Type: Protected Health Information (PHI): Privacy, Security, and Confidentiality Best Practices

Subject: Managing Health Information and Technology

Subject area: Nursing

Education Level: Undergraduate/College

Length: 2 pages

Referencing style: APA

Preferred English: US English

Spacing Option: Double

Title: Protected Health Information (PHI): Privacy, Security, and Confidentiality Best Practices

Protected Health Information (PHI) Privacy, Security, And Confidentiality Best Practices

Student's Name

Institutional Affiliation

Protected Health Information (PHI) Privacy, Security, And Confidentiality Best Practices

The use of modern technology in healthcare institutions has raised a new problem concerning the protection of the security, safety and confidentiality of patient data in healthcare organizations. The advent of new technologies in healthcare has raised the possibility of breaches of data protection, privacy and confidentiality. To avoid this, the Health Insurance Portability and Accountability Act (HIPAA) has been introduced to compel health care providers to monitor patient data protection, anonymity and security (Iyiewuare, Coulter, Whitley, & Herman, 2018). In order to be able to comply with these laws, a high degree of interdisciplinary cooperation and self-discipline in the use of healthcare technologies and social networks should be maintained by healthcare institution workers.

Privacy, confidentiality and protection for patients is a personal responsibility as a health care provider, particularly when using smartphones and social media sites (Ross & Myers, 2017). Any part of the health care team should adopt good personal safety improvement policies to protect patient information. Some of these activities involve signing out of individual accounts after each use, using a password manager, not regularly exchanging credentials and modifying passwords, and only sharing medical information with approved persons and for the intended purpose. Both electronic devices used for health care services must have a code to guarantee their inaccessibility in the event of a breach by unauthorized individuals. Every member who

intends to share patient data via the network system should encrypt the data to avoid interception, which could compromise secrecy, security, and privacy.

One of the most common causes of HIPAA violations by health-care staff has been identified as social media. It is widely accepted that people currently use mobile technology and social media to exchange information, links, and data through dialogue. The use of social networking sites can be extremely beneficial in exchanging relevant information with staff and clients, including general medical information that patients could need to stay healthy (Gardner & Allen, 2019). However, using social media as a health care specialist unit comes with a number of threats. One of them is a lack of message management. It is indeed important to remember that a tweet, even if sent by accident, will spread fast on social media, with little regulation or limits. As a result, it is critical to ensure that no protected patient information is sent via social media, except to a colleague. Sending confidential images, videos, audio files, or data over social networking sites runs the risk of revealing patient data to third parties, whether intentionally or unintentionally, putting HIPAA at risk.

When using social media to submit protected patient data, the IP addresses can be checked to ensure that the content and information are secured. In conjunction, when engaging in online patient engagement, adequate clinical boundaries should be enforced to protect patient confidentiality and privacy. It's also crucial to make sure the person on the other end is the rightful owner, rather than a third-party lurking behind the computer or the recipient's account.

Patient data protection will potentially be jeopardized if information gets into the wrong hands. Professionals must always be cautious about what they share on social media, particularly because they never know how the user could use the information to the public. It is difficult to keep details shared online private, particularly on social media. As a result, it is preferable to

protect what comes from you rather than hoping that the receiver will recognize its sensitivity and safeguard it for you. Careless posting of info on social media will severely harm an individual's professional reputation and also lead to legal action. As a result, it is important to maintain a high standard of ethics while sharing any medical information on different platforms.

References

Gardner, J. M., & Allen, T. C. (2019). Keep calm and tweet on: legal and ethical considerations for pathologists using social media. *Archives of Pathology & Laboratory Medicine*, *143*(1), 75-80. Retrieved from https://pdfs.semanticscholar.org/afd9/ca08cbe3810ce9af69f0d30d10f8306eb844.pdf.

Iyiewuare, P. O., Coulter, I. D., Whitley, M. D., & Herman, P. M. (2018). Researching the appropriateness of care in the complementary and integrative health professions part 2: What every researcher and practitioner should know about the health insurance portability and accountability act and practice-based research in the united states. *Journal of Manipulative and Physiological Therapeutics*, *41*(9), 807-813. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6684225/.

Ross, J. G., & Myers, S. M. (2017). The current use of social media in undergraduate nursing education: A review of the literature. *CIN: Computers, Informatics, Nursing*, *35*(7), 338-344. Retrieved from https://nursing.ceconnection.com/ovidfiles/00024665-201707000-00004.pdf.