Security of health records essay examples

Law, Security

Introduction

One of the biggest challenges in health care is the maintenance of security of records. Since the inception of electronic health records, this challenge has escalated and health institutions have been required to adopt new strategies to ensure that data security is not compromised. In health care, the rule is that all physicians, nurses and medical practitioners must ensure integrity of the patients' data that they handle on a daily basis. At the University of Illinois Medical Centre, there is a large database of data involving personal and community data that has been preserved either for research purposes or that due to the patients. It is therefore critical that those handling this data utilize the most effective methodologies to ensure safety of this data from being mishandled or used for personal gains without approval by its owners or those responsible of maintaining this data. The focus is on the role nurses take in ensuring the security of this data. They are involved in the collection, maintenance and dissemination of this data and thus hold a great role in how it can be kept secured.

The introduction of HIT has had great implications in terms of maintaining security. The biggest challenge has been brought about by the fact that HITs provide accessibility for large amounts of data from a single point. This makes it easier to manipulate the data from a single point to affect many people. Similarly, the rate at which technology has been growing in recent years has been a major challenge since medical institutions have been required to frequently adopt new mechanisms to replace the obsolete ones. These frequent replacements have resulted to cost challenges especially for medium and small sized health care institutions. (Goodman, K. W. 2010)

Several security and ethical issues have resulted when the medical institutions fail to adhere to the demands of changing technologies together with those set by Health Insurance Portability and Accountability Act (HIPAA), (Rothstein, M. A. 2010). Some of these have been the use of patient data for personal gains by health care workers without the approval by the patients which has in most case sled to legal tussles between medical institutions and the affected patients. Similarly, invasion of networks by hackers and spies has compromised the quality and integrity of data. This is because such attacks on networks puts the attackers in an administrative position where they take control of modification of data including tapping it and storing it in their own systems or devices. While patients have in most cases recommended the use of electronic HITs, most of them have never taken concern of how the health institutions maintain security of their records. This lapse of openness between the institutions and patients has caused medical institutions to relax their efforts on ensuring security. According to Rothstein, M. A. 2010 this is has gone to levels beyond acceptable in the event that there were any. He attests that “ More health information is being disclosed to more entities for more non-medical reasons than ever before. Clearly, these disclosures are beyond the contemplation of the Hippocratic bargain.”(pg 8)

Medical institutions have also at times shared patient data with other medical institutions, research institutions, government agencies and legal agencies. This has been a big challenge since laws have not been set to clearly define what levels of sharing are not acceptable without the owner’s consent. In times, these records have been used for monetary gain by those

involved. The lack of transparency between the medical institutions and their patients has been the major factor. The owners of the data have no prior knowledge and may live to never realize how much their health records have been exploited and benefited some individuals or institutions.

The University of Illinois Medical Centre has set up more effective systems to ensure greater accountability between the institution and the patients concerning their data. This has been achieved through the evolution of software that is run from the patient's desktops or mobile phones that notifies the patient when their data is interfered with. This software enables the patient to know the location from where the data is being accessed and the legibility of the accessing individual or organization. Each patient is issued with an account name and password and in case they are notified of intrusion into their health records by suspect access, they are required to report to relevant authorities in the institution. Similarly, this institution has set up strict ethical guidelines for its employees to ensure they do not misuse their offices or privileges to interfere with health records. The institution has also partnered with Microsoft Company and Suns Microsystems to help in maintaining high-level modern technologies of data security both offline and over the World Wide Web.

These measures have been effective in ensuring the security of health records. Though, the institution needs to find an amicable solution to the security of manually stored data. While the above measures have ensured security of health records mostly from a technological view, the manually stored data has been the biggest loophole. The solution to this lies in the

institution streamlining the number of people who handle such data while also striving to eliminate the manual records completely. (Brown, B. (2009)

References

Brown, B. (2009). Improving the privacy and security of personal health records. Journal of Health Care Compliance, 11(2), 39–40, 68.. Retrieved from http://auth. waldenulibrary. org/ezpws. exe? url= http://search. ebscohost. com/login. aspx? direct= true&db= bth&AN= 36917377&site= ehost-live&scope= site

Goodman, K. W. (2010). Ethics, information technology, and public health: New challenges for the clinician-patient relationship. Journal of Law, Medicine & Ethics, 38(1), 58-63. Retrieved from http://www. ncbi. nlm. nih. gov/pmc/articles/PMC3266146/

Rothstein, M. A. (2010). The Hippocratic bargain and health information technology. Journal of Law, Medicine & Ethics, 38(1), 7-13. Retrieved from https://www. ncbi. nlm. nih. gov/m/pubmed/20446978/? i= 3&from=/20446982/related