Annotated Bibliography

How does IT security protects patients' medical records in the health department?

(OCR), O. for C. R. (2021, June 28). *Summary of the HIPAA security rule*. HHS.gov. Retrieved September 28, 2021, from https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronically protected health information. The Security Rule applies to health plans, health care clearinghouses, and to any health care provider who transmits health information in electronic form in connection with a transaction for which the Secretary of HHS has adopted standards under HIPAA (the "covered entities") and to their business associates. The HIPAA Privacy Rule protects the privacy of individually identifiable health information, called protected health information (PHI), as explained in the Privacy Rule. The Security Rule protects a subset of information covered by the Privacy Rule, which is all individually identifiable health information a covered entity creates, receives, maintains, or transmits in electronic form. The Security Rule calls this information "electronically protected health information" (e-PHI).3 Technical safeguards are Acess controllers, Audit controllers, Integrity controllers, and transmission authority.

Guide to Privacy and Security of Electronic Health Information. Guide to Privacy and Security of Electronic Health Information. (n.d.). Retrieved from https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf. https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

Cybersecurity An Internet connection is a necessity to conduct the many online activities that can be part of EHR and ePHI use. Exchanging patient information electronically, submitting claims electronically, generating electronic records for patients' requests, and e-prescribing are all examples of online activities that rely on cybersecurity practices to safeguard systems and information.It is important to have strong cybersecurity practices in place to protect patient information, organizational assets, your practice operations, and your personnel, and of course to comply with the HIPAA Security Rule. 61 Cybersecurity is needed whether you have your EHR locally installed in your office or access it over the Internet from a cloud service provider.The security management process standard is a requirement in the HIPAA Security Rule. Conducting a risk analysis is one of the requirements that provides instructions to implement the security management process standard. ONC worked with OCR to create a

Security Risk Assessment (SRA) Tool83 to help guide health care providers (from small practices) through the risk assessment process. Use of this tool is not required by the HIPAA Security Rule but is meant to provide helpful assistance.

> Harman, L. B., Flite, C. A., & Bond, K. (2012, September 1). *Electronic health records: Privacy, confidentiality, and security*. Journal of Ethics | American Medical Association. Retrieve September 28, 2021, from https://journalofethics.ama-assn.org/article/electronic-health-records-privacy-confidentiality-and-security/2012-09. https://journalofethics.ama-assn.org/article/electronic-health-records-privacy-confidentiality-and-security/2012-09

The National Institute of Standards and Technology (NIST), the federal agency responsible for developing information security guidelines, defines *information security* as the preservation of data confidentiality, integrity, availability (commonly referred to as the “CIA” triad) [11]. Not only does the NIST provide guidance on securing data, but federal legislation such as the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act mandate doing so. Violating these regulations has serious consequences, including criminal and civil penalties for clinicians and organizations. The increasing concern over the security of health information stems from the rise of EHRs, increased use of mobile devices such as the smartphone, medical identity theft, and the widely anticipated exchange of data between and among organizations, clinicians, federal agencies, and patients. If patients’ trust is undermined, they may not be forthright with the physician. For the patient to trust the clinician, records in the office must be protected. The HIPAA Security Rule requires organizations to conduct audit trails [12], requiring that they document information systems activity [15] and have the hardware, software, and procedures to record and examine activity in systems that contain protected health information [16]. In addition, the HITECH Act of 2009 requires health care organizations to watch for breaches of personal health information from both internal and external sources.

In Conclusion, I picked these articles because they provide and cover all the information regarding how I.T security protects the data in the health departments. HIPPA rule is the biggest security followed in the health industry. I picked the second article because it talked about how Important and wide is Cyber Security and how it is applied in the Healthcare industry.