Health information confidentiality

Health & Medicine

HIPAA and HITECH Acts al Affiliation) What are some safeguards that you think can reduce fear among individuals and groups who oppose identifiable health data collection?

Some patients still exhibit fear towards the current information security systems with the belief that their privacy could be breached through the various gaps that exists in the systems (Hebda & Czar, 2013). It is important for various institutions to embrace different security strategies such as appointing security officers on Private Boards and IRBs, who would assess the needs for data protection and implement staff training among other solutions. The use of encoding and encryption techniques on removable media and laptops would also help protect identifiable personal health information and thus promote patient confidence in the existing systems. In addition, through implementing breach notification requirements, patients protect their identity if a breach occurs (Hebda & Czar, 2013).

Do the benefits of confidential health data collection outweigh the risks? Why or why not?

The benefits of collecting the confidential data of patients are more than the risks. It is important for the health care providers to conduct a review of the appropriate utilization and protection to ensure that patient data is protected (Davies & Collins, 2006). Improved technology and the current development of security software have made it possible for health care organizations to protect the private data of their patients and reduce the risk of data breaching.

What, according to you, is the purpose of HITECH?

The major purpose of HITECH in to develop a nationwide electronic health records network that would allow for proper linking of health care

professionals in ensuring quality health care for all citizens. The Act aims at promoting investment into information technology and thus promotes safety, quality health care, and efficiency in health management (Davies & Collins, 2006).

What are the new notification requirements? Do you feel these are sufficient? Why or why not?

The new HITECH notification requirements include notification of patients in the occurrence of an unsecured breach. In case the breach has an impact on more than 500 individuals, then there is need for the HHS to be aware (Institute of Medicine, 2009). Such notification will allow for automatic posting of the name of the entity that is carrying out the breach on the HHS website. The local media also have to be notified considering various conditions. These requirements are greatly effective in ensuring that the patients are kept up to date of any breach and that the involved entities are brought to book. This allows for timely counteraction of a breach and securing of patient data.

What possible HIPAA violations could occur with portable PHI?

The use of portable PHI could result in HIPAA violation involving the breaching of individual private data. Portable devices such as mobile phones store data on the devices, either in the SIM card, memory card, or the onboard memory, exposing such information to breaching (Hebda & Czar, 2013). Such portable devices are not encrypted and thus the PHI could be shared by anyone who accesses the device. In addition, the devices lack authentication, thus allowing for accessibility of the information by any individual.

What strategies should be put into place to make sure these violations do

not occur?

Measures against HIPAA violations involve performing periodic assessments of the risks involved in mobile device use and ascertaining the presence of proper encryption, authentication, and physical protections that safeguard PHI. Installing and frequently updating anti-malware on portable devices could also prove helpful in preventing breaching of PHI (Institute of Medicine, 2009). In addition, biometric authentication tools could be adopted in the verification and authorization of individuals using portable devices such as mobile phones.

What are the requirements that a covered organization must take to be in compliance with HIPAA?

The HIPAA requirements for covered entities include obtaining of satisfactory assurance that any involved business associate will properly secure Protected Health Information (PHI). The Covered entities are also not expected to carry out monitoring practices. They are also expected to facilitate curing or termination of a contract in the case a known violation takes place (National Institute of Health, 2007).

References

Davies, C., & Collins, R. (2006). Balancing potential risks and benefits of using confidential data. British Medical Journal, 333(7563), 349–351.

Hebda, T., & Czar, P. (2013). Handbook of Informatics for Nurses & Healthcare Professionals (5th ed.). Upper Saddle River, NJ: Pearson.

Institute of Medicine. (2009). Beyond the HIPAA Privacy Rule:: Enhancing Privacy, Improving Health Through Research. Washington, D. C.: The National Academic Press.

National Institute of Health. (2007, February 2). To Whom Does the Privacy

Rule Apply and Whom Will It Affect? Retrieved from U. S Department of Health and Human Services: http://privacyruleandresearch. nih. gov/pr_06. asp