COSMOS
Navigate the Compliance Universe

Complete Healthcare Compliance Manual 2024
Patient Privacy and Security: Social Media

By Sheila Price Limmroth,[1] CHC, CIA

What Issues Are Associated with Social Media and Patient Privacy and Security?

When the Health Insurance Portability and Accountability Act (HIPAA) originally passed in 1996, discussions surrounding patient privacy in the context of social media were nonexistent.[2] It wasn't until MySpace launched in 2003, followed by Facebook in 2004, that "social media" became a common buzzword and way to communicate virtually. *Merriam-Webster Dictionary* defines social media as forms of electronic communication (such as websites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (such as videos).[3]

In February 2009, Congress passed the American Recovery and Reinvestment Act of 2009 (ARRA).[4] ARRA contains the Health Information Technology for Economic and Clinical Health (HITECH) Act. The HITECH Act provided some needed clarification to HIPAA. While HITECH does not specifically address social media concerns in the healthcare environment, both the HIPAA Privacy and Security Rules can be analyzed and applied to the current social media environment.

When discussing social media in terms of HIPAA, covered entities are typically concerned with two distinct components: (1) employee, physician, or vendor social media posts and (2) the entity's own approved website and organizational presence on social media platforms and the internet. This article will discuss the risks associated with both unauthorized and authorized use of social media platforms and the internet by covered entities.

Risk Area Governance

Although social media usage in relation to patient privacy and confidentiality is not specifically addressed by HIPAA, we can determine the need for compliance through a thoughtful review of both the HIPAA Privacy and Security Rules.

Defining Protected Health Information

HIPAA defines protected health information (PHI) as individually identifiable information, including demographic information related to the:

- Past, present, or future physical, mental health, or medical condition of a patient
- Provision of healthcare to a patient
- Past, present, or future payment for such healthcare created or received by a covered entity

PHI may exist verbally, electronically, or physically. The U.S. Department of Health and Human Services (HHS) lists individually identifiable information as including the following 18 patient identifiers:

1. Patient names
2. Geographical elements (such as a street address, city, county, or zip code)
3. Dates related to the health or identity of individuals (including birthdates, date of admission, date of discharge, date of death, or exact age of a patient older than 89)
4. Telephone numbers
5. Fax numbers
6. Email addresses
7. Social Security numbers
8. Medical record numbers
9. Health insurance beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers
13. Device attributes or serial numbers
14. Digital identifiers, such as website URLs
15. IP addresses
16. Biometric elements, including finger, retinal, and voiceprints
17. Full-face photographic images
18. Other identifying numbers or codes[5]

Covered entities (health plans, providers, healthcare clearinghouses, and business associates) have an obligation to protect PHI. This duty to protect PHI extends to electronic PHI posted to social media.

Covered entities must consider also how PHI is used without a patient's consent. Covered entities may use and disclose PHI for treatment, payment, and certain healthcare operations without written consent.[6] The use of PHI on social media does not fall within the HIPAA defined uses and disclosures exempt from written consent. Based on a review of the uses and disclosures language within HIPAA, one can infer social media posts related to PHI require the patient's consent via a valid written authorization.

The HIPAA Security Rule specifically protects electronic PHI (ePHI), and PHI shared on social media is ePHI. The security regulations specifically require that covered entities and business associates must:

1. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the Privacy regulations; and

4. Ensure workforce complies with the Security Rule.[7]

Beyond HIPAA, the Centers for Medicare & Medicaid Services (CMS) provides for patient rights as part of conditions of participation in federally funded programs. Hospitals, which bill federally funded programs, must promote and protect each patient's rights. These include, but are not limited to, the right to personal privacy, to be free from all forms of abuse or harassment, and the right to confidentiality of their clinical records.[8]

Common Compliance Risks

Unauthorized Use of Social Media

Generation Z (born between 1997 and 2012) grew up with the internet. This generation used and continues to use social media to connect with friends, express themselves, and find jobs. However, this is not the only generation using social media to connect with friends and blog about their day, often posting experiences (humorous and otherwise) from their work environment. People of all generations may have difficulty distinguishing between their personal and professional lives when using social media platforms. After all, it is easy to make a social media post without much thought.

The consequences of work-related social media posts in healthcare can range from job loss to civil and criminal liability. While HIPAA does not specifically address the use of social media, compliance must apply the Privacy and Security Rules to social media content. News reports from across the nation provide insight into what is considered inappropriate as it relates to sharing a patient's PHI on social media.

Headlines Related to Social Media

News headlines indicate the dire results for employees who post PHI on social media. In 2018, for example, a Texas nurse was terminated for remarks she posted on Facebook about a toddler who contracted measles after overseas travel.[9] Her comments, posted to the group, "Proud Parents of Unvaccinated Children—Texas," divulged detailed information from her treatment of the patient. "The kid was super sick. Sick enough to be admitted to the ICU and he looked miserable," the nurse posted to an antivaccine Facebook page. The nurse's employing hospital stated they were "made aware that one of our nurses posted protected health information regarding a patient on social media."[10]

A nurse in Massachusetts routinely posted TikTok videos she labeled "humorous skits," which others described as "videos that appeared to show [her] joking about mistreating her patients."[11] Her employer released a statement stating, "Be assured we have handled the situation and reported her actions to all appropriate state and federal agencies."[12] This case indicates that using a patient's name is not necessary for an employer to consider a social media post as compromising both a patient's right to privacy and right to dignity.

In 2021, a group of resident physicians posted on Instagram photos of body parts removed from patients in the operating room. The covered entity released a statement, saying it was "shocked and dismayed" by the incident, had already taken "corrective action," and was "actively and comprehensively investigating this unfortunate incident."[13]

In 2019, a Chicago nursing home terminated two employees after a Snapchat video surfaced showing them

taunting a 91-year-old resident with dementia .[14] The video resulted in a lawsuit against the nursing home for abuse.

Authorized Use of Social Media

Most covered entities have a social media presence, whether it's an organizational website, company-sponsored social media pages, or online reviews pages (e.g., Yelp, Google). It is important that organizations follow the HIPAA Privacy Rule when developing and responding to content on these platforms, as demonstrated in recent Office for Civil Rights (OCR) settlements.

In March 2022, the OCR issued a press release stating, "a dental practice with offices in Charlotte and Monroe, North Carolina, impermissibly disclosed a patient's PHI on a webpage in response to a negative online review."[15] The practice was assessed a civil monetary penalty.

In 2019, a dental practice in Dallas, Texas, released PHI without authorization when it responded to online reviews. The practice received a monetary penalty and was placed under a corrective action plan (CAP) that included two years of monitoring by the OCR. The OCR investigation found that dental practice impermissibly disclosed the PHI of multiple patients in response to patient reviews on the practice's Yelp review page. Additionally, the practice did not have a policy and procedure regarding disclosures of PHI to ensure that its social media interactions protect the PHI of its patients.[16]