New policy statements- hipaa

Business

New Policy ments - HIPAA Table of Contents Table of Contents 2 Introduction 3 Reviewing the Policy 4 Recommendations 4 New Policy for Permanent& Temporary Employees5

Additional Network Privileges6

Conclusion7

References8

Introduction

The environment of business is undergoing a constant change and along with it the customs of working are experiencing paradigm shift (Gitman & McDaniel, 2007). Previously, information in organizations in relevance to their business operations was stored manually in the form of written documents. But recently, this concept of storing information has witnessed a sea modification (Takai & Et. Al., 2011; Pozgar, 2007). Now-a-days, information in organizations is usually stored in computers. However, it was gradually recognized that even this method was not completely secured and information were accessed and misused from the computers without having the need to operate the computer physically from which the data was supposed to be accessed. Developments in technology were making the business operations and way of working easier whereas, at the same time those developments assisted in manipulating ways and misusing the information for one’s own benefit (Pesante, 2008).

Reviewing the Policy

The organization or company whose policies regarding information security need to be reviewed is in the business of insurance and deals with health insurance. The review is proposed in order to make certain that it fulfills the regulatory obligations and meet up to the obligations of the associated

standards as well as regulations.

The company comes under the Health Information Portability and Accountability Act (HIPAA) according to which any information regarding health requires to be protected. Taking into account the federal standards, patients should be capable of accessing information in relation to their respective medical records (HIPAA, 2007). Based on the nature of business operations, the company complies with the guidelines of HIPAA, HITECH, GLBA and PCI-DSS.

Recommendations

In spite of abiding by all the relevant regulations, the policy regarding accessing information by a fresh user and the prerequisite for passwords are becoming a grave concern for the supervisor of the company. Although the present policy of the company ensures high level of security but still it should structure a new policy. According to the new policy the request to access information by the new user along with the personal details and signature would be initially taken down. According to the policy, access would be provided only to the particular information or area specifically requested by the new user. There should be a time limit mentioned in the policy for accessing information by a new user and once the limit is over, the access should be automatically denied by the software. In case the user requires more time, a fresh request should be submitted again. In case of accessing any kind of sensitive information or administrator level information, manager’s approval should be made mandatory. This new policy in relation to a fresh user should be implemented in the organization.

New Policy for Permanent & Temporary Employees

According to the new policy the temporary employees need to abide by the

same procedure applicable for new users. But a separate guideline should be framed for the permanent employees. The guidelines would signify the implementation of a unique code provided by the organization to their permanent employees. The permanent employees are supposed to access information with the help of their respective unique codes. From the stated guidelines, it is evident that the policy regarding the permanent and temporary employees would not be the same.

Additional Network Privileges

The policy in case of requirement for additional network privileges by the employees would involve obtaining an approval for the same from the concerned manager of the department. Once the approval has been arranged, a temporary code would be provided to the employee for the day. According to this policy the additional network privileges would be arranged for permanent employees only.

According to the new information security policy statement of Heart-Healthy Insurance a fresh user should be provided access only after meeting the above mentioned security standards laid down in the policy statement. This is essential so as to protect the information from being accessed and used for unethical reasons. In addition, the new policy statement should clearly mention the need of the manager’s approval in case of accessing information in the administrator level. This would help controlling the access of a fresh as well as the existing users by the administration.

The policy with regard to the requirements for password was considered to be quite secure but minor alterations were still needed. A new policy needs to be developed in this regard according to which, in case of rearranging a password, the user should be asked for the previous password before making

changes. In case of feeding wrong passwords for three consecutive times, access to the site should be blocked and the user should reset the password from the mail id that is registered with the company. Thus, a new policy in regard to a fresh user and password should be developed incorporating the above mentioned modifications.

Conclusion

The above modifications have been recommended in order to protect the information of the company from being stolen or misused. The suggested new policy along with some modifications compared to the existing one are made in accordance with the US federal regulatory requirements as according to it a company should protect any kind of information related to its business functions and people involved. The suggested new policy meets up to the HIPAA Security Regulations and fall under the category of Technical Security Controls. According to the US federal regulatory requirements, companies need to develop a security program that would assist in protecting the information but no particular system chiefly has been stated to be adopted. So, it completely depends on the company to adopt security systems which they think would work best and would be compliant with the law as well.

References

Gitman, L. J. & McDaniel, C., (2007). The Future of Business: The Essentials. Cengage Learning.

HIPAA, (2007). The HIPAA Guide – Security and Privacy Policies. Home. Retrieved Online on October 10, 2011 from http://www. hipaaguide. net/

Pesante, L., (2008). Introduction to Information Security. Carnegie Mellon University. Retrieved Online on October 10, 2011 from http://www. us-cert.

gov/reading_room/infosecuritybasics. pdf

Pozgar, G. D., (2007). Legal aspects of health care administration. Jones & Bartlett Learning.

Takai, T. M., (2011). Managing Information Security Risk: Organization, Mission and Information System View. DIANE Publishing.