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

School of Nursing and Health Sciences, Capella University

NURS-FPX4040 Managing Health Information and Technology

May 18, 2023

Protected Health Information (PHI)

- As the use of technology in healthcare continues to grow, so does the risk of security, confidentiality, and privacy breaches (Javaid., 2021).
- Patient medical records are protected against unauthorized access thanks to HIPAA.
- To ensure that former employees continue to have access to health insurance and to reduce healthcare costs through the standardization of electronic transmission of financial and administrative processes, HIPAA was enacted. These goals are supported by both the HIPAA Privacy Rule and the HIPAA Security Rule.
- The adoption of HIPAA was prompted by worries about the improper use of health information technology.


PROTECTED
HEALTH
INFORMATION


PII VS. PHI

The state of being able to keep oneself or one's activities secret.

- **Security**

The state of being secure; freedom from danger, state of safety.

- **Confidentiality**

The restrictions placed on who may access, distribute, and use data.

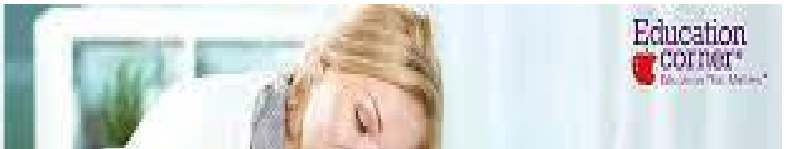
Example of Privacy

Respecting patients' right to privacy requires following the protocols they have set up to keep their health information secure. Information covered by the Privacy Rule is further safeguarded by the HIPAA Security Rule (CDC, 2020).

To ensure patients' rights to confidentiality, preferences, and values are respected, it is imperative that all healthcare workers demonstrate a multidisciplinary commitment to social media and EHR.

Privacy, Security, and Confidentiality

Complex passwords, enforcement of restrictions that limit access to authorized personnel, encryption of data to avoid interception, and regular resetting of passwords are only some of the interdisciplinary measures advocated to secure sensitive medical data.



Importance of Interdisciplinary Collaboration to Safeguard Sensitive Electronic Health Information

- Personal health information of patients must be protected during electronic storage, transmission, and exchange.
- It is essential that nurses, physicians, and IT specialists collaborate for this to be successful (He et al., 2021).
- All professionals should be accountable for enforcing priva regulations and should report policy violations to the prope authorities for disciplinary action.
- The IT expert may also advise the specialists on how to utilize social media without jeopardizing patient confidentiality.
- Over the last two years, there has been a rise in the number nurses who have been reprimanded for unethical social me use.
- The students living with disabilities or special needs can al participate in technology-aid learning.

Disciplinary actions may take several forms when it becomes clear that members of an interdisciplinary team have broken the rules. As a result of the harm they caused, many have had their licenses revoked or suspended, while others have gone to prison or been fired (Kleib et al., 2022). Healthcare businesses are severely hampered by the prohibitive compensation expenses brought on by employee violations of the rules.

Evidence Relating to Social Media Usage and PHI

- As in other fields, the healthcare sector has seen an increase in the need of protecting sensitive data as a result of technological advancements.
- Due to this pandemic, the healthcare business has obviously increased its use of social media to save time and travel enormous distances.

Careless use of social media by healthcare workers in contemporary healthcare facilities has been connected to violations of HIPAA privacy requirements and standards (Kleib et al., 2022).

- In addition, the browsers on smartphones and tablets grant access to numerous media platforms that promote content debate, link sharing, photo sharing, and other forms of inter-personal information transmission.
- As a result, this paradigm makes it easier for healthcare professionals to share private patient information with one another, which could put patients at risk (Kleib et al., 2022).

Consequently, it is the responsibility of every medical professional to keep this platform secure and to review its material on a regular basis to ensure that patient privacy is respected. Throughout, there should be a consideration for professional boundaries in all online contacts with patients. It is the responsibility of the healthcare practitioner to verify that only the patient receiving care is present throughout the whole exchange (Arvisais-Anhalt et al., 2022).

References

Arvisais-Anhalt, S., Lau, M., Lehmann, C. U., Holmgren, A. J., Medford, R. J., Ramirez, C. M., & Chen, C. N. (2022). The 21st century cures act and multiuser electronic health record access: potential pitfalls of information release. Journal of medical Internet research, 24(2), e34085. https://doi.org/10.2196/34085

Javaid, M., & Khan, I. H. (2021). Internet of Things (IoT) enabled healthcare helps to take the challenges of COVID-19 Pandemic. Journal of Oral Biology and Craniofacial Research, 11(2), 209-214. https://doi.org/10.1016/j.jobcr.2021.01.015

Chan, A. H. (2021). Logistics of rehabilitation telehealth: documentation, reimbursement, and Health Insurance Portability and Accountability Act. Physical Medicine and Rehabilitation Clinics, 32(2), 429-436. https://doi.org/10.1016/j.pmr.2021.01.006

Centers for Disease Control and Prevention. (2020). Health Insurance Portability and Accountability Act of 1996 (HIPAA). https://www. cdc. gov/phlp/publications/topic/hipaa

He, W., Zhang, Z. J., & Li, W. (2021). Information technology solutions, challenges, and suggestions for tackling the COVID-19 pandemic. International journal of information management, 57, 102287. https://doi.org/10.1016/j.ijinfomgt.2020.102287

Kleib, M., Nagle, L. M., Furlong, K. E., Paul, P., Wisnesky, U. D., & Ali, S. (2022). Are future nurses ready for digital health?: informatics competency baseline assessment. Nurse Educator, 47(5), E98-E104. https://doi.org/10.1097/NNE.0000000000001199