Assignment 1.1

Amy E. Haisten

Georgia Northwestern Technical College

HIMT 1200: Legal Aspects of Healthcare

Dr. Donna Estes

August 22, 2021

Assignment 1.1

Many healthcare entities share data with third parties, including government agencies and research firms. HIPAA protects an individual's health information, but this information is often used for reasonable endeavors like research and public health. For this information to be used for any other purpose than providing healthcare, it must be de-identified. Still, it is possible to later identify an individual from de-identified health data (El Emam, 2009).

HIPAA protects patient data and privacy and has some protection regarding de-identified data, including the Safe Harbor and Expert Determination standards. HIPAA considers patient data to be de-identified if it does not contain any one of 18 specific identifiers. A few examples of such identifiers include the date of service, telephone number, and zip code. HIPAA claims that the risk of re-identifying anyone is relatively low, and for this reason, it does not protect de-identified data and allows it to be shared (Simon, 2019).

Re-identification can put patients at risk. Intruders, who re-identify data contained in a database, can identify patients by known identifiers deliberately or accidentally. Intruders can identify someone they know personally or use public information, including data found on social media or sports team memberships or rosters (El Emam, 2009).

As society and healthcare become more reliant on technology and the EHR, security factors become an increasingly more significant risk. HIPAA has regulations to protect patients, and their privacy, including Safe Harbor, by setting some standards for how much data is de-identified (Simon, 2019). Protecting de-identified data is like walking a tight rope. If information is de-identified too much, it diminishes the clinical usefulness of the data. However, not de-identification the data enough can lead to a breach of privacy (El Emam, 2009). Healthcare providers should be held liable for security breaches, while regulations and facility policies should be specific and improved to protect patient data as much as possible. With technology, security risk will never be zero, and the advantages outweigh the disadvantages.

References

El Emam K., Dankar F. K., Vaillancourt R., Roffey T., & Lysyk M. (2009 July). Evaluating the Risk of Re-identification of Patients from Hospital Prescription Records. *NCBI.* https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2826964/

Simon, G.E., Shortreed, S. M., Coley R. Y., Penfold, R. B., Rossom, R. C., Waitzfelder, B. E., Sanchez, K., & Lynch, F. L. (2019, Mar. 29). Assessing and Minimizing Re-identification Risk in Research Data Derived from Health Care Records. *NCBI.* https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6450246/