Social Media Compliance in Health Care

By Eric Newman, JD, CCEP, CHPC

¶53,150 Introduction

[*] Social media sites are designed to allow users to easily share information and content with each other, which is why it's one of the most common ways to communicate, especially among younger people.[1]

Companies have the responsibility of understanding both the risks and benefits of social media in the workplace. Employees commonly use social media at the workplace, and many companies have developed policies to help guide their staff on appropriate use.

Highly regulated industries, like health care, present unique opportunities around social media use. Public laws, such as Health Insurance Portability and Accountability Act of 1996 (HIPAA) (P.L. 104-191) and various state privacy laws, have restrictions around disclosing patient information. This chapter discusses how the HIPAA regulations relate to social media and some common misconceptions employees have. The chapter also explains how to prevent incidents by developing a smart social media policy and effectively educating and training the workforce on the policy.

¶53,155 HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) (P.L. 104-191) establishes privacy and security standards for health care information. HIPAA applies to covered entities and their business associates. "Covered entities" are health care providers (e.g., doctors, hospitals, clinics), health plans (e.g., health insurance companies, HMOs), and health care clearinghouses.[2] HIPAA also applies to business associates of a covered entity. A "business associate" is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.

The HIPAA Privacy Rule establishes standards for the protection of certain health information, known as Protected Health Information (PHI).[3] PHI goes beyond just the patient's name, and includes demographics (e.g., address, date of birth, phone number), financial (e.g., billing information, account number), and medical information (e.g., diagnosis, medications, lab results). PHI also can be a patient's IP address for a computer or even a patient's vehicle identification number (VIN). The HIPAA Security Rule establishes standards for protecting PHI that is held or transferred in electronic form, such as information contained within electronic health record systems and information transmitted by a computer or mobile device. By their nature, social media HIPAA incidents are bound by both the Privacy and Security rules.

A Giant Breach

HIPAA prohibits the use or disclosure of PHI to any unauthorized persons. Social media breaches

---

[*] Eric Newman is the privacy officer for Sutter Health North Bay Hospitals & Sutter Pacific Medical Foundation. Eric is a licensed Minnesota attorney and the former social media manager for the Society of Corporate Compliance and Ethics and Health Care Compliance Association (SCCE/HCCA).

[1] Newport, Frank. "The New Era of Communication Among Americans." *Gallup*, November 10, 2014, http://www.gallup.com/poll/179288/new-era-communication-americans.aspx.

[2] Covered Entities and Business Associates, U.S. Department of Health & Human Service, http://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html.

[3] A complete list of the 18 PHI identifiers can be found at 45 C.F.R. §164.514, and include names; all geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geocodes . . . ; All elements of dates (except year) for dates directly related to the individual, including birth date, admission date, discharge date, date of death; telephone numbers; fax numbers; electronic mail addresses: Social Security numbers; medical record numbers; health plan beneficiary numbers; account numbers; certificate/license numbers; vehicle identifiers and serial numbers, including license plate numbers; device identifiers and serial numbers; Web Universal Resource Locators (URLs); Internet Protocol (IP) address numbers; biometric identifiers, including finger and voice prints; full face photographic images and any comparable images; and any other unique identifying number, characteristic, or code . . . http://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

generally involve an unauthorized disclosure of PHI shared on a social media site. A recent example involved a New York Giants football player, Jason Pierre-Paul. On July 4, 2015, Pierre-Paul was involved in a fireworks accident and went to Jackson Memorial Hospital in Miami to be treated. A hospital employee took a screen shot of Pierre-Paul's medical record and sent it to ESPN reporter Adam Schefter. Schefter took to Twitter to reveal this hot news to his followers, tweeting "ESPN obtained medical charts that show Giants DE Jason Pierre-Paul had his right index finger amputated today" beneath the medical record screenshot.[4] Two hospital employees were terminated for leaking the records and the hospital system may be subject to significant regulatory fines.[5]

This example demonstrates how quickly and effortlessly it is to obtain sensitive PHI and share it with millions of people via social media. This example illustrates how bad actors, with malicious intentions, can create significant risk for an organization. However, many incidents arise from employees improperly trained about social media privacy compliance or workers with misconceptions about the perceived privacy of personal social media accounts.

Common Misconceptions

The following misconceptions about HIPAA and social media may lead to breaches:

1) "**It's OK to discuss patients on social media sites if I don't use the patient's name.**"

   - Some employees may not be aware that other types of identifiable patient information need to be protected in addition to the patient's name. Also, if the social media post can identify the patient, even without using any specific PHI, it may still be a HIPAA breach.

     • **Question:** Jacki, a hospital nurse, posts the following status on Facebook: "I just treated a survivor from that huge car accident that happened this morning." Is this a breach?

     • **Answer:** It depends. Although Jacki didn't technically disclose PHI, if this was a small town and there was only one huge car accident that happened in the area, then this information could identify the patient.

2) "**It's OK to take pictures at work and share them on social media sites as long as they aren't of patients.**"

   - Smartphones allow employees the ease and convenience of taking pictures and sharing them on social media sites. It's a great start that the employee is aware enough to avoid taking pictures of patients as that would constitute PHI that shouldn't be shared. Employees may not realize, however, that their picture contains other types of PHI hiding in the background.

     • **Question:** It's Amber's birthday and her department co-workers decorated her desk to celebrate. Amber wants to take a picture with her co-workers in front of her desk. Amber posts the photo on her Instagram page with the status "Best. Co-workers. Ever." What concerns might you have?

     • **Answer:** Although it's great that Amber and her co-workers have strong relationships, I would be mindful of whether there is any PHI hiding in the background of the photo. For instance, PHI may be visible on her computer screen or on paper documents on her desk.

3) "**It's OK for me to post PHI on my personal Facebook page because I changed the privacy settings so it's not 'Public.'**"

   - A common misconception is that there is an expectation of privacy on personal social media sites because of the advanced privacy settings you can apply. Employees should understand, however, that privacy settings

[4] Bonesteel, Matt. "Jason Pierre-Paul, Adam Schefter and HIPAA: What it all means." *The Washington Post*, July 9, 2015, https://www.washingtonpost.com/news/early-lead/wp/2015/07/09/jason-pierre-paul-adam-schefter-and-hipaa-what-it-all-means/.

[5] Gantt, Darin. "Hospital fires two employees for leaking Jason Pierre-Paul records," NBC Sports, Feb. 5, 2016, http://profootballtalk.nbcsports.com/2016/02/05/hospital-fires-two-employees-for-leaking-jason-pierre-paul-records/.

are not absolute and, once on the Internet, content can exist there permanently.

- **Question:** Dennis is a medical assistant in the hospital emergency department. Dennis' co-worker Angela just gave birth to a beautiful baby boy. Dennis took a picture of the baby and posted it on his Facebook page, tagging Angela in the post. Dennis then realized that maybe Angela wanted to announce the news herself so he quickly changed his mind and deleted the post. Is there a HIPAA privacy breach?

- **Answer:** It depends. By posting the photo on Facebook without authorization from Angela, Dennis committed an unauthorized disclosure. The hospital privacy officer would need to conduct a risk assessment to determine whether there was a low probability of compromise to this information, which will be difficult to do. The picture was identifiable because Dennis tagged Angela in the photo, and although Dennis promptly deleted it, the privacy officer would be challenged to confirm how many of Dennis and Angela's friends may have seen the picture.

There can't be an expectation of privacy if your "Friends" can see your posts. It's important for staff to understand that many social media privacy incidents are reported to the covered entity or regulators by those same "Friends" who saw the post and identified it as a potential privacy incident.

¶53,160 Developing a Social Media Policy

Social media policies should remind employees that they have an obligation to report potential HIPAA privacy incidents even when they aren't at work. An organization can best prevent social media incidents by effectively training and educating employees on its social media policy.

People are changing faster than companies[6]

An effective social media policy doesn't discourage employees from participating in social media. Creating a policy with that goal would be naïve. How would the organization enforce it? Smartphones allow employees to access social media sites at work and employees can access social media when they're off the clock. Instead, the organization policy should encourage meaningful and targeted social media participation.

Four steps to an effective social media policy:

1. Determine the objectives for the policy.
2. Collaboratively draft and approve the policy.
3. Effectively educate and train the organization's employees.
4. Moderate and enforce.

Step One: Determine the Objectives

Pick and choose what works best for the company brand and culture. Does the company already use social media for marketing and communications purposes? If so, would it be practical to significantly limit employees' ability to share its content and spread its messages?

Before the company drafts the policy, it must understand the internal culture and itsemployees' current involvement with social media. Only then can the company understand the organizational objectives and determine the goals of employee social media engagement.

Ask the following questions before drafting the policy:

- What does the company hope to accomplish with the policy?
- What does the company want to accomplish through the use of a social media presence?
- How does itensure the policy is consistent with the other corporate policies and guidelines? Be sure to consider other policies in employee manuals and employee agreements. Also, determine whether the company is in compliance with applicable government or industry regulations.
- Does the company use social media for its advertising and marketing?

[6] Kirkpatrick, David. "Social Power and the Coming Corporate Revolution," Forbes, Sept. 7, 2011, http://www.forbes.com/sites/techonomy/2011/09/07/social-power-and-the-coming-corporate-revolution.

- Does the company use social media to share information about its work in the community?
- Are employees already using social media to assist in work-related tasks?
- How important is Internet access and mobile usage to the company?
- How do employees personally use social media?

  —How many public pages do they have?

  —On which sites do they have a profile?

  —Are they actively using these sites? If so, what are they using the site for?

The primary objective for the company social media policy is to encourage responsible social media use. Employees should be ambassadors for their company. To that end, employees need to understand how their own behavior can impact the company. Employees should be educated about how posting something can cause any of the following to happen:

- HIPAA privacy and security breaches,
- spread of viruses and malware,
- copyright infringement,
- brand hijackings and lack of control over corporate content,
- defamation by employees,
- defamation by third parties posting negative comments about the business, and
- noncompliance with record management regulations.

Regulatory compliance:

Agencies such as the Federal Trade Commission (FTC) and the National Labor Relations Board (NLRB) have all brought complaints against companies for employee social media-related actions. The NLRB's Acting General Counsel has issued a report addressing the outcomes of NLRB cases that involve employees' use of social media and the legality of employers' social media policies.[7]

The company policy should consider the following issues:

- **Be aware of protected and concerted activities.** The policy should not prohibit lawful protected activity such as complaining about work conditions or compensation/benefits, or whistle blowing. Also, remember to emphasize the available communication channels for reporting wrongdoing, such as your hotline. For more information on what the NLRB deems concerted social media activity to be, visit https://www.nlrb.gov/news-outreach/fact-sheets/nlrb-and-social-media.
- **Implement a training program.** The company employees should know how to appropriately use social media and should be aware of company-specific concerns. These include not disclosing confidential information, protecting the company brand, protecting client privacy, antitrust compliance, and compliance with regulatory social media guidelines (e.g., the Financial Industry Regulatory Authority (FINRA) or the U.S. Securities and Exchange Commission (SEC)).
- **FTC guidelines.** The FTC guidelines for online endorsements with employees prohibits employees from giving reviews for company or competitors' products without disclosing their conflicting relationship. The FTC guidelines for endorsements and testimonials in advertising state that if there is a connection between the endorser and the seller of the product or service, full disclosure is required.[8]
- **Sarbanes-Oxley (SOX) considerations.** Financial information should not be released on social media sites unless it has been published in a press release. Make sure the information is updated to reflect any material changes.[9]

[7] Solomon, Lafe E. "Report of the Acting General Counsel Concerning Social Media Cases." *National Labor Relations Board*, Jan. 24, 2012, http://op.bna.com.s3.amazonaws.com/dlr-cases.nsf/id/ldue-8qunub/$File/OM%2012-31%20GC%20Report%20on%20Social%20Media%201-24-12.pdf.

[8] 16 C.F.R. Part 255. Guides Concerning the Use of Endorsements and Testimonials in Advertising. *Federal Trade Commission*, 2009, https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-publishes-final-guides-governing-endorsements-testimonials/091005revisedendorsementguides.pdf.

[9] Porcaro, John. "Social Media Laws and Regulations You Should Know," *Metia Group*, Aug. 26, 2011, http://

- **Hiring concerns.** Any employee who has the power to make hiring decisions should be trained to not use information from social media sites to discriminate against anyone based on legally protected factors.

Step Two: Collaboratively Draft and Approve the Policy

Creating the policy should be an organization-wide effort to adapt to the realities of today's social marketplace. In developing the content, partner with and seek approval from key internal colleagues including Compliance and Privacy, Risk Management, Legal, Information Technology (IT), Human Resources (HR), and Marketing and Communications.

The company policy should cover the following areas:

- a statement on the purpose of social media use,
- general information on social media including common definitions,
- guidelines for employee conduct on social media sites,
- management responsibilities including how social media activity is monitored by your organization, and
- enforcement options/violations.

Tips for creating the social media policy:

- The policy should not be full of legalese. Most employees don't speak that language.
- The policy should be easy to read, easy to understand and easy to remember.
- Provide specific examples and be clear on what the policy covers. Consider breaking down the policy into categories, subgroups or types of actions.
- Include which social media sites are covered and update this list periodically (e.g., Facebook, LinkedIn, Twitter, YouTube, Instagram, Snapchat).

Review sample policies: Don't recreate the wheel. Search through sample policies to find a template that can be altered to accommodate the structure and needs of the company. One sample policy can be found at the end of this chapter at ¶53,175.

Key messages: Some of the most common key messages in these social media policies are:

- be authentic and transparent,
- use good judgment,
- respect your audience,
- protect confidential information,
- respect copyrights,
- obey terms of service on specific platforms.

Other resources to consider:

- **Mayo Clinic - Social Media Guidelines** www.sharing.mayoclinic.org/guidelines/for-mayo-clinic-employees. Mayo's guidelines are limited to ten (10) clear statements. Mayo Clinic also has its own Social Network with resources including a comprehensive list of health-related organizations that actively use social media sites.[10]
- **Sutter Health - Social Media Tip Sheet & Video** www.sutterhealth.org/employees/social-media-policy.html. Sutter Health's Social Media Tip Sheet and Video are quick references that remind employees of the social media policy principles. The one-page tip sheet encourages employees to protect patients, respect sensitive information, and engage with colleagues. The social media video is a 90-second overview of Sutter Health's social media principles.
- **Vanderbilt University Medical Center - Social Media Toolkit** http://www.mc.vanderbilt.edu/root/vumc.php?site=socialmediatoolkit. Vanderbilt has an online toolkit with links to their social media policy, participation guidelines, and best practices. Also, there are resources for physicians to manage their online reputation and descriptions of popular platforms.
- **Social Media Policy Database** www.socialmediagovernance.com/policies. Chris Boudreaux, author of *The Social Media*

(Footnote Continued)

www.metia.com/seattle/john-porcaro/2011/08/social-media-laws-and-regulations-you-should-know/.

[10] Mayo Clinic Social Media Network, http://socialmedia.mayoclinic.org/.

Management Handbook, has a robust social media policy database for the health care industry.

Step Three: Effectively Educate and Train Your Employees

"Integrity is doing the right thing, even when no one is watching." - C.S. Lewis

Getting the word out:

- **Policy training.** Ensure your employees have an opportunity to learn from social media privacy violation examples. Also, employees should have a forum where they are able to ask questions.
- **Disseminate the policy company-wide**. Post the policy online in a place where employees can easily find and access it.
- **The format should be clear and easy to digest.** In addition to the text version of the policy, you may want to create a video or slideshow for employees to reference. For example, Sutter Health provides a short video and a social media tip sheet for employees, http://bit.ly/sutterhealthsm.
- **Inform employees of any policy updates.** Social media is quickly evolving, which may require updates if to keep the policy relevant.
- **Share the policy with the world.** The company values social media connections, and customers should know about it. Post the policy on the company website and social media sites.

Instill the *Triple-A* principles in employees:

- **Authenticity:** ***Be open and honest. Transparency is the key to a sustainable social media presence.***
- **Accountability:** ***You are responsible for your actions online. Assume everything you post is public to the world.***
- **Awareness:** ***What you say is permanent. Be respectful and know what you are talking about. Unless an employee is an official company spokesperson, he or she should add a disclaimer such as: "The opinions and positions expressed are my own and do not necessarily reflect those of [Company Name]."***

Step Four: Moderate, Archive, and Enforce

Ways to Moderate and Archive Content:

- **Pre-review**: Moderate or pre-approve the content before external publication.
- **Post-review:** Take down inappropriate content. Use alerts to notify social media administrators of inappropriate content.
- Capture any relevant social media content and securely store it.
- Retain the social media content based on SEC and FINRA rules, legal hold requests, and any additional retention policies.
- Monitor content by utilizing search engines for relevant keyword.
- Monitor changes made to company social media pages to ensure compliance policies are being enforced.

Enforcing the Policy

Be sure to include an "Enforcement" section in the policy that states that policy violations will be subject to disciplinary action up to and including termination for cause.

In addition, create an agreement for employees to sign. The agreement should state that the employee understands the company's social media policy, as well as the ethics and governance rules. Clear policy guidelines are necessary so the company can hold its employees accountable for using social media responsibly.

¶53,170 Conclusion

Social media is here to stay. Today's technology allows employees to share sensitive information on social media sites in mere seconds. It's the company's responsibility to give employees the tools they need so they can identify appropriate social media behavior and understand the risks of posting sensitive patient information. Empower employees to act with awareness, authenticity, and accountability. Effective guidance can help achieve social media compliance.

¶ 53,175 APPENDIX: Sample Policy: Social Media Policy for Physicians and Staff

Sample Policy: Social Media Policy for Physicians and Staff[11]

Social media includes websites such as Facebook, YouTube, Twitter and many others. New social networking websites allowing/encouraging online collaboration and/or commentary are being added each day. This policy covers all existing and future social networking media.

When You Engage in Social Media as a Company Employee

Emerging platforms for online collaboration are fundamentally changing the way we work, offering new ways to engage with patients and colleagues. It's a new model for interaction and we believe social media can help us to build stronger, more successful patient relationships. It's a way for you to take part in conversations related to the work we are doing at our company and the things we care about within our communities.

If you participate in social media, these are the guiding principles of the company:

- When you engage in comments or discussions about the company, use the company-related website or other sites (e.g., company Facebook account) for these activities. Please do not engage in comments or discussions about the company on other websites.
- Stick to your area of expertise and provide unique, individual perspectives on what's going on at our company and in the world.
- Post meaningful, respectful comments—in other words, no spam and no remarks that are off-topic or offensive.
- Always pause and think before posting – is this something you would say in person or to a mixed audience? That said, reply to comments in a timely manner when a response is appropriate.
- Patient privacy is of utmost concern. Do not share anything that can identify a patient or otherwise constitutes disclosure of Personal Health Information of any of our patients. Alert management if you see information posted by others, including patients themselves, that is confidential.
- When disagreeing with others' opinions, keep it appropriate and polite.
- Know and follow the company Confidentiality Agreement and HIPAA Privacy and Security Rules. Do not post pictures or images of employees, providers or patients without authorization.

RULES OF ENGAGEMENT

Be Transparent

- Your honesty—or dishonesty—will be quickly noticed in the social media environment.
- If you are blogging about your work at our company, use your real name, identify that you work for this company, and be clear about your role.
- If you have a vested interest in something you are discussing, be the first to point it out.
- Transparency is about your identity and relationship to this company.
- You need to safeguard private information and patient information as confidential.

Be Judicious

- Make sure your efforts to be transparent don't violate patient privacy, confidentiality, and legal guidelines.

---

[11] **"Healthcare Social Media Policy for Physicians and Staff,"** *Symplur*, http://www.symplur.com/public/healthcare_social_media_policy_for_physicians_and_staff.pdf.

- Ask permission to publish or report on conversations that are meant to be private or internal to the company.
- All statements must be true and not misleading and all claims must be substantiated and approved.
- Never comment on anything related to legal matters, litigation, or any parties with whom the company is in litigation or who have made a claim of malpractice, or lodged a formal complaint.
- Do not write or comment about other physicians or health care providers. Also be smart about protecting yourself, your privacy, and patient privacy.
- What you publish is widely accessible and will be around for a long time, so consider the content carefully.

Write What You Know

Make sure you write and post about your areas of expertise, especially as related to the company and its services. If you are writing about a topic with which the company is involved but you are not the expert on the topic, you should make this clear to your readers. If you are not a licensed provider such as a physician, nurse practitioner, or physician assistant, do not write or comment on clinical topics or issues. Write in the first person. If you publish to a website outside the company's website, please use a disclaimer something like this: "The postings on this site are my own and don't necessarily represent this company's positions, strategies or opinions, and do not constitute medical advice." Also, please respect brand, trademark, copyright, fair use, confidentiality, and financial disclosure laws. If you have any questions about these, contact management. Remember, you may be personally responsible for your content.

Perception is Reality

In online social networks, the lines between public and private, personal, and professional are blurred. Just by identifying yourself as this company's employee, you create perceptions in stakeholders, patients, and the general public about your expertise and about the company. You also create perceptions about you in your colleagues and managers. Do us all proud. Be sure that all content associated with you is consistent with your work and with the company's values and professional standards.

It's a Conversation

Talk to your readers like you would talk to real people in professional situations. In other words, avoid overly pedantic or "composed" language. Don't be afraid to bring in your own personality and say what's on your mind. Consider content that's open-ended and invites responses. Encourage comments. You also can broaden the conversation by citing others who blog about the same topic and allow your content to be shared or syndicated.

Are You Adding Value?

There are millions of words out there. The best way to get yours read is to write things that people will value. Social communication from our company should help our patients, partners, and co-workers. It should be thought-provoking and build a sense of community. If it helps people improve knowledge of health-related topics or skills, improve their lifestyle, solve problems, or understand the company better—then it's adding value.

Your Responsibility

What you write is ultimately your responsibility. Participation in social media networking on behalf of the company is not a right but an opportunity, so please treat it seriously and with respect. Failure to abide by these policies and the HIPAA Privacy and Security Rules could put your employment at risk. Please also follow the terms and conditions for any third-party sites.

Be a Leader

There can be a fine line between healthy debate and incendiary reaction. Do not denigrate other physicians, hospitals, or other health care providers, the company or other employees/providers, and do not engage with others who have done so. You do not need to respond to every criticism or barb. Try to frame what you write to invite differing points of view without inflaming others. Some topics—like politics or religion—slide more easily into sensitive territory so be careful and considerate. Once the words are out there, you can't really get them back, and once an inflammatory discussion gets going, it's hard to stop.

Did You Make a Mistake?

If you make a mistake, admit it. Be upfront and be quick with your correction. If you're posting to a blog, you may choose to modify an earlier post—just make it clear that you have done so.

If it Gives You Pause, Pause

If you're about to publish something that makes you even the slightest bit uncomfortable, don't shrug it off and hit "send." Take a minute to review these guidelines and try to figure out what's bothering you, then fix it. If you're still unsure, you might want to discuss it with your manager. Ultimately, what you publish is yours—as is the responsibility.