Protected Health Information and Social Media

Carissa Floyd

Capella University

NURS-FPX-4040

Jennifer Carroll

April 29, 2022

Protected Health Information and Social Media

Protected health information (PHI) is any health-related information linked to an individual related to their past, present, or future health status like diagnoses, test results, prescriptions, or procedures. Did you know that HIPAA also lists 18 identifiers as PHI? Included are the obvious such as name, but there are others that you may not have given much thought to. Others included are geographical data except for state, dates including birthdate, admission and discharge dates, telephone and fax numbers, email addresses, social security numbers, medical record numbers, health insurance beneficiary numbers, account numbers, license numbers, vehicle identifiers, device attributes or serial numbers, digital identifiers such as website URLs or IP addresses, biometric elements including fingerprints, retinal scans, or voiceprints, full-face photographs, and any other identifying numbers or codes (*Protected Health Information: HIPAA PHI and HIPAA Data*, n.d., para. 3).

Privacy, Security, and Confidentiality

Privacy is the state of being free from public attention. An example of a violation of a patient's privacy would be posting a picture of you and your coworker on your nursing unit, failing to realize your patient's face is in the photo's background. Security is protecting the patient's PHI using appropriate safeguards. An example of a security breach would be leaving your computer screen open with a patient's chart accessed and an unauthorized passerby accessing or seeing patient information. Confidentiality is keeping something secret or private. You must keep patients' PHI confidential by not discussing any information you learn through caring for the patient with anyone who does not need to know. An example of this would be your

husband asking you for information on his hospitalized coworker in your unit. You must not share any information about this patient.

Social Media and PHI

Although your intentions may not be malicious, you can find yourself suffering harsh consequences from seemingly innocent social media encounters. For example:

-A student nurse in awe of the bravery of her three-year-old patient receiving chemotherapy posted a picture of the boy on her Facebook page. Although her profile was private, another nurse who was not her Facebook friend saw the photo and notified the hospital. The student nurse was expelled from the nursing program, and the hospital no longer accepted students from the school's nursing program (Veatch, n.d.).

-A New York hospital fired an ER nurse after sharing a photo taken and posted by a doctor of an empty, bloody trauma bay with the hashtag #manvs6train. Ultimately, she was fired for insensitivity, but her post did contain enough information that the patient could possibly be identified (Veatch, n.d.).

Fines for violation of HIPAA Privacy Rule can range from hundreds to millions of dollars. There can be criminal and civil penalties. You can lose your license and your job. If a breach occurs, you must report this to your compliance officer. The individual affected must be notified of the breach within 60 days of discovery (Sharpe, 2017). Most HIPAA violations occur from mishandling of PHI. Examples of social media violations include posting about a patient even if the name is not disclosed, sharing photos or any form of PHI without written consent, and sharing seemingly innocent photos with visible healthcare information (Sharpe, 2017).

Social Media Tips

According to ncsbn.org, the following are some tips and reminders to protect yourself and your patients in the context of social media.

-Avoid accepting friend requests from patients and their families.

-Understand that even deleted posts can still be found in cyberspace.

-Know that even your personal, private pages can be accessed by those other than your friends or followers.

-Remember, the HIPAA 18 identifiers must stay private. Such information can help someone quickly and easily identify when and why someone is in the hospital in small towns.

-Do not take pictures of patients on your phone or any device not covered by the hospital policy or without the patient's written consent.

-Know that patients' images or PHI must not be visible in the background of any photos taken in the facility.

-Never post information on social media pages that could be misconstrued as the voice or representative of the facility.

-Even if a patient shares details of their medical issues on social media, you should not repost or share that information on your own social media pages.

-Do not speak of patients or your institution negatively, even when not identified by name.

-Report any breaches of confidentiality or privacy promptly.

References

A nurse's guide to the use of social media. (n.d.). NCSBN.org. Retrieved April 26, 2022, from https://www.ncsbn.org/NCSBN_SocialMedia.pdf

Protected health information: HIPAA PHI and HIPAA data. (n.d.). Compliancy-group.com. Retrieved April 26, 2022, from Compliancy-group.com

Sharpe, S. (2017). Social media and patient protection: Don't ignore the HIPAA implications for your social media efforts. *The Dental Assistant*, *86*(4), 16. Retrieved April 26, 2022, from

Veatch, K. (n.d.). *a checklist for avoiding HIPAA violations on social media*. LAW360. Retrieved April 26, 2022, from https://www.law360.com/articles/743560/a-checklist-for-avoiding-hipaa-violations-on-social-media