Security and privacy grading criteria research paper example

Business, Management

Over time, there has been a lot of publicity when patients' medical data is accessed and disclosed to the media without authorization. To safeguard against this violation of patient privacy and security, the Health Insurance Portability and Accountability Act was enacted. The HIPAA stipulates the standards governing the handling of health information in terms of privacy and security. All health practitioners are expected to adhere to these regulations with prosecution in the case of breach (Vivian, 2009).

Compliance with the HIPAA is very crucial for the credibility and success of health institutions as patients have a better sense of security in as far as their medical information is concerned. HIPAA regulations govern not only issues of information confidentiality, but also the integrity and availability of information In order for the reinforcement of the HIPAA to be effective it is necessary for all the members within the health care institution to be actively involved. Organizations need to have clearly defined structures to assess and control privacy and security related risks (Mercuri, 2004).

The administration at St. John's Hospital takes pride in its sound policies and procedures for the protection of confidential client information. In fact, it serves as a model for other institutions in the area; however, printouts discarded in the restricted-access IS department are not shredded. On numerous occasions, personnel working late have observed the cleaning staff reading discarded printouts.

This portrays a case of violation of the HIPAA policy due to the fact that the restricted-access printouts are disposed of without being shredded hence making the confidential information in them available to unauthorized individuals who are the cleaning staff in this case. It is, therefore, a case that

requires immediate action by the hospital administration to ensure that it is immediately stopped and that it does not repeat itself.

This case indicates the importance of involving all members of the organization in HIPAA compliance efforts (Mercuri, 2004). This would have made it possible for a mistake to be reported to the relevant authorities in time. There seems to be a chain of mistakes that could be avoided if the necessary measures were put in place. The most important course of action is to equip the employees with knowledge on the various ways through which breach of the HIPAA policy may occur and the consequences of the breaches.

The people working in the restricted area of the IS department need to have known the risks involved in discarding unshredded restricted documents and this would have made them responsible for their actions. They would be able to know that, that kind of mistake would be prosecutable and could lead them into trouble with the law or even possible loss of employment (Moskop et al., 2005). The cleaning staff should also have known that reading the restricted documents was illegal, while, the night duty employees who witnessed the cleaning staff reading the printouts should be able to report the matter to the administration who in return should act accordingly and with immediate action.

The mistakes that may have occurred to bring about this kind of breach can be avoided if the hospital has a clearly defined management structure incorporating adequate training to allow for accountability and effective compliance with health information procedures and policies such as the HIPAA policy (Mercuri, 2004). According to the HIPAA policy, this case

warrants self-reporting owing to the fact that, the hospital been involved in violations involving availability and access of patient information to unauthorized individuals (Vivian, 2009).

Management plan and implementation

The management plan that would be appropriate would involve the establishment of a clear chain of command with clearly defined roles at each level, training of the hospital personnel on key policies and procedures governing the hospital industry including the courses of action in case of a breach.

Training and responsibilities

It is the responsibility of the information manager, and for this case, of the IS department to handle this matter on notification about the breach. He or she should be well equipped with knowledge in information technology procedures and data security measures. On the other hand, the personnel in the IS department should be trained and certified on the HIPAA policy. They should also update their knowledge in HIPAA by taking online classes often, say, twice a year. It is also necessary that all the employees in the hospital should have basic training in HIPAA protocols. Retraining and retesting is also important especially for those employees handling patient records (McLeod, 2007).

Procedures

The employees in the hospital work under specified procedures which ought to be effectively implemented and enforced to direct and control their

activities. These procedures include for instance the regulations pertaining to handling of patient records securely and confidentially. Frequent training, retraining and retesting on these procedures and policies is important to prevent possible breaches which could lead to dire consequences to the patients, personnel and the institution as a whole (McLeod, 2007).

Self-Reporting path

There should be a clear path through which reporting of breaches can be effected. In this case, it would be from the witnessing night shift employees to the IS department manager, to the human resources manager, to the administrator of the hospital and finally to the HIPAA enforcement body which is the Health and Human Services department (Vivian, 2009).

References

McLeod, L. (2007). Comply with HIPAA to Comply with the Joint Commission: Briefings on
HIPAA: Retrieved from. http://www. healthleadersmedia. com/content/HOM-91196/Comply-With-HIPAA-To-Comply-With-The-Joint-Commission##

Mercuri, R. T. (2004 July). The HIPAA-Potamus in Health Care: Retrieved from. http://www. notable-software. com/Papers/HIPAA. pdf

Moskop, J. C., et. al. (2005). From Hippocrates to HIPAA: Privacy and Confidentiality in
Emergency Medicine—Part I: Conceptual, Moral And Legal Foundations. Retrieved from. http://www. acep. org/assets/0/16/898/904/2196/2280/C798499F-59F2-42A3-A23A-A575767D4234. pdf

Vivian, J. C. (2009). HIPAA Breach Notification Rule: Retrieved from.

http://www. uspharmacist. com/content/c/16133/54