Analysis of security plan

Technology

Analysis of Security Plan

Executive Summary

Concerning the upcoming transition to Electronic Health Record (EHR) system, it is necessary to implement security measures to ensure that all processes flow seamlessly. This is necessary to maintain confidentiality, data integrity and prevent loss of data. The proposed security measures discussed include physical security of hardware, data security, confidentiality, access, disaster recovery, backups, business continuity planning, appointment of chief security officer, employee training methods, and institution of penalties for violating policies.

Proposed Security Measures

1. Physical security of hardware

Hardware includes the equipment used in the facility such as computers, printers, and other systems. It is necessary to guarantee the safety of hardware especially because most of the equipment is expensive. Physical security measures are essential to ensure that physical circumstances do not trigger severe losses or damage to the faculty.

2. Data Security

Data security involves back up of software to avoid threats such as hacking. It is essential to ensure that data is used for only its intended purpose, and by authorized personnel. The implementation of this proposal must be in line with existing data security laws and policies.

3. Confidentiality

Confidentiality is essential to ensure that client data is secure and safe from the public. Security officers must place boundaries and limit admission on certain types of information. Loss of confidentiality may result in patient discomfort or even serious consequences such as lawsuits.

4. Access

Access to information involving company operations should be restricted to a few security officers. Access of information and facilities must be in line with the logical expectations of the faculty.

5. Disaster Recovery

There must be measures to ensure that data recovery is done in a timely manner. The process involves a set of procedures that enable the continuation of service provision and transition to Electronic Health Record (EHR) system.

6. Backups

Backups of data are an essential security measure that ensures that there are backups of all company and client information. Loss of financial records or disappearance of clients' private information may have disastrous consequences on the credibility of an organization. Cloud computing methods are useful in contemporary backup services (Khameesy 1).

7. Business Continuity Planning

Business continuity ensures that the operations and plans of an organization continue in the shortest time possible despite the integration of the new EHR system. The transition to the new HER system is a localized short term procedure, but necessary security measures are necessary to ensure business continuity.

8. Penalties for Violating Policies

It is essential to institute stringent rules to enforce the security policies set. The chief security officers must outline penalties clearly to ensure confidence in operations and company objectives.

9. Appointment of Chief Security Officer

A Chief Security Officer will ensure the enforcement of the proposed measures. In addition, the person oversees all security departments and ensures proper enforcement of faculty laws and regulations.

10. Employee Training Methods

Employees must receive proper training to ensure that there are no misunderstandings in implementation of the proposed security measures. Technology-based training enables employees to understand the functioning of the new system.

Works Cited

Khameesy, Nashaat and Rahman, Hossan. A Proposed Model for Enhancing Data Storage

Security in Cloud Computing Systems. Journal of Emerging Trends in Computing and Information Sciences, VOL. 3, NO. 6, June 2012.