MHA-FPX5066 Assessment 3: Data Management and Best Practices

Student Name

Program Name or Degree Name (e.g., Bachelor of Science in Psychology), University

COURSE XXX: Title of Course

Instructor Name

Month XX, 2024

Data Management and Best Practices

The data collected, stored, and maintained in healthcare organizations is vast and contains confidential information that needs security. Each healthcare institution, therefore, is expected to work with the IT department and Health Information Management (HIM) system suppliers to ensure that their systems maintain high privacy and security standards while complying with the privacy regulations available (Hathaliya & Tanwar, 2020). More so, the institution should strive to apply data security and privacy best practices to maintain the integrity and confidentiality of patient information. This essay analyzes a healthcare organization's security and privacy issues, describes the end-user responsibilities and best practices related to the security and privacy of patient data, develops best practices for privacy, data security, and the integrity of patient information, and finally recommends particular end-user training for ensure end-user compliance with privacy and data security standards.

Healthcare Organization's Security and Privacy Issues Analysis

Patient information is sensitive, mainly due to containing personally identifiable details. The use of healthcare technology in care delivery has increased security and privacy-related concerns. Hence, it is vital to identify potential risks and compliance challenges that may cause privacy and security issues. Various security and privacy issues exist in healthcare organizations. Security issues in a healthcare organization may include cybersecurity threats, data breaches, unauthorized access to patient records, and physical security. Cybersecurity threats may consist of malware, ransomware, and other cyber threats. Data accessed by unauthorized persons is also a security issue due to the negative impact that the accessed data may have on individual patients.

Furthermore, privacy issues in a healthcare organization may entail patient consent management in data sharing, HIPAA compliance, and third-party sharing. Data may be shared without the patient's consent, which concerns privacy. Additionally, the healthcare organization must comply with the HIPAA regulations on patient information protection. HIPAA non-compliance raises significant privacy issues. Keshta and Odeh (2021) note that sharing electronic health records with third parties violates the confidentiality and privacy of a patient, thus requiring the establishment of sharing agreements.

End-User Responsibilities and Best Practices Related to the Security and Privacy of Patient Data

End-users in healthcare organizations play a significant role in maintaining the security and privacy of patient data. These end-users are mainly healthcare providers and administrators. Their responsibilities are to enhance the security and privacy of patient data. These responsibilities include data access control, password management, incident reporting, and training and awareness creation on the security and privacy of patient data. According to Khan et al. (2022), the end-users of health information systems are responsible for protecting patient data by adhering to access control policies. They should also maintain robust and unique passwords and protect login credentials to prevent unauthorized access to patient data. Additionally, end-users are responsible for reporting any incidents related to data breaches and suspected unauthorized access, thus preventing related issues by taking the necessary action immediately.

Best practices related to the security and privacy of patient data include using biometric passwords for patient data access, regular software, ensuring end-end encryption, and patient data backup. According to Bani Issa et al. (2020), biometric passwords are a best practice in protecting unauthorized access to patient data. Additionally, regular software updates keep the

operating systems up to date with new security features to prevent data breaches. End-end encryption protects data access while being shared among care providers and administrators.

Best-Practices for Privacy and Data Security and the Integrity of Patient Information

Healthcare organizations must ensure patient data privacy, security, and integrity by implementing best practices to safeguard the data and maintain patients' trust in their personal information. The best practices to maintain patient privacy include access controls and developing privacy policies. Soni et al. (2021) note that organizations should develop customized standard privacy policies and place access control measures such as biometric authentication in place. The data security best practices will include end-end encryption and two-factor authentication. Encryption will enhance data security during transmission. Additionally, implementing two-factor authentication will make data inaccessible to unauthorized persons. Patient information integrity best practice will entail accuracy training. The staff will be trained on data accuracy to maintain the data integrity of patient information.

End-User Training to Ensure Compliance with Privacy and Data Security Standards

As mentioned earlier, end-users play an essential role in maintaining data privacy, security, and integrity. Therefore, training them on the privacy and data security standards is critical. The end-user training to promote compliance with privacy and data security standards will emphasize safeguarding patient information, enhancing understanding of institutional privacy policies and regulations, and training on security and privacy control measures. The training should be customized to meet the institution's specifications and promote continuous education to update end-users.

Conclusion

Privacy and security issues in patient health information may have negative impacts on individual patients. Therefore, healthcare organizations should maintain privacy and security standards to maintain the confidentiality and integrity of patient information. In addition, they should apply best practices and train the end-users to comply with privacy and security standards.

References

Bani Issa, W., Al Akour, I., Ibrahim, A., Almarzouqi, A., Abbas, S., Hisham, F., & Griffiths, J. (2020). Privacy, confidentiality, security, and patient safety concerns about electronic health records. *International Nursing Review*, *67*(2), 218–230. https://doi.org/10.1111/inr.12585

Hathaliya, J. J., & Tanwar, S. (2020). An exhaustive survey on security and privacy issues in Healthcare 4.0. *Computer Communications*, *153*, 311-335. https://doi.org/10.1016/j.comcom.2020.02.018

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

Khan, M. M. A., Ehabe, E. N., & Mailewa, A. B. (2022, May). Discovering the Need for Information Assurance to Assure the End Users: Methodologies and Best Practices. In *2022 IEEE International Conference on Electro Information Technology (eIT)* (pp. 131-138). IEEE. https://www.researchgate.net/profile/Akalanka-Mailewa/publication/360773243_

Soni, M., Barot, Y., & Gomathi, S. (2021). A review on privacy-preserving data preprocessing. *Journal of Cybersecurity and Information Management*, *4*(2: Special Issue-RIDAPPH), 16-6. https://doi.org/10.54216/JCIM.040202