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

Name of the Writer

Institution Name

Instructor Name

Date formatted as Month Day, Year

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

Protected health information PHI is the personal information collected by healthcare professionals for the aim of patient identification. Protected health information includes demographic information, the medical history of a patient, their tests and laboratory results, the patient’s health conditions, and the patient's insurance information. The HIPAA requires healthcare institutions to maintain safeguards that ensure confidentiality, privacy, integrity, and unavailability of protected health information to unauthorized persons. The act also lays out guidelines for running health apps that potentially use, store, or transmit protected health information. HIPAA does not necessarily cover data collected by these apps. However, the healthcare institution applying the app is required to have a HIPAA compliance officer evaluating the app before implementation to ensure that it safeguards patients' privacy, security, and confidentiality (HIPAA journal, 2022).

**Privacy, security, and confidentiality**

Protection of the patient's privacy and treating their information with confidentiality protects them from security issues that would develop when unauthorized persons access their information. Patient privacy is the protection of the information that the institution collects about the individual. It is the right one to determine for themselves when and how personal information can be accessed or shared. Confidentiality is the protection of sharing information with unauthorized persons. Security is the level at which personal information is restricted and allowed for those authorized only. According to Keshta and Odeh (2021), patient privacy, security, and confidentiality concerns include failure to safeguard various information directly affecting patients' families. Also, accessing personal patient information would expose the patients to security risks such as being conned.

**Importance of the interdisciplinary collaboration in safeguarding sensitive electronic health information**

The interdisciplinary team has the role of safeguarding electronic health information, whether they come into contact with the information directly or indirectly. Since the consequences of breaching the protection of electronic health information may affect the entire healthcare institution, each interdisciplinary team member needs to maintain privacy, security, and confidentiality safeguards. It is the role of the interdisciplinary team to promote patient safety. One way to promote patient safety is by safeguarding patient privacy and confidentiality and ensuring patient security. Effective safeguarding of sensitive electronic patient information requires the collaboration of the interdisciplinary team (Keshta & Odeh, 2021).

**Evidence relating to social media usage and PHI**

The issue of electronic health information and the protection of protected health information should be taken seriously by all interprofessional team members. It is worth noting that the US government takes inappropriate social media use by the healthcare team very seriously. It has legal complications ranging from license termination, individual fines, and even fines to the healthcare organization. Healthcare institutions also set consequences for the interdisciplinary team when caught with social media misconduct. A healthcare professional may be suspended from working in the institution or initiate legal action. The misconduct may also make the institution to attract financial penalties or even affect its licensure.

Our institution's evidence-based strategies to prevent and reduce confidentiality, privacy, and security breaches, especially related to social media use, include staff training, disciplinary action taken against the staff found breaching and taking legal action (Zhou et al., 2018). The institution has annual social media and information technology training for all staff members, whereby the staff is reminded of the safety issues of social media use. There are also set steps to report social media misconduct and breaches, and all the staff members are aware of the consequences.

**Professional Staff Update**

Every member of staff should be careful when using social media so that we can maintain patient safety. We need to safeguard the patient’s privacy, confidentiality, and security to achieve desired patient outcomes and make our work safe.

**Social Media Best Practices**

* Healthcare professionals should have a clear distinction between social media and work.
* Care providers should not post content that may bring privacy and security concerns to the patient.
* Care providers should not post patients' personal information on social media platforms, especially personal identification information.
* The doctors and nurses should not post any diagnostic or patient medical history on social media without the patient's consent.
* Avoid sharing any sensitive patient information on social media platforms.
* Social media misconduct should be reported to the disciplinary of the institution or the relevant authority.

**Social Media Risks to Patient Information**

 The profound use of social media in healthcare poses a significant risk to sensitive patient information (Terrase et al., 2019). Patient information that hackers access may have detrimental effects on the patient’s safety and security. Personal information can be used to con the patient and patient families in the name of the healthcare institution. Some hackers can also use patient information to illegally access insurance reimbursements that cater to the patient’s treatment expenses. Also, healthcare professionals' accounts can be hacked, and patient information shared by malicious hackers, thus attracting legal implications to the owner of the hacked accounts. Therefore, it is integral for all healthcare staff in the interdisciplinary team to maintain good social media use and avoid as much as sharing patient information on their accounts.

**References**

Keshta, I., & Odeh, A. (2021). Security and privacy of electronic health records: Concerns and challenges. *Egyptian Informatics Journal*, *22*(2), 177-183. <https://doi.org/10.1016/j.eij.2020.07.003>

Terrasse, M., Gorin, M., & Sisti, D. (2019). Social media, e‐health, and medical ethics. *Hastings Center Report*, *49*(1), 24-33. <https://doi.org/10.1002/hast.975>

What is Protected Health Information? January 2, 2022. *HIPAA Journal*. Accessed on July 11, 2022. <https://www.hipaajournal.com/what-is-protected-health-information/>

Zhou, L., Zhang, D., Yang, C. C., & Wang, Y. (2018). *Harnessing social media for health information management. Electronic Commerce Research and Applications, 27, 139–151.*  <https://doi.org/10.1016/j.elerap.2017.12.003>