Social Media and Healthcare

Best Friends or Worst Enemies

Gallagher
Healthcare

Gallagher | HEALTHCARE

Social Media and Healthcare: Best Friends or Worst Enemies?

Summary

Social media isn't just a fad. Facebook is a $100 billion company with 1.1 billion users,[1] LinkedIn has over 200 million users throughout 200 countries,[2] Twitter has successfully filed its initial public offering, and Google is one of the most valuable and powerful companies on the planet. The social media revolution has affected every industry, yet it poses unique challenges for the healthcare sector. The Health Insurance Portability and Accountability Act ("HIPAA") places a strong emphasis on the protection of individually identifiable patient information. The omnipresence of social media in the workplace can make protecting this information extremely difficult for healthcare providers. The growing use of mobile devices, such as smartphones and tablets, has made it virtually impossible for employers to monitor their employees' social media use while working. This challenge poses significant problems for HIPAA compliance and complicates public relations and employment law matters. However, some healthcare providers have embraced social media and use it to connect with their patients and communities, encourage preventive care, and create online support groups and communities. This paper discusses the need for healthcare employers to educate and embrace the use of social media by creating a comprehensive social media policy and educating their employees on the best uses of this powerful tool.

Social Media Trends

Social media is commonly defined as the means of interactions among people in which they create, share, and exchange information and ideas in virtual communities and networks. Some of the most popular social media communities include Facebook, Twitter, LinkedIn, Pinterest, YouTube, Google+, Instragram, Tumblr, Foursqaure, Yammer, and Snapchat. Each site or application serves a slightly different purpose and has its own unique functionality. Many of the sites integrate with one another and allow users to share content through multiple channels. Facebook is the most popular network; however, Twitter, Youtube, Google+, Linkedin, Pinterest, and Tumblr are all rapidly growing, popular platforms.

Increase in Digital Sharing

As a whole, the population continues to become more comfortable with the digital sharing of information. This is especially true for people under the age of thirty who are commonly referred to as "digital natives." People are not only sharing digital information with friends and family, but also with the government, corporations, and other institutions. Examples include:

- Blogging
- Sharing photos
- Sharing videos
- Online banking
- Electronic filing of tax returns

The amount of digital information created and shared online has grown over 900 percent in the past five years. An estimated 500 million photos are uploaded to the internet and shared every day, while 100 hours of video are uploaded each minute on YouTube. While people have become more comfortable with digital sharing, there are still serious concerns about privacy when it comes to healthcare information. One study found that 63 percent of people are strongly concerned that their confidential health information will be publicly shared, and 57 percent are afraid that this information is susceptible to hacking.[3]

The Shift to Mobile Devices

There are approximately 1.5 billion smartphone users, comprising over 21 percent of the world's population. In fact, an estimated 15 percent of all internet traffic now comes from mobile devices. Consumers are moving away from PCs and increasingly accessing the internet from mobile devices such as smartphones and tablets. Facebook reported that 68 percent of its 1.1 billion users now access the site from a mobile device giving credence to the theory that people access social media anytime and anywhere. Therefore, even if employers block popular social media sites from internal internet service providers, employees can easily bypass this restriction by accessing social media from their personal mobile devices.

Social Media Risks

HIPAA: The Privacy and Security Rules

HIPAA's privacy rule protects against the improper use or disclosure of protected health information ("PHI") by increasing patients' rights and limiting a provider's use and disclosure of PHI. PHI is defined as individually identifiable health information ("IIHI") that is: (1) transmitted by electronic media, (2) maintained in any electronic media, or (3) transmitted or maintained in any other form or medium. The privacy rule applies to all PHI, whereas the security rule deals specifically with electronic PHI.

HIPAA's security rule's general requirements include ensuring the confidentiality, integrity, and availability of all electronic PHI a covered entity creates, receives, maintains, or transmits; protecting against any reasonably anticipated threats or hazards to the security or integrity of such information; and protecting against any reasonably anticipated uses or disclosures of such information and ensuring compliance by the workforce. These rules apply to all "covered entities." Covered entities include providers of medical or health services and any other person or organization who furnishes, bills, or is paid for healthcare in the normal course of business, and who electronically transmits data in connection with any covered transaction.

HIPAA Compliance and Cyber Security

Employees of healthcare providers should be very careful about social media use while on the job. Tweeting about a patient, posting a picture to Facebook, or uploading a video to Youtube may all result in serious HIPAA violations. Every healthcare employee should know not to take a picture of a patient and post it on a social media page; however, not all HIPAA violations are this straightforward. A Facebook post stating "I took care of a celebrity this morning!" could easily lead to a HIPAA violation. The Facebook post could have included the employee's location, which is now very common. If an individual could locate the hospital and determine the identity of the celebrity being treated there, a HIPAA violation has occurred. Tweeting a picture of the employee and a colleague at work may also lead to a HIPAA violation. The picture of the employee and the colleague may have inadvertently displayed a patient's PHI in the background, and if so, this would also constitute a HIPAA violation. It is important to recognize that once information is disseminated via social media, it is almost impossible to remove. People "retweet" tweets, "share" Facebook updates, and post Youtube videos to blogs constantly. The social networking site or application may not even have the ability to remove certain content once it has been shared. This can turn a small mistake into a multimillion dollar problem.

There is also an ongoing concern regarding cyber security for individuals, governments, and corporations. Even the most sophisticated servers

are not immune from hacking, the United States government and some of the largest companies in Silicon Valley have recently been victims of hackers.[4] All companies, especially healthcare providers, should have procedures in place in the event of a security breach and/or HIPAA violation.

Public Relations

Social media allows anyone to have his or her opinion communicated to a large number of people. Used negatively, this can have a devastating impact on an organization's or a professional's reputation. Healthcare providers and professionals should monitor social media and track patients' comments made to social media sites. It is advisable to designate an individual within the organization to be responsible for responding to patient complaints that are made via social media. Additionally, hospitals and other healthcare providers should consider creating and maintaining official social media accounts and only permit specific employees to post on behalf of the organization.

Healthcare professionals should maintain separate personal and professional social media accounts. For example, physicians and other professionals should avoid "friending" patients on Facebook, but LinkedIn can be a great place to maintain a professional presence online.

Employment Law

Social media has had a serious impact on labor and employment law. There are three primary areas in which all employers need to be cognizant about how they are handling social media.

During the Hiring Process

- Arkansas, California, Colorado, Illinois, Maryland, Michigan, New Mexico, Oregon, Utah, and Washington have all enacted laws restricting an employer's right to access password protected material on a prospective employee's social media account.
- The Federal Government and additional states are considering similar legislation.
- An employer may Google an applicant and access his or her publicly available social media account.
- Typically, an employer cannot request or require an applicant or employee to provide user names or passwords for personal social media accounts.

During Employment

- Employers should create, maintain, and enforce a policy prohibiting social media use while employees are "on the clock" (except when authorized).
- While this policy is difficult to enforce, it will help an organization's legal defense in the event of a negative event.
- It is virtually impossible to control an employee's use of social media when not at work.
- The National Labor Relations Board has stated that limiting an employee's use of social media may infringe on his or her right to "self-organize, to form, join, or assist labor organizations, . . . and to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection" under Section 7 of the National Labor Relations Act.[5]

After Employment

- Questions may arise regarding the ownership of content posted on social media. For example, a physician uses an employer-sponsored Linkedin page to disseminate preventative health tips but then leaves the employ of the employer.
- Solicitation may be a concern. For example, a physician announces on social media that he is leaving Practice Group A and that his patients should now follow him to Practice Group B.
- These concerns should be addressed in employment contracts or other written agreements whenever possible.

Recommendations

Healthcare providers should create, maintain, and enforce a comprehensive social media policy. Employees should receive education regarding social media's impact on PHI, HIPAA, and the organization as a whole. Progressive healthcare providers are using social media to their advantage by creating online patient support groups, increasing awareness about preventive care, soliciting patient feedback, and responding to patient complaints. Implementing an effective social media policy can have distinct financial advantages as well. With the implementation of the Affordable Care Act's pay-for-performance initiatives, 6 percent of an organization's Medicare reimbursement is tied to measures such as hospital readmission rates, the number of hospital acquired infections, and quality of care (which includes patient satisfaction).[6]

Tips for creating an effective social media policy:

- Define the scope of the policy and give examples ("policy includes, but is not limited to Facebook, Twitter, LinkedIn, etc").
- Describe the organization's social media philosophy.
- Provide guidelines for employee's use of social media.
- Provide guidelines for the organization's use of social media.
- Identify the parties who must comply with the policy.

DO	DO NOT
Use common sense	**Ignore the issue!**
Treat discussions on social media the same as if they were occurring in a crowded elevator.	Be "friends" with, link to, or otherwise communicate with patients through personal social network.
Maintain the confidentiality of patient information at all times.	Use the organization's email to register on social networks, blogs, or other online tools utilized for personal use.
Maintain the confidentiality of trade secrets or other private or confidential information of the organization.	Speak on behalf of the organization, unless you have permission.
Be honest and correct any posts with incorrect information in a timely manner.	Use statements, photographs, video or audio that reasonably could be viewed as malicious, obscene, threatening or intimidating, or that might constitute harassment.
Consult with legal counsel and/or human resource professionals when drafting a social media policy.	Use text or instant messaging to communicate patient information.

About the Authors

Beth Berger, CIC, RPLU

Arthur J. Gallagher & Co.

National Managing Director—Gallagher Healthcare Practice

Beth Berger is the National Director for Gallagher's Healthcare Practice. She joined Gallagher in 1997 and has focused primarily on Healthcare Facilities, Integrated Programs and Complex Risks. Ms. Berger has an extensive property and casualty background serving in various commercial lines, sales, service, consulting and marketing positions within Gallagher. As a healthcare industry specialist she works with Gallagher offices across the country on providing risk solutions for Integrated Healthcare Systems, Healthcare Providers, and Healthcare Associations.

Ms. Berger specializes in tailoring casualty programs which address each client's unique exposures and complex risks. Her 25+ year insurance background includes risk analysis, program design, marketing and account coordination of conventional as well as alternative risk finance products. She has achieved her Certified Insurance Counselor (CIC) and Registered Professional Liability Underwriter (RPLU) Designations. She works with the Renal Service Exchange as part of the Risk Services Committee. Ms. Berger is currently a member of the Healthcare Finance Management Association (HFMA), the American Society of Healthcare Risk Management (ASHRM), the American Academy of House Call Physicians and the National Association of Professional Women (NAPW). Ms. Berger was recently awarded the 2013/2014 Woman of the Year Award by the NAPW for her work in the insurance industry

Douglas A. Grimm, FACHE

Stradley Ronon Stevens & Young, LLP—Chair, Healthcare

Douglas A. Grimm, FACHE, is the Chair of the Healthcare Practice at Stradley Ronon Stevens & Young, LLP. Mr. Grimm's practice focuses on the general representation of healthcare systems, with an emphasis on regulatory counseling in the areas of compliance planning, government investigations, health information privacy and security, health information technology, peer review/ medical staff and certificates of need, development of new service lines, licensure and provider enrollment and insurance issues. Prior to practicing law, Mr. Grimm served as Chief Operating Officer of multiple acute-care hospitals throughout the United State, and is a Fellow in the American College of Healthcare Executives. He holds a Master's degree in Healthcare Administration from the Medical College of Virginia, a law degree from South Texas College of Law and an LL.M. in health law from George Washington University Law School.

Arthur J. Gallagher & Co.

12621 Featherwood, Dr., Ste 300
Houston, TX 77034

Gallagher Healthcare

[1] United States Securities and Exchange Commission, Facebook, Inc. Form 10-K (2012), http://www.sec.gov/Archives/edgar/data/1326801/000132680113000003/fb-12312012x10k.htm.

[2] United States Securities and Exchange Commission, Linkedin Corporation Form 10-K (2012), http://www.sec.gov/Archives/edgar/data/1271024/000127102413000010/lnkd12312012-10kdoc.htm.

[3] Social Media "likes" Healthcare. PricewaterhouseCoopers Health Research Institute (April 2012) page 24, available at http://www.pwc.com/us/en/health-industries/publications/health-care-social-media.jhtml.

[4] Bosch, Torie, The Biggest Data Breaches in the History of Cybersecurity, Slate.com (Aug. 2, 2013, 4:32 PM), http://www.slate.com/blogs/future_tense/2013/08/02/infographic_shows_biggest_data_breaches_in_history_of_cybersecurity.html.

[5] NLRB Releases Advice Memo on Social Media Policies, Increases Focus on Employee Handbooks, Lexology.com (Aug. 13, 2013), http://www.lexology.com/library/detail.aspx?g=17bbc275-27d7-4650-8275-310243757345.

[6] Fiore, Kristina, Hospitals Already Feeling ACA Pinch, Medpage Today (June 28, 2013), http://www.medpagetoday.com/Washington-Watch/Reform/40160.