Hipaa security compliance

HIPAA SECURITY COMPLIANCE 1

HIPAA privacy and security rules work together for purposes of governing how a health institution handles and manages the information of a patient. The privacy rules of HIPAA cover the methods which a health practitioner can use to disclose the information of a patient (Beaver and Herold, 2004). The security rules of HIPAA provide the standards to use in safeguarding and protecting information of a patient. This is while permitting an appropriate use and access of the information under consideration (Carter, 2009). This leads to the promotion of the use of electronic health care information (e-PHI). This is a major goal of the HIPAA security system. The HIPAA security rules require that there is maintenance of an appropriate and reasonable technical, administrative and physical safeguard. This is with the intention of protecting the e-PHI. It is essential for an institution to (Beaver and Herold, 2004),

- Ensure the availability, confidentiality, and integrity of any e-PHI system that is created, maintained, and transmitted.
- Identification and protecting of any anticipated threats to the integrity and security of the e-PHI.
- Protection against the impermissible use of a patient’s electronic data.
- Ensuring that the workforce complies with these standards and procedures.

This is a memo that gives an overview of how the hospital organization can achieve HIPAA security compliance. The following are the steps the hospital organization can follow, for purposes of achieving HIPAA compliance.

The first step in working towards HIPAA compliance is to carry out a risk assessment. A risk assessment helps in equipping the hospital organization with accurate information where it stands, in regard to HIPAA security compliance (Carter, 2009). This helps the institution to decide on the levels of risks that are acceptable, and the levels of risks that are not acceptable. Furthermore, risk assessments help in revealing the various steps that the hospital organization can use, in achieving compliance with HIPAA security rules or guidelines (Beaver and Herold, 2004). Most health care organizations normally think that they have carried out a health care assessment, and in reality they have not. This is because a risk assessment must comprise of a study of all devices that store, maintain, generate, and transmit e-PHI. These health care organizations normally overlook devices or tools that are not on the network of the facility (Maiwald and Sieglein, 2002). For instance, the respiratory therapy tools normally generate information of a patient, and they are not connected to the information technology network of a facility (Carter, 2009). This is because they are normally plugged in, during the process of therapy, and taken out when the process is complete. An effective risk assessment program will analyze all these components of a health care organization, and identify all the acceptable and unacceptable risks that the organization faces (Carter, 2009).

The second step is collaborating with the stakeholders of the health care institution. Cooperation and collaboration amongst the stakeholders of the health care organization is an important element in ensuring that the organization would build effective and efficient HIPAA security compliance strategies (Beaver and Herold, 2004). Collaboration that occurs amongst the

decision makers of the health care institution is essential in ensuring that there is a lasting and successful alteration of the security and privacy policies of the organization (Keller, 2013). This is because people will have an opportunity to contribute ideas and opinions on how best to develop the HIPAA security compliance system (Carter, 2009). The contribution of these stakeholders helps in safeguarding against unrealistic or inadequate policies, especially the policies that would affect the care of a patient (Maiwald and Sieglein, 2002). The stakeholders of the health care institution have experienced different parts of a problem, and their contribution will help in getting a solution to the problem, and on how to improve the security of the system, or health care organization (Carter, 2009).

The third step is crafting a policy aimed at creating a solution that will make the organization to be HIPAA security compliant. These measures have to target the entire organization, and not a specific department (Maiwald and Sieglein, 2002). To achieve success, it is necessary to receive input from various departments of the hospital organization. This would help to develop a policy that serves the needs of the entire organization (Beaver and Herold, 2004). Take for instance, the lab department of the health care organization. The lab department receives very few visitors, when compared to the radiology department. When creating an HIPAA security compliance policy, it is necessary for the organization to write a policy that satisfies all their needs. For example, the organization can create a policy that, every computer screens that contain information of a patient should not be viewed by the public. This policy is applicable in a lab department, which has few visitors, but it is not applicable in a radiology department, which has many

visitors (Beaver and Herold, 2004). To serve the needs of these departments, the organization can create a password system that would allow employs and patients to view their information that is stored in the organizations computer database.

The fourth and the fifth steps involves a review of the purchase of capital tools, in the perspective of risk management and creation of the culture of accountability (Carter, 2009). When making decisions regarding capital purchase, it is essential that the organization should consider factors such as the total cost and the purchase price of the equipments (Keller, 2013). It is also important for the organization to consider the standards of security that these equipments come with. It is important to analyze the security features of the products, and judge whether they are compatible with the HIPAA security requirements. Developing a culture of accountability helps in encouraging the members of staff to report any problems that arise out of breaches of the HIPAA security compliance regulations. This will help the organization in improving its systems, and correcting the various mistakes that arise out of a breach of the HIPAA security regulations.

In conclusion, by following these five procedures, the organization will manage to create an effective solution that will help it to achieve HIPAA security compliance. Through these actions, the company would avoid the various laws suits and fines that may emanate from breaching the privacy of its patients, and employees.

References:

Beaver, K., & Herold, R. (2004). *The practical guide to HIPAA privacy and security compliance* .

Boca Raton: Auerbach Publications.

Carter, P. I. (2009). *HIPAA compliance handbook* . Austin, Tex.: Aspen Publishers/Wolters

Kluwer Law & Business.

Keller, J. J. (2013). *HIPAA Essentials* . Neenah: J. J. Keller & Associates, Inc..

Maiwald, E., & Sieglein, W. (2002). *Security planning & disaster recovery* . New York:

McGraw-Hill/Osborne.