Text	Allows the exchange of short, text messages between fixed line or mobile phone devices. Also called SMS (Short Message Service)	• Various platforms/ applications provided by phone, web or mobile communications systems vendors	• Short, point-to–point or person-to-person communications • Typically used for personal communications • Increasing business use
Wiki	Website that allows users to add, modify, or delete text/content via a web browser	• Web-based Wiki software such as MediaWiki	• Knowledge management, document management and note-taking • Community websites • Other collaborative uses

Table 1 – Social Media <u>Platforms/Applications/Examples.</u> There are many types of "social networking" platforms, applications and mechanisms that allow users to communicate with others.

<u>Current Uses in Healthcare</u>

Much like the general population and other businesses, healthcare organizations are increasingly using social media. Example uses in healthcare include:

- <u>Managing conversation/interaction between providers and patients</u> (individual or population)
- <u>Marketing/brand management</u> – many healthcare organizations advertise their services, offer health resources, conduct interactive discussions, etc., using social media in order to enhance

patient satisfaction and/or attract new patients. This type of activity facilitates awareness of the organization's name and/or brand as well.

- Manage Google rankings, web hits – healthcare organizations spend some IT and/or marketing resources creating a website and/or patient portal. The organization also would like its name, brand or website to be listed when an individual patient does an internet search (using Google's or other online search engine) on a medical condition or a particular health service. Participation in social media activities by the organization can increase the likelihood of the organization being listed by the search process, as it increases the presence of the organization on the internet.

- Engage e-patients – patients are increasingly technology-savvy and many are already engaged in online and social media activities. A commonly used term for these patients is "e-patients," or those that are engaged electronically in a significant way. An organization can benefit in using social media technologies to reach already engaged e-patients.

- Promote wellness – social media provides a way to communicate with patient populations regarding wellness information, activities, and tools.

- Professional collaboration – social media tools, such as Doximity for physicians (see Table 1) facilitate secure professional collaboration.

- Consumer, patient, professional education – Blogs, media sharing platforms, podcasts and other social media mechanisms provide engaging platforms to deliver educational materials.

- Clinical trial recruitment – many research organizations are now using social media to reach potential research participants.

- Workforce recruitment – recruiting employees is a very important activity for healthcare organizations. Social media, such as LinkedIn or other professional networking platforms, is being used for this purpose.

Challenges for Healthcare Organizations

Ethical Challenges

According to the Merriam-Webster dictionary, the term "ethical" is defined as – "conforming to accepted standards: consistent with agreed principles of correct moral conduct.[1]"

The practice and regulation of Healthcare ethics date back to the early 1800's with the development of the Hippocratic Oath and the Nightingale Pledge. Ethical focus continues in healthcare with the regulatory and legal requirements mandated by Title II of the Health Insurance Portability and Accountability Act of 1996 (HIPAA); Sarbanes-Oxley Act of 2002 (SOX); The National Center for Ethics

[1] http://www.merriam-webster.com/dictionary/ethical

in HealthCare (NCEHC) launched in 1991; and the launching of the World Health Organization Ethics and Health Initiative in 2002. Social media utilization in healthcare brings with it ethical challenges on which to focus.

Misconduct or unethical behavior by employees is a serious issue with respect to any entity's employees' use of social media. The 2011 National Business Ethics Survey,[2] incorporating a look at employee use of social media for the first time, identified the following key findings relating to social media:

- Active social networkers report far more negative experiences in their workplaces. As a group, they are much more likely to experience pressure to compromise ethics standards and to experience retaliation for reporting misconduct than co-workers who are less involved with social networking.
- Active social networkers show a higher tolerance for certain activities that could be considered questionable.

There may be an opportunity for corporations to work with active social networkers in ways that they have not yet fully explored. Active social networkers are somewhat more likely to use social networks to say positive things about their company and co-workers, than to post negative feelings.[3] In her article, "7 Social Media Mistakes Made in HealthCare,[4]" Susan Giurleo, PhD, made several key points that need to be considered with utilization of social media. She stressed that "social media is free and open access and social media puts all of us on an equal playing field." In the age of electronic advancement in the healthcare environment, the utilization of social media will continue to expand among healthcare providers and organizational team members will need to address the ethical challenges that social media presents. The social media mistakes identified by Giurleo as "Unethical Shenanigans" address:

- not breaching your clients' confidentiality online;
- not telling your client how to use social media - thereby misusing your position of power in the treatment dynamic; and
- avoiding the unethical trap of "Google-ing" clients.

The American Medical Association (AMA) also addresses considerations for physicians when utilizing electronic systems including social media.[5] These concepts are applicable to all healthcare providers in considering the ethical challenges of social media. A summary of these concepts and practices to employ to address ethical challenges of social media are:

[2] Ethics Resource Center. National Business Ethics Survey®. http://www.ethics.org/nbes/findings.html. Accessed August 13, 2012.
[3] Ibid.
[4] http://www.kevinmd.com/blog/2010/10/7-social-media-mistakes-health-care.html
[5] http://www.ama-assn.org/ama/pub/meeting/professionalism-social-media.shtml

- Be cognizant of standards of patient privacy and confidentiality that must be maintained in all environments, including online, and do not post sensitive patient information online or transmit it without appropriate protection.

- Use privacy settings to safeguard personal information and content to the extent possible, but realize that privacy settings are not absolute and that once on the Internet, content is likely there permanently.

- Maintain appropriate boundaries of the patient-physician relationship in accordance with professional ethical guidelines just as you would in any other context.

- Report unprofessional postings to appropriate authorities.

- Do not post any identifying information about your clients, patients, and affiliate care providers. This is a breach of confidentiality.

- Avoid searches on individuals that you relate with professionally; "Googling" can lead to a violation of privacy.

- Create a separate professional/business page in social media. Keep your personal page profile content, friends and responses separate.

There are significant benefits to utilizing social media in healthcare. With these benefits come the ethical and legal concerns about preserving patient confidentiality and protecting patient privacy. Employers need to understand that employee behavior is influenced by social media in ways that are not yet completely understood. Organizations should consider this issue as they codify policies and procedures on employee and organizational use of social media, and should train and monitor employee's behavior.

Privacy Challenges

HIPAA Privacy Rule and Security Rule

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") was enacted by Congress in order to improve the delivery of healthcare services in the U.S. Congress recognized that the movement of electronic data exchange in the healthcare sector posed a possible threat to privacy and accordingly, mandated that the U.S. Department of Health and Human Services ("HHS") promulgate regulations to protect the privacy and security of electronically-transmitted health information.

In December 2000, HHS created a set of rules to protect the privacy of personal health information known as the Privacy Rule. The Privacy Rule establishes national standards to protect individuals' medical records and other sensitive personal health information by requiring appropriate

safeguards, uses and disclosures, patient authorizations, and certain rights over their health information.

The HIPAA Security Rule was finalized in February 2003 along with the Privacy Rule. The HIPAA Security Rule establishes national standards to protect individuals' sensitive electronic health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of sensitive electronic health information.

It is important to note that the HIPAA Privacy and Security Rules are designed to establish minimum standards for the purpose of setting the "legal floor." States are free to develop more rigorous requirements as long as these requirements do not conflict with HIPAA. Each covered entity under the Act is, therefore, required to consider all state healthcare privacy and security laws, and to operate with these laws even if they exceed the HIPAA standards.

The Evolution of Privacy and Technology in Today's Culture

During Colonial times in America, privacy concerns were addressed by finding an open field to have a private conversation to protect against "snooping." In the 1800's, privacy concerns were focused on the advent of the telegraph and the press becoming "invasive." In the 1900's, technology drove many of the privacy issues domestically and globally. Between 1900 and 1965 the first "bugging" devices, telephone communications over wires, and the constitutionality of searching electronic conversations raised privacy concerns that were only heightened by the Cold War, prompting increased government surveillance of civilians without their consent or knowledge.

The latter part of the 20th century brought the birth of the Internet, the personal computer, and public-key encryption. Government and social concerns were raised by the advent of sensational journalism and the Watergate scandal. The Privacy Act of 1974[6] established Fair Information Practices (FIPs) and the issue of privacy began to be shared on a national scale resulting in the development of data and privacy protection laws. Technologies such as AOL, Netscape and email began to increase the consumer use of the Internet and dominate technology and privacy issues near the end of the millennium.

The trends have continued in the new millennium. New technologies such as blogs, YouTube, and Facebook continue to create an online "Reality Show" generation. Additional technologies such as cloud computing, public Wi-Fi, retail loyalty cards, smart phones and electronic medical data exchanges are changing the landscape for information privacy and security.

Locks and bank vaults are no longer the primary forms of protection in the United States. Today, information security professionals are waging a different kind of war, focused on the protection of sensitive personal, private health information from threats caused by hackers, malware, spyware,

[6] Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896, enacted December 31, 1974, 5 U.S.C. § 552a

viruses and cookies. Concerns over employee theft of PII, PHI and intellectual property need to be addressed.

Recent and Relevant Cases and Examples of Social Media Concerns

The availability of medical data due to electronic medical records combined with the increased use of social networking poses challenges to the healthcare community. In 2009, ABC News reported that 13% of medical students are sharing sensitive health information regarding patients on blogs or social networking websites.[7] Reports of nurses and physicians posting x-rays and pictures on Facebook pages are an alarming trend. A more recent study by the Journal of Medical Internet Research[8] found that 24.1% of physicians used social media daily to scan or internet search engines for medical information.

The Canadian Broadcasting Corporation (CBC) conducted investigative research after learning of a woman in Canada who lost her medical benefits due to research conducted using Facebook.[9] The insurance company found that the woman posted pictures of herself at a bar show, birthday party, and on a sun holiday. When the CBC contacted the insurance provider, they said they would never cancel benefits based on just a few Facebook pictures, but they did confirm that they use Facebook as a source of investigating insurance fraud.

Security Challenges

The Social Media Information Security Problem for Healthcare Organizations

The implications on communicating in healthcare using social media are numerous. Networks represent many-to-many relationships. The links from a single person to others can be so numerous that it would be impracticable to trace the network of relationships. Moreover, an individual's network is likely an amalgamation of friends, acquaintances, co-workers, and friends of friends with whom they share no common interests. And let's not forget, each individual in the network has their own collective network of relationships with which they can share information. Individuals have become empowered to communicate. From a networking perspective, this is extremely effective. But where we typically applied rules for the information we shared (sensitivity of the information, ownership of the data/copyright) and the people we shared it with (need to know), we now treat the network as a single entity, sharing with everyone equally, unless of course we understand and apply stringent privacy settings. Social networking concepts seem to run contrary to privacy and security requirements, providing everyone with equality in communications.

[7] http://abcnews.go.com/Technology/AheadoftheCurve/medical-students-leak-patient-info-facebook/story?id=8650491
[8] http://www.jmir.org/2012/5/e117/
[9] http://www.cbc.ca/news/canada/montreal/story/2009/11/19/quebec-facebook-sick-leave-benefits.html

Information Flow

Data transmission is expedited in social networking sites. Once information is released, in any form, it is released to the entire set of connected entities. This is unlike other mediums. For instance, when you send an email, it only goes to those listed on your distribution. Some email systems allow you to prevent forwarding or copying an email to avert further dissemination. Social networks act more like group "listserves,[10]" where everyone can see the same information even when it does not pertain to them.

We often call this challenge "data leakage." Through social media channels, employees can inadvertently or purposely disclose (leak) patient or company sensitive information, make comments that damage the corporate brand or increase liability exposure, or otherwise take actions that expose sensitive patient, company, personal or other information.

Persistency

Digital information can be copied and can be stored indefinitely. While the user may not have intended for the data to be copied, forwarded, or stored in other systems, this can and does occur. The data could be sensitive patient information. The problem is compounded by the numerous links (relationships) and nodes (other networks) along which the data can travel and upon which it can be stored.

Authenticity

People assume that the information in their network comes from trusted reliable sources. But human nature tells us something else – people love to gossip and embellish. A 2009 report in the Journal of the American Medical Association provided significant insights into the behaviors of medical students' use of social networking sites and blogs. Of the 78 U.S. medical schools surveyed in the report, 60% of them "reported incidents of students posting unprofessional online content."[11] "Thirteen percent of the deans cited violations of patient confidentiality."[12] People invariably trust the relationships in their network. They want the information they are passing to be interesting and sound smart. Human behavior takes over and people go too far. The opportunities for violating patient confidentiality have moved from the healthcare setting, where actions can be monitored and managed, to cyberspace, where the compromise can propagate at epidemic rates, and at least at this point, where there is little understanding of implication on the Health Insurance Portability and Accountability Act (HIPAA).

---

[10] The term **"**listserv**"** has been used to refer to a few early electronic mailing list software applications, allowing a sender to send one email to the list, and then transparently sending it on to the addresses of the subscribers to the list. http://en.wikipedia.org/wiki/LISTSERV

[11] http://jama.jamanetwork.com/article.aspx?articleid=184624

[12] Report on Patient Privacy", Volume 9, Number 12. http://www.aishealth.com/

Summary

The security challenges identified above will have negative impacts to the confidentiality of the data and the privacy rights of the individual. "The HIPAA Privacy Rule provides federal protections for sensitive health information held by covered entities and gives patients an array of rights with respect to that information. At the same time, the Privacy Rule is balanced so that it permits the disclosure of sensitive health information needed for patient care and other important purposes."[13]

But the primary burden of ensuring that the Rule is applied is placed squarely on the shoulders of the healthcare workforce including volunteers, contractors, and business associates. It's also important to point out that there may be other areas of consideration with respect to social media use in related to Payment Card Industry Data Security Standard (PCI DSS), Red Flags Rule, and others.

Social networking tools distance individuals from their legal responsibilities, leaving them to apply moral judgments. The space on social networking sites where individuals operate do, after all, belong to them, not to the covered entity. So how do CE's manage the risk associated with these tools while recognizing and accepting their application to the work space? Most, even in the federal government, are implementing policies, procedures, rules of behavior, and in many cases, governance over the tools (see Policy section, below).

Legal/Liability

Social network sites can also be liability minefields, exposing companies to risks as diverse as copyright infringement, consumer fraud and discrimination. Employers can be held liable for the unsupervised activities of their employees on social media network sites.[14] Organizations should have written policies and procedures on employee and organizational use of social media, and should train and monitor employees. Organizations can also consider liability insurance to mitigate risk in this area.

Operational Challenges

There are many benefits to planned use of social media by healthcare organizations. However, poorly managed social media outreach can cause serious damage to the reputation of the entity and its relationship with its patients and the community at large. Here are some real operational challenges to consider:

- Ability to be responsive/bandwidth – organizations that become active with social media normally do so with specific objectives in mind – whether it's interacting with patients, marketing, etc. These external parties generally expect two-way interaction with the

[13] U.S. department of Health and Human Services; Understanding Health Information Privacy: http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html

[14] Bradford, D. Online Social Networking: A Brave New World of Liability. https://www.advisen.com/downloads/SocialNetworking.pdf. Accessed August 13, 2012.

organization. Therefore, organizations should implement a planned project, with specific objectives and responsibilities assigned to individual employees. In this way, the organization can monitor progress against objectives and ensure that the needs of external parties/individuals are met and response times are actively managed.

- Control/monitoring employee behavior – as mentioned above, with the use of social media, there is a risk that employees can purposely or inadvertently leak sensitive company information, use social media for nefarious/illegal purposes, compromise the company brand and/or create liability issues.

  Therefore, organizations should put in place a program of social media policies and procedures relating to employee use of social media, provide training, and actively monitor employee behavior as it relates to company policies. Retraining and/or sanctions should be used with employees as a deterrent to unauthorized behavior.

- Inviting negative comments/feedback – with any social media mechanism that invites participation from external entities, there is a risk that negative comments/feedback or other negative exposure could be contributed. Organizations need to evaluate this concern in planning its use of social media mechanisms and consider controls such as having a moderator approve external party data/comments before posting or ongoing review and removal of offensive, criminal or overly negative contributions.

- Dominance of the loud and opinionated – in addition to eliciting negative comments/input, social media provides an opportunity for external parties to dominate discussions/forums, etc. While the input may not even be overly negative, this can result in other external contributors feeling bullied, neglected, and/or frustrated in not having their voice heard. Organizations should consider how to manage external party input to achieve their objectives while providing a positive experience for all external participants. Mitigating strategies such as a moderating function or review/removal of content can be considered.

- Ownership of data – the question of "who owns the data" or the information contributed to social media interactions (whether it be the organization or the external party) is still under debate in the online community. It is hard to apply copyright, patent, and trade secret law to information that is in digital form and highly sharable. Efforts to define who owns a piece of data under what circumstances and thereafter control copying and sharing have been difficult at best.

  At least for the time being, consider that when sharing data/information via social media mechanisms, assume it is difficult if not impossible to control dissemination and use. Hence, organizations should consider the risks associated with data ownership challenges for both company and external party contributions when creating its social media strategy, projects and policies and procedures.

Social Media Policy

A very important component to addressing risks associated with social media is developing a set of social media policies. One policy should be focused on the human behavioral aspects of social media and another policy should be focused on how the organization plans to use social media.

A behavioral policy should describe what social media activities employees are prohibited to do, such as discussing a patient, exposing confidential data over a social media medium, etc. When creating the behavioral policy, organizations should involve key stakeholders from across the organization to ensure that a well-rounded policy is developed. For starters, an organization should at a minimum involve their legal, privacy/compliance, and human resources teams to incorporate their perspectives. Involving these teams means that not only will your policy be sound from an IT perspective but also sound from the legal/compliance/HR perspective as well. Once the policies are developed, on-going involvement with these stakeholders will be necessary as organizations will want to monitor and update their policies as the legal landscape concerning social media evolves.

A second policy should address how to leverage social media to further the company's strategy. When creating a social media use policy, the most critical teams to involve will be the sales/marketing/communication teams, which will provide perspective on how they see the organization leveraging social media. Such a policy should set the overall bounds of how social media shall be used by the organization including activities such as creating an organizational Facebook page and a campaign to increase wellness, or driving consumers to the organization's services.

When setting policy, organizations need to remember that these are public forums which carry certain constitutional protections, and as such should consider those boundaries before taking a "you have no privacy" approach with their policy.

In summary, social media is here to stay and will continue to grow. As such, organizations need to determine how to utilize them in a secure and private manner. Developing social media policies will be an important element in this process. These policies should address social media use at the individual and organizational level. Training and educational resources should be available to help employees understand these policies and how social media activities should be conducted. Using this approach allows an organization to say "yes, we can" use social media in our organization.

Some questions to consider when creating your policies are:

1) Can we make this policy operational?
2) Can we truly police this policy?
3) How will we know this policy is effective?
4) Are we ready to sanction individuals who violate these policies?

For an example of the following policies please see the Appendices:

1. Social Media Use by Workforce – Appendix A
2. Use of Social Media for Official Company Business – Appendix B

Risk Mitigation Strategies for Social Media

Risk Mitigation can be described as the systematic reduction in the extent of exposure to a risk and/or the likelihood of its occurrence. Risk mitigation relating to social media is unique because so many of the risk factors are beyond the control of the business.

CASE STORY EXAMPLE

A disgraced Portland nursing assistant has been banned from Facebook and other social media sites after posting a photo of a dying patient's buttocks.

In addition to being fired from her job, the assistant also spent eight days in jail and had her nursing license revoked following a two-day trial.

Convicted of invasion of personal privacy, the assistant was found to have posted graphic photos of patients on Facebook and to have written derogatory comments about them.

http://articles.nydailynews.com/2012-03-07/news/31133978_1_social-media-sites-facebook-graphic-photos

In Deloitte LLP's 2012 Ethics and Workplace Survey[15] it was reported that 53% of employees believe that their social networking activity is none of their employer's business while 60% of executives state the organization has a "right to know" how employees portray themselves and their organizations online. Thirty percent acknowledge informal monitoring practices. Finally, 49% of employees indicate that even if there was a policy in place, it would not affect their behavior.

Today, social media is ubiquitous in the corporate environment. Nearly every provider has some kind of social media presence - - inside and outside of the organization. These sites and these activities, however, lack consistent management, control or policy. Most organization's control approach falls into one of four practices:[16]

1. No policy
2. Block everything (works only within the corporate network)
3. Limited access, or
4. Controlled access

[15] http://www.deloitte.com/view/en_US/us/About/Ethics-Independence/
[16] http://www.isaca.org/Education/Upcoming-Events/Documents/2012-NACACS-Presentations/246-nac2012.pdf

Totally blocking access to social media sites is not sufficient to prevent their use since many organizations legitimately use the tools to interact with patients, families or prospective patients and employees. Also, blocking access does not preclude the use of social media by employees on employee-owned equipment and/or personal accounts.

Alternately, by doing nothing, organizations increase their legal risk because no clear guidelines articulate how staff should participate in social communities, how doctors share medical advice on blogs and where patients get medical information.

Although a complete prohibition might seem to be the simplest solution to deal with the security risks in social media, it is not necessarily the best approach because it doesn't actually address the problem - - it simply moves it further from the organization's control or ability to monitor. Thus, management and mitigation, not prohibition, is the best response to social media security risks.

While all businesses face risks around social media including loss of control over content, brand/reputation loss, negative publicity, identity theft and impersonation, healthcare is unique in that risks include patient privacy and regulatory compliance.

Social Media Risks Today

While no one can argue that social media technology has arrived and there is no turning back, we can't forget that it has arrived with a lot of risks. The risks presented by the pervasive use of social media come at healthcare organizations from two different directions. First, risks are presented by human behavior; secondly, of course, are the technological risks. When these two types of risks combine, it presents a formidable risk environment for management and information technology staff to address.

Social media is dangerous to enterprises exactly because it is "social." That implies that people will be sharing information. Unfortunately, that information also can be used by potential hackers or thieves to introduce additional risks. In some cases, the information being shared is simply private and confidential and shouldn't be shared, such as patient or employee information. The information may be inappropriate for public consumption, such as corporate announcements.

Social media sites are ripe for technological abuse by hackers and other disreputable users. As millions of users post links, content, pictures and more, it has become next to impossible for these site owners to keep track of what is legitimate and what is malicious. At the same time, users are accessing the sites via corporate computers, home PCs, and personal mobile devices that may lack adequate protection or have unsecured versions of web browsers. This means that when users do stumble on a bad link or malicious content, the bad guys are very likely to succeed in infecting the machine or initiating a broader attack.

Common Social Media Malware/Attacks[17,18]	Risk
Obfuscated Links	On many sites, URL shortening is normal. Attackers can entice users to click a link about an interesting topic and because the link is cloaked by a service like Bit.ly, they won't suspect it is a dangerous link.
Click Jacking	This tactic tricks users into revealing personal information with a sensational message or with transparent .gifs that hover over the "Like" button found on many corporate pages.
Malicious Codecs/Updates	A favorite tactic in this category is pretending to share a video and redirecting the user to a malware installer posing as an update to a browser plug-in or codec. Browsers and traditional AV is limited in stopping this kind of focused, personal attack.
Spear Phishing	Emails that seem to come from someone you know (like your bank) asking for information (like passwords). This technique now makes up nearly a quarter of all social media attacks.
Password Guessing	Are your secret password retrieval questions really that secret? A study by IEEE in 2009 found that 28 percent of those that simply knew and trusted an individual could often guess that person's answers to their account secret questions.[19]
Password Sniffing	If a hacker can access your password, his or her ability to steal more information only increases when people rely on the same password across multiple accounts.

Table 2 – Common Social Media Malware/Attacks and Risks. Social media can exploit system vulnerabilities and put your organization at risk.

Risks and Risk Mitigation Techniques

The process for developing risk mitigation strategy, policy and procedure is not unlike any other technology-focused risk management technique. It starts with a multi-step approach outlined here at a high level.

1. Perform a social media risk assessment

[17] http://www.lumension.com/Media_Files/Documents/Marketing---Sales/Others/3-Step-Guide-to-Safe-Social-Media.aspx
[18] http://blog.lumension.com/3964/keys-to-the-kingdom/
[19] http://www.technologyreview.com/news/413505/are-your-secret-questions-too-easily-answered/

The risk assessment, like any technology risk assessment, should identify the risks to the organization from the use of social media. Assessing the risk of identity fraud for organizations relying on personal data for identity verification is critical. While organizations face different types and levels of risk when engaging in social media, the steps to mitigate those risks tend to be fairly similar. To accomplish a social media risk assessment, a simple set of steps can be completed. These include setting up a kickoff meeting with client stakeholders, holding stakeholder interviews, and defining individual brand, regulatory, and infrastructure-level workshops. In addition, organizations can then compare benchmarks and best practices, analyze their findings, and prepare a final report and presentation for future implementation.

2. Develop an overarching, risk-based social media strategy consistent with organizational goals and objectives

   The first step toward securing the social media environment is to develop and implement a comprehensive, risk-based strategy. A social media strategy, should be built on existing privacy, security and risk policies and procedures and specify the process/approach for managing social media strategy, enable a governance structure including assigning roles and responsibilities, and create policy/education for the new governance approach. A team of representatives from all departments including legal, human resources, compliance, data security, IT and clinicians should be assembled to help shape and implement the social media policies.

3. Define a strategy to protect the organization's online reputation and brand from harm

   Social media has been shown to play an important role in how an organization's brand is perceived. Ad hoc approaches to engaging in social media and not involving all relevant stakeholders are a common risk. At least one employee should be assigned to monitor their organization's reputation. In addition, organizations should proactively engage on social network venues to understand how reputation can be impacted by the interactions. It is important that organizations build a process to identify new reputation risk elements as social media evolves.

   Healthcare organizations should also create an Internet reputation risk management plan. This plan will need to address what visitors to the social media site express, what their employees share on other sites and, most significantly, what things are said about the organization over which there is no direct control. By establishing, following and updating protocols related to addressing Internet-based negative reputation events you can make social-media chaos less risky to your healthcare organization.

4. Develop social media policies and procedures

   The organization's social media policy should be updated to address blogs, podcasts, and videos, as well as provide guidance for giving medical advice online. A strategy on how to blog and use Twitter, podcasts, mobile apps, and video should be developed to guide thought leadership

communication. Procedures should be developed that support end-users, making it clear what is and is not allowed and what the implications of violating policy and procedures may be. These may include terms of use/user agreements, employee code of conduct, disclaimers, community guidelines, privacy and security policies, legal and regulatory violations, copyright policies, antitrust policies, branding/trademark guidelines, blogging guidelines, and blog moderation policies.

5. Educate staff and volunteers

   Employees should be educated on the consequences of violating social media policies and guidelines for addressing and reporting potential incidents related to social media.

   Once the organization has approved the policy and procedures, it is important that the staff is up-to-date on those that relate to social media. Regular privacy and security training related to HIPAA/HITECH, as well as other relevant Federal and State laws, should also include specific social media risks. To ensure employees know how to conduct themselves online, a standard of conduct manual with appropriate disclaimers should be created.

6. Minimize regulatory and other legal/liability risks

   Write policies and procedures to make sure HIPAA and HITECH are addressed (protection of sensitive patient data) but don't forget other legal and regulatory issues, such as intellectual property, copyright and trademark infringement; PCI and Sarbanes-Oxley, not to mention applicable state law. Establish policies to ensure communications that include sensitive data is tracked and logged and use content filtering where appropriate.

7. Proactively monitor social media for compliance

   There are numerous ways to monitor social media in a healthcare setting. An important step in monitoring social media compliance is to check out exactly what the content looks like before exposing it to the rest of the world. Healthcare organizations should pay attention not only to their comments and postings, but also to the feedback being posted by others. Be alert for information that could be construed as defamatory or that could evoke offensive or overly negative comments, such as via a blog. Close attention should also be given to ensure copyright and intellectual property right infringements are not violated.

   It is critical that healthcare organizations define sanctions for noncompliance and ensure employees know them. Watch out for exceptions to policies. Granting too many exceptions tends to make exceptions the rule. Therefore, a policy to discourage exceptions should be created. And, to ensure organizations develop a consistent, repeatable process for compliance, a quarterly audit policy trickled down to department heads to ensure that they review how their direct reports spend time online should also be developed.

Risk mitigation monitoring should align with routine audit techniques so that risks are identified, control objectives are defined and activities that support those control objectives are also reviewed. The parties responsible for the activities should be held accountable for defining control objectives and assuring appropriate controls are in place.

As shown in Table 3, auditing social media will have controls around four key areas: 1) people; 2) process; 3) technology, and; 4) data.[20]

Generally, risks, mitigating controls, activities and responsible parties by area would address, but are not limited to:

Social Media Controls	Risks	Control Objectives	Risk Mitigation Activities/Techniques	Responsible Parties
People	Identity Theft, Loss of Productivity, Infiltration through Social Engineering, Social Media Policy Violations	Employees, volunteers, contractors, 3rd parties and business associates are aware of their responsibilities relating to social media	• Establish user agreements for social media use • Conduct awareness training to inform users of the risks involved in using social media websites • Use content-filtering technology such as Data Loss Prevention (DLP) • Manage and control access to social media sites	HR, IT, Security, Risk Management
Process	Regulatory Compliance Risk, Legal/Liability Issues (Copyright, trademark infringement, privacy issues), Reputational Loss, False Impression	The organization's brand is protected from negative publicity or violation of regulations.	• Establish policies to ensure legal/sensitive communications are tracked and archived • Monitor employee behavior/activity for adherence to Policy and Procedure • Scan the Internet for misuse of the enterprise brand	Legal, HR, IT, Information Security
Technology	Virus/Worms via Social Media Sites, Constraint of Network Bandwidth, Data Theft from Mobile Devices	IT infrastructure mitigates risks presented by social media	• Install anti-virus applications and encryption on all systems, including mobile devices, as needed and appropriate • Use content-filtering technology such as Data Loss Prevention (DLP) software • Limit access to social media sites during business hours, if practical and appropriate. Install gateway security devices or services to prevent access to known "bad" sites in order to reduce risks from	Information Security, IT

[20] http://www.isaca.org/Education/Upcoming-Events/Documents/2012-NACACS-Presentations/246-nac2012.pdf

			URL shortening abuse (URL filtering)	
Data	Improper Content, Unauthorized Disclosure, Intellectual Property leakage	Organization's information is protected from unauthorized access or leakage through or by social media	• Establish user agreements for social media sites • Develop policies on the use of enterprise-wide intellectual property • Ensure capability to log all the communications	Legal, HR, IT, Security, Risk Management

Table 3 – Social Media Controls. Social media controls can help your organization mitigate risk.

Summary

We know that organizations will need to adapt old policies, procedures, privacy and security protocols and work to mitigate the risks related to these new channels of communicating and sharing data – "social media" This paper has explained common social media technologies and platforms, the challenges that arise, and provided strategies as to how these can be used effectively, while protecting the healthcare organization from risk and respecting patient's individual privacy.

In order to address the practical implementation, the HIMSS Privacy and Security Committee has provided two generic sample policy documents, as well as a list of social media-related resources. These may be found in the Appendices.

Summary Guidance –

The "Do's and Don'ts" of Provider Use of Social Media

DO - "Engage and Educate"

- have policies and procedures for your organization
- train your staff, monitor employee behavior
- know where social media is being used – departments and people
- use social media to share information that promotes quality healthcare and up-to-date medical information
- recognize that you represent your profession and/or organization

DON'T - "Diagnose or Treat"

- discuss individual patient's illnesses, medical conditions, or personal information online
- share confidential information about patients or the organization
- give clinical advice or diagnosis
- let questions, inquires, and posts go unanswered
- let just anyone speak for your organization

Appendix A: Sample Policy - Social Media Use by Workforce

Introductory Note: *The sample social media policies below are examples of policies that are being used by a health system to manage social media use in its environment. It is only an example and is not meant to be a complete or exhaustive list of policy elements. Because organizations, along with regulatory and legal requirements, are different, each organization should develop unique policies that are aligned with the needs of the organization, applicable laws, and is consistent with its policies and procedures.*

Purpose:

To describe the appropriate use of Social Media by XYZ Health System Workforce regarding XYZ Health System-related content.

This policy applies to any member of the XYZ Health System Workforce who use Social Media for personal purposes and posts XYZ Health System related content, whether during or off work. It applies to the use of Social Media when away from work, when the Workforce member's XYZ Health System affiliation is identified, known or apparent. It does not apply to content that is unrelated to XYZ Health System.

Policy:

A. XYZ Health System expects its employees to reflect the organization's core values when posting content about XYZ Health System in any Social Media. This rule applies to all Social Media postings, even those on personal sites or pages, such as Facebook. All XYZ Health System employees are personally responsible for their posting on Social Media.

B. XYZ Health System employees must comply with all laws and regulations that apply to them as XYZ Health System employees when they post on any Social Media.

    a. All XYZ Health System employees are prohibited from disclosing on any Social Media site any Protected Heath Information (PHI) or Personally Identifiable Information (PII) they have obtained through their work at XYZ Health System.

    b. All XYZ Health System employees are prohibited from disclosing any of XYZ Health System's Confidential or Proprietary Information on any Social Media site.

    c. All XYZ Health System employees are prohibited from engaging in any unlawful discrimination or bullying of other XYZ Health System employees through postings on any Social Media.

    d. All XYZ Health System employees must refrain from violating the privacy rights of XYZ Health System's patients, members and visitors by posting a photo, image or description of the patient, member or visitor on any Social Media site without consent of the patient, member or visitor. Privacy rights can be violated if the posting on Social Media contains enough detail so the patient, member or visitor can be identified even if the person's identity is not expressly stated.

C. XYZ Health System employees may not disparage the services and care XYZ Health System patients and members receive in postings on Social Media. This violation is more serious when patients and members have access to the Social Media posting, such as when patients or members are "friends" on an employee's personal Social Media site or page, such as a Facebook page.

D. XYZ Health System employees must obtain advance approval to use official XYZ Health System logos, photos, videos or images on personal Social Media sites or postings.

E. Contractors and vendors performing services for XYZ Health System are subject to the rules and prohibitions of this policy when posting XYZ Health System related information on any Social Media site.

Enforcement:

XYZ Health System Employees: Conduct deemed in violation of this policy may result in corrective action up to and including termination of employment. Human Resources will assist decision-makers in determining corrective action.

Contractors and Vendors: Conduct deemed in violation of this policy will result in a XYZ Health System request that the contractor be immediately removed from XYZ Health System property and from XYZ Health System related work or the termination of the related XYZ Health System contract.

This policy shall be interpreted and applied in a manner as to comply with all applicable laws.

Definitions:

Confidential Information: XYZ Health System employee, customer, patient and proprietary information that is not generally available in the public domain. This is the default level for all information under XYZ Health System custody and control except that information specifically declared to be either Public or Restricted. Examples of Confidential Information include, but are not limited to:

- Protected Health Information (PHI) and Personally Identifiable Information (PII)
- Passwords
- Operating methods
- Marketing tactics and supporting materials not otherwise available in the public domain
- Patient/customer/member information
- Employee information and records
- Any and all financial or business strategy information including, but not limited to, all enterprise strategy, business unit and entity plans, drafts and supporting data.

Personally Identifiable Information (PII): Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

Protected Health Information (PHI): PHI consists of health information that has been transmitted or maintained in any medium (for example, written, oral, or electronic) that:

a) Identifies the Individual; or
b) There is a reasonable basis to believe the information can be used either alone or in combination with other information to identify the Individual;

And the information

a) Relates to the past, present, or future physical or mental health or condition of an Individual or the provision of healthcare to an Individual; or
b) Relates to the past, present, or future payment for the provision of healthcare to an Individual.

Social Media: Any online publication and content, including but not limited to, postings, pages, blogs or wikis and social networking sites such as Facebook, LinkedIn, Twitter, Flickr, and YouTube.

Workforce: XYZ Health System Employees, contractors, volunteers, trainees, and other persons whose conduct, in the performance of work, is under the direct or indirect control of XYZ Health System, whether or not they are paid are subject to this policy.

References:

Policy Ownership Information:

Department or Committee which Owns Policy: _____

Department Leader or Committee Chair: _____

Policy Author / Subject Matter Expert: **_____**

Next Review Date:

Appendix B: Sample Policy - Use of Social Media for Official Company Business

Introductory Note: *The sample social media policies below are examples of policies that are being used by a health system to manage social media use in its environment. It is only an example and is not meant to be a complete or exhaustive list of policy elements. Because organizations, along with regulatory and legal requirements, are different, each organization should develop unique policies that are aligned with the needs of the organization, applicable laws, and is consistent with its policies and procedures.*

Purpose:

To describe the rules governing appropriate access to and utilization of Social Media by XYZ Health System Workforce for XYZ Health System business-related purposes including XYZ Health System sponsored sites.

Policy:

1. The XYZ Health System XXXX Department is the only department that can authorize the creation and/or maintenance of Social Media and/or internet sites/outlets that represent XYZ Health System, and/or all other XYZ Health System entities, facilities and services, including the regional facilities. The XXXX must approve all Social Media initiatives/activity on behalf of XYZ Health System outside the department.

2. Approved XYZ Health System Workforce may access and utilize XYZ Health System's Social Media sites, programs and tools only for XYZ Health System business-related purposes.

3. All Social Media users of any site are prohibited from disclosing any content that is Protected Health Information (PHI) or Personally Identifiable Information (PII) in any Social Media medium without the express written authorization of the individual who is the subject of the PHI or PII, and the XYZ Health System Privacy Officer.

4. All Social Media users of any site are prohibited from disclosing any content that is XYZ Health System's confidential or proprietary information in any Social Media environment without the express written authorization of a senior manager (Vice President or above).

Procedure:

1. **General Requirements**

   A. It is important to be honest and transparent when participating in Social Media. XYZ Health System Workforce members shall identify themselves as a XYZ Health System employee when publishing or commenting on Social Media sites for XYZ Health System business purposes (other than as an incidental mention of place of employment in personal Social Media on topics unrelated to XYZ Health System).

B. XYZ Health System trusts and expects its Workforce members to exercise personal responsibility whenever participating in any Social Media. All Workforce members, including physicians, are personally responsible for their posts. Therefore, Workforce members must take care not to violate the law or others' legal rights in their postings on any site, such as violating an individual's (such as a patient or visitor or employee) right to privacy and publicity by showing a person's image without permission.

C. Workforce members may not post any material that is obscene, defamatory, profane, libelous, threatening, harassing, abusive, hateful, or embarrassing to another person or entity when posting to XYZ Health System-hosted sites or representing XYZ Health System.

D. Workforce members may not post content or conduct any activity that fails to conform to any and all applicable state and federal laws on XYZ Health System sites or while publishing official XYZ Health System content on other sites. For example, Workforce members must abide by copyright and trademark laws by ensuring that they have permission to use or reproduce any copyrighted text, photos, graphics, video or other material owned by others.

E. Workforce members may not post content or conduct any activity that fails to conform to any and all applicable laws and regulations on XYZ Health System sites or while posting official XYZ Health System material on public sites.

F. Workforce members shall not attempt to address misrepresentations made about XYZ Health System in the media or in Social Media and shall alert the appropriate Public Relations/Communications Department contact.

G. Workforce members shall obtain permission for use of official XYZ Health System photographs, images, videos, or logos from the XXXX Department prior to use.

2. **Authorization for Use of Social Media**

A. To request access to Social Media sites Workforce members (or their XYZ Health System contact, in the case of non-employee Workforce members) shall contact the XYZ Health System Information Technology Department.

B. The Information Technology (IT) Department shall route all such requests to the requestor's supervisor for approval prior to consideration by the IT Department.

C. Requests shall be evaluated on a case-by-case basis and must include documented justification of the business need to use Social Media.

D. Social Media identities, logon IDs, and user names for non-business purposes shall not include the "XYZ Health System" name without prior approval.

3. **Security and Monitoring**

A. XYZ Health System may monitor electronically transmitted messages and information on XYZ Health System systems and equipment. XYZ Health System does not guarantee privacy for

Workforce members regarding electronically stored or transmitted content using XYZ Health System information technology.

B. Use of XYZ Health System's Social Media sites will be subject to monitoring, without consent or notice, within the parameters of Information Technology Acceptable Use policy.

4. **Enforcement**

A. Conduct in violation of this policy shall result in disciplinary action up to and including termination of employment or contractual services. Human Resources will assist decision-makers in determining disciplinary action.

B. This policy shall be interpreted and applied in a manner as to comply with all applicable law.

Definitions:

Confidential Information: XYZ Health System employee, customer and proprietary information that is not generally available in the public domain. This is the default level for all information under XYZ Health System custody and control except that information specifically declared to be public. Examples of Confidential Information include, but are not limited to:

- Protected Health Information (PHI) and Personally Identifiable Information (PII)
- Passwords
- Operating methods
- Marketing tactics and supporting materials not otherwise available in the public domain
- Patient/customer/member information
- Employee information
- Any and all financial or business strategy information including, but not limited to, all enterprise strategy, business unit and entity plans, drafts and supporting data.

Personally Identifiable Information (PII): Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

Protected Health Information (PHI): PHI consists of health information that has been transmitted or maintained in any medium (for example, written, oral, or electronic) that:

a) Identifies the individual; or
b) There is a reasonable basis to believe the information can be used either alone or in combination with other information to identify the Individual;

And the information

a) Relates to the past, present, or future physical or mental health or condition of an Individual or the provision of healthcare to an Individual; or

b) Relates to the past, present, or future payment for the provision of healthcare to an Individual. PHI does **not** include employment records held by XYZ Health System.

Social Media: Any facility for online publication and commentary, including but not limited to, blogs, wikis, social networking sites such as Facebook, LinkedIn, twitter, flickr, and YouTube.

Workforce: XYZ Health System employees, contractors, volunteers, trainees, and other persons whose conduct, in the performance of work, is under the direct control of XYZ Health System, whether or not they are paid, are also subject to this policy.

References:

Policy Ownership Information:

Department or Committee which Owns Policy: _____

Department Leader or Committee Chair: _____

Policy Author / Subject Matter Expert: **_____**

Next Review Date:

Appendix C: Social Media Resources

American Medical Association (AMA): http://www.ama-assn.org

AMA: Professionalism in the Use of Social Media:
http://www.ama-assn.org/ama/pub/physician-resources/medical-ethics/code-medical-ethics/opinion9124.page

Mayo Clinic for Social Media: http://socialmedia.mayoclinic.org/

CSC: Should Healthcare Organizations Use Social Media?:
http://assets1.csc.com/health_services/downloads/CSC_Should_Healthcare_Organizations_Use_Social_Media.pdf

HCCA: Social Media Survey:
http://hccainfo.org/staticcontent/2011SocialMediaSurvey_report.pdf

Online Database of Social Media Policies:
http://socialmediagovernance.com/policies.php#axzz1je5ucH7k

Ed Bennett List of Social Media Use: http://ebennett.org/hsnl/

The ECRI Institute: http://www.ecri.org

eHOW.Com: Ethical and Legal Issues in Healthcare:
http://www.ehow.com/facts_5501394_ethical-legal-issues-health-care.html#ixzz2BGy4gJfe

IT Pro's 3 Step Guide to Safe Social Media:
http://www.lumension.com/Media_Files/Documents/Marketing---Sales/Others/3-Step-Guide-to-Safe-Social-Media.aspx

ISACA: Social Media Risk and Mitigation Guidance:
http://www.isaca.org/Education/Upcoming-Events/Documents/2012-NACACS-Presentations/246-nac2012.pdf

ISACA: Social Media: Legal Risk Mitigation:
http://isacahouston.org/documents/SocialMedia_LegalRiskMitigation_ISACAHouston.pdf