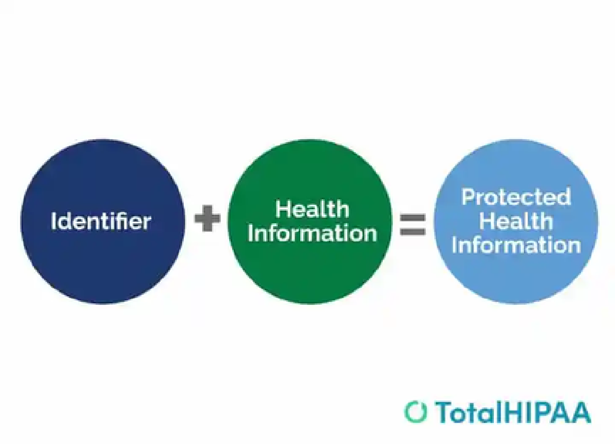

WHAT NOT TO DO: SOCIAL MEDIA RISKS

Avoid sharing screenshots, anecdotes, and discussions linked to telehealth sessions on social media as it could expose PHI to unauthorized personnel.

Refrain from posting derogatory comments about patients, colleagues, and health institutions, as it could compromise professional integrity and violate HIPAA mandates.

EVIDENCE AND STRATEGIES FOR PHI PROTECTION

Health institutions have implemented evidence-based measures to prevent confidentiality breaches and mitigate social media risks. Some of the techniques include:

1.Development of comprehensive social media policies and providing continued training to health personnel

2.Enforcing strict disciplinary actions, including sanctions and termination, for violations of these policies (Dong et al., 2021)

3.Collaboration with IT professionals to enhance cybersecurity measures and ensure the secure transmission of PHI within telehealth platforms.

4.Conducting regular audits and assessments to identify vulnerabilities and strengthen privacy and security measures.

REFERENCES

Bennett, K. G., & Vercler, J. C. (2018). When is posting about patients on social media unethical "Medutainment"? AMA Journal of Ethics, 20(4), 328-335. https://doi.org/10.1001/journalofethics.2018.20.4.ecas1-1804

Catlett, G., Flowe, W. D., & Henderson, A. (2023, October 16). HI professionals must post with caution on social media to protect patient privacy. Journal of AHIMA. https://journal.ahima.org/page/hi-professionals-must-post-with-caution-on-social-media-to-protect-patient-privacy

Cohen, I. G., & Mello, M. M. (2018). HIPAA and protecting health information in the 21st century. JAMA, 320(3), 231. https://doi.org/10.1001/jama.2018.5630

Dong, S. W., Nolan, N. S., Chavez, M. A., Li, Y., Escota, G. V., & Stead, W. (2021). Get privacy trending: Best practices for the social media educator. Open Forum Infectious Diseases, 8(3). https://doi.org/10.1093/ofid/ofab084

HIPAA And Social Media Guidelines. (n.d.). The HIPAA Journal. https://www.hipaajournal.com/hipaa-social-media/

PROTECTED HEALTH INFORMATION

TELEHEALTH SERVICES

INTRODUCTION

Due to digitalization, telehealth services are rapidly evolving. There is a need for healthcare professionals to uphold high standards of privacy, security, and confidentiality to protect patient information. The Health Insurance Portability and Accountability Act (HIPAA) mandates health professionals to safeguard protected health information (PHI) (Cohen & Mello, 2018). Therefore, this is an interprofessional staff update for provision of essential guidance on HIPAA compliance and appropriate use of social media within telehealth settings.

SOCIAL MEDIA RISKS TO PATIENT INFORMATION

Social media poses inherent risks to patient information, which include potential breaches of confidentiality, privacy violations, and harm an organization's reputation. Unauthorized disclosures of PHIU on social media platforms can have legal ramifications, affect trust, and damage relationships between a patient and a medical provider.

INTERDISCIPLINARY COLLABORATION AND PHI PROTECTION

Interdisciplinary collaboration involves ensuring the comprehensive protection of sensitive electronic health data (HIPAA And Social Media Guidelines, n.d.). Open communication and a mutual understanding among health professionals can help in addressing privacy, security, and confidentiality issues in telehealth setups.

STEPS TO TAKE IF A BREACH OCCURS

In the event of a social media breach involving PHI, health professionals should:

1.Remove unauthorized content from social media

2.Notify appropriate privacy and security officers in a health organization

3.Conduct an investigation to determine the scope and impact of the breach

4.Implement corrective measures to prevent future incidents and mitigate potential harm to affected persons.

SOCIAL MEDIA BEST PRACTICES

The best practices to follow when using social media is:

1.Strict adherence to HIPAA regulations when discussing patient cases or sharing health content on social media platforms.

2.Avoiding posting identifiable health information such as photos, names, and medical histories to prevent data breaches.

3.Using of privacy settings to control visibility of personal and professional social media content hence limited access to unauthorized persons (Bennett & Vercler, 2018).

4.Exercising caution in online discussions about telehealth experiences and avoiding disclosing of specific patient encounters and clinical details.

PHI AND HIPAA OVERVIEW

Protected Health Information (PHI) comprises of individually identifiable health information transmitted either electronically, written, or orally. HIPAA regulations provide strict guidelines for enhancement of privacy, security, and confidentiality of PHI hence safeguarding the rights of patients and prohibiting unauthorized disclosure.

PRIVACY, SECURITY, AND CONFIDENTIALITY IN TELEHEALTH

Privacy is the right of individuals to control access of their health information (Catlett et al., 2023).

Security is the safeguarding of this information from unauthorized access, use, or disclosure.

Confidentiality ensures that sensitive patient information remains protected from disclosures and breaches.

In Telehealth: Privacy concerns emanate from the use of unsecured platforms, potential eavesdropping, and unauthorized access to video conferences. Security risks may including hacking, malware attacks, and data breaches. Such attacks compromise the integrity of PHI.

Confidentiality breaches arise through unauthorized sharing of patient information during telehealth sessions and inappropriate usage of social media (Catlett et al., 2023).