Paper Details

School: Capella University
Subject: Nursing
Topic: Protected Health Information Privacy, Security and Confidentiality Best Practices
Course: Nursfpx 4040
Referencing: APA
Pages: 2

Internal Memo

Date:

To: ALL STAFF

Cc:

From:

RE: **PROTECTED HEALTH INFORMATION PRIVACY, SECURITY AND CONFIDENTIALITY BEST PRACTICES**

Priority: High

The objective of Protected health information (PHI) and Health Insurance Portability and Accountability Act (*HIPAA*) is to safeguard an individual's health information, and at the same time allow different healthcare units to implement advanced technologies to expand the quality and effectiveness of care provided to patients. Considering that healthcare is a diverse field, the security rules put in place is intended to be flexible, and accessible such that covered organizations can apply the policies, measures, and appropriate technologies suitable for the organizational structure.

Privacy, Security, and Confidentiality

The privacy rules cover the usage and sharing of a person's health data known as PHI by entities such as hospitals, long-term care homes, ambulatory care centers and other healthcare settings (Jiang & Bai, 2019). A patient has a right to decide how to use personal information (Jiang & Bai, 2019). For example, not disclosing a person's PHI to the employer or family members. Security covers the measures put in place to protect the means used to secure data and protect client's privacy and protect professionals holding the confidential information (Craig, 2017, p. 14). This includes software that limits unauthorized access to protected health information. For example, PHI includes diagnosis, the name physician who treated the patient

and the medications given to the patient, this information should not be disclosed to a third party. Confidentiality means the obligation of healthcare practitioners who access patient records to keep the information in confidence (Moore & Frye, 2019, p. 269). It also refers to the communication between two individuals in a professional relation, such as a patient and a nurse, physician or any healthcare professional (Moore & Frye, 2019, p. 270). An example is that physicians are not allowed to share patient's information disclosed to them in the course of doctor-patient relations.

Importance of Interdisciplinary Collaboration to Safeguard Sensitive Electronic Health Information.

Interdisciplinary collaboration needs to protect sensitive electronic health information since they provide specialist knowledge and skills used to address complex healthcare challenges. Sharing confidential electronic information is essential in the sense that it contributes to the delivery of team-based healthcare and enhances health outcomes (Koch, 2016, p.6). It also facilitates the effective delivery of healthcare and improves health outcomes and promote teamwork. It encourages cooperation and collaboration among the team members in sharing crucial information required for making critical healthcare decisions (Koch, 2016, p. 9).

Appropriate Social Media Use in Healthcare

With the upsurge in the use of social media, users must be careful about the things they post. Interprofessional team members must understand that once they post anything, it is hard to take away (Koch, 2016, p.5). The best option is to completely avoid posting about patients, coworkers or identifying your employer in social media. For instance, three nurses working in an assisted living facility were fired in Arizona for uploading a video of a resident on Snap Chat. Taking and posting photos on social media is irresponsible and can create problems both to the

employer through fines and may result in the employee being terminated. In another case, a

nurse in New York was forced to surrender her nursing license after taking a photo of a penis of

an unconscious patient and sharing it with colleagues. She also faced felony charges (De

Gagne et al., 2018)

References

1. Craig, D. J. (2017). Ensuring compliance with the HIPAA Security Rule: Think twice when
   e-mailing protected health information. The Nurse Practitioner, 42(6), 12-14.

2. De Gagne, J. C., Yamane, S. S., Conklin, J. L., Chang, J., and Kang, H. S. (2018). Social media
   use and cyber civility guidelines in US nursing schools: A review of websites. Journal of Professional Nursing, 34(1), 35-41.

3. Jiang, J. X., and Bai, G. (2019). Types of Information Compromised in Breaches of Protected
   Health Information. Annals of internal medicine.

4. Koch, D. D. (2016). Is the HIPAA security rule enough to protect electronic personal health
   information (PHI) in the cyber age? Journal of Health Care Finance, 43(3). 5-10.

5. Moore, W., and Frye, S. (2019). Review of HIPAA, part 1: history, protected health information, and privacy and security rules. Journal of nuclear medicine technology, 47(4), 269-272.