Report on hipaa compliance

Law, Security

Any hospital security engineer must observe the HIPAA privacy rule, which monitors the access and sharing of individual health information, as well as the HIPAA security rule, which comprises of the national security standards that safeguards the electronic health information. Since the hospital stores patient information using the paper based system, the manager will ensure that the implementation of electronic based health information systems is achieved within the shortest time possible (Keller & Associates, 2011). The paper records are always not secure and they contain massive irregularities and drawbacks towards the process of patient care and treatment. The paper based health records do not comply with the HIPAA standards, an amendment in the constitution of the United States. The HIPAA security rule guarantees physical safeguards, technical safeguards, technical policies, and network and transmission security towards the protection of patient health information (Envision, 2010). The legislation expects every hospital to safeguard the health information of a patient and uphold high standards to information privacy and confidentiality.

The security engineer should put emphasis on the execution of physical safeguards to the manual health records. The patient information should be secure and prevented from any unauthorized parties. The workstations and the electronic media to be implemented must be protected by policy's safeguards the privacy of the information. The management of the hospital must allocate funds to help in the transformation from the paper-based records to electronic health records. The manual records must be converted into a digital form and this will comply with the electronic protected health information (ePHI), a requirement of the HIPAA security rule.

On the part of the technical safeguards, the main roles include the access and authorization of electronic Protected Health Information. The manager must ensure that unique user IDs protects the information to their best. He is also responsible for implementing an emergency access procedure to the electronic information to save the lives of patients under circumstances that are a threat to their lives. Other key criteria that must be developed to guarantee safe access and authorization of the patient health information is the adoption of encryption and decryption standards together with the automatic log off procedures. In the process of pinpointing the security violations, the tracking logs will assist in monitoring the activities of both the hardware and the software (Keller & Associates, 2011).

The compliance of the HIPAA standards can only be guaranteed if they are technical policies to conceal integrity measures that assure no form of alteration to ePHI. The security manager will be responsible for adopting the IT disaster recovery mechanisms and offsite backup that helps in the process of recovery of lost health information (Beaver & Herold, 2004). The network and transmission security must be ensured to comply with the HIPAA since it will protect patient information from unauthorized access. Every procedure of data transmission should be secure to avoid the cases of exposure of confidential information as it is against the laws. The electronic health records serve a better purpose in service delivery compared to the manual records that require a huge office space and much time to be organized. In cases of fire emergencies, paper records are the worst since they are no backups and that can be a great loss to the hospital and the patient himself (Envision, 2010).

The key to successful compliance with the HIPAA security rule requires a sustainable risk assessment. The security manager has an obligation to perform accurate and thorough assessment to master any potential threats that can harm the integrity and confidentiality of the information. The security engineer must analyze potential environmental threats to identify the uncertainties fails to satisfy the standards outlined in the HIPAA security rules in guiding the hospitals. The security engineer should be well informed to avoid the use of outdated risk assessment strategies that will not help in the process of compliance. Before the introduction of the electronic patient information system kicks off, the engineer is expected to develop well-documented policies aligned according to the standards of the HIPAA (Beaver & Herold, 2004). The regulation will help the hospitals to successfully implement the new systems and dispose of the manual records in a professional and acceptable way. The structure of the hospital will also be structured to avoid conflicts of interest and assure responsibilities important for complying with the HIPAA standards.

The transmission of paper records to electronic form requires the use of digital forms. This is where the paper based health records are scanned and captured by digital cameras and saved in the computers for storage. During the process of conversion, the digital electronic records are stored in the database of the central server. To access the patient information, the use must be authorized by the responsible persons to avoid frauds associated with access. With this is mind, the security engineer will attain the specifics of compliance with the HIPAA security measures.

As expounded above, the success of the security engineer requires efforts,

hard work and determination to become a reality. The top hospital management must support the change and allocate funds that will assist the security engineer to achieve the goals of compliance with the HIPAA standards.

References

Beaver, K., & Herold, R. (2004). The practical guide to HIPAA privacy and security compliance. Boca Raton: Auerbach Publications.

Envision, Inc. (Nashville, Tenn.) (2010). Privacy & security: The new HIPAA rule. Nashville, TN: Envision Incorporated.

J. J. Keller & Associates (2011). HIPAA compliance manual for employers: A practical approach to programs and information security, 2011 edition. Neenah, Wis: J. J. Keller & Associates.