How Acceptable Use Policies Coincide with HIPPA Requirements

Submitted by Jody Rouse

DTEC 6823 Section 601

July 23, 2004

How Acceptable Use Policies Coincide with HIPPA Requirements

Preface

Use of the Internet and networked computers are resources available to many workers in today's work environment. Many of these resources allow the user to transmit confidential data especially within the health care field. However, many of these resources are not required or related to the worker's job. One solution to this problem is to develop an Acceptable Use Policy (AUP) that outlines the permissible parameters of employee computer use. To combat the transference of health care data through inappropriate means and the use of private health care data in a non-private way, a new act was passed. This act is called the Health Insurance Portability and Accountability Act (HIPAA). This paper will define AUP, HIPAA requirements and how AUPs coincide with HIPAA requirements.

Introduction

According to IDC Research based in Framingham, Massachusetts, 30 to 40% of Internet use in the workplace was not related to business. Websense, an employee Internet management software company, reported estimates of over $85 billion annually in lost productivity due to the lost time of wrongful use of the Internet. [5] Lawsuits have even been dismissed due to the use of an AUP. For example, when a company establishes a specific policy within an AUP stating the only use for company email is business related, chances are that company will not be held liable for slanderous email acts performed by one of its' employees. An AUP can be considered the first line of defense for such an act. Many would say the AUP keeps the honest people honest, and holds the dishonest accountable for their actions.

With health care security in mind, the HIPAA Privacy Rule became a federal law and has been a rather large issue. Anyone not compliant with the HIPAA Privacy Rule can face up to $250,000 in fines or up to 10 years in prison. HIPPA is a group of federal regulations that were developed mainly to protect the transfer of health care data.

The Development of an AUP

An AUP should clearly define acceptable and unacceptable use of all the company's resources. "This policy addresses activities such as sending offending emails to coworkers, running password crackers or other malicious applications on the network, installing unlicensed/pirated software, running file-sharing or streaming-media applications and infringing on copyrighted material." [1] An AUP policy should also specify the standards for access to the networks and secure use of usernames, passwords, and computer accounts. It simply warns that the company is paying for the all the resources in use and that the violators will pay if misuse is done. [5] Generally, an AUP is a written agreement, which outlines the permissible and non-permissible use of the network resources. However, this can be an electronic agreement that must be accepted before a user can access a particular resource such as a computer or the network.

Effective AUPs contain common characteristics. A few of these common characteristics are: comprehensive scope, clear language, adaptive content, extension to other company policies, enforcement provisions, consent and accountability. A comprehensive scope clearly defines what is covered by the AUP. This should include all personnel and resources. To obtain maximum enforcement an AUP must be of clear and concise language. This must address enforcement of the policy. An effective AUP must be of adaptive content, which will allow it to be readily revised without any complications. The extension of other company policies can be a rather large section within an AUP. This section will contain extensions to provisions of a standard company policy, HIPAA Policy and many more. There should be a signed consent for each individual, which lets the company know they are knowledgeable of the AUP and what's expected of them. The last section mention, accountability, should include contact information for anyone who has questions in regards to the AUP policy. This group will monitor compliance and enforcement activity. [5]

HIPAA Requirements and Development

HIPAA was enacted to protect the confidentiality and security of health-care data. This is done by establishing and enforcing standards and by standardizing electronic data change.[6] HIPAA can be separated into four basic requirements that must be fulfilled in order to meet compliance. These requirements as stated in the Journal of Health Care Compliance are "1. Ensure the confidentiality, integrity, and availability of all electronic protected health information created, received, maintained, or transmitted. 2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information. 3. Protect against any reasonable anticipated uses or disclosures of such information that are not permitted or required under the privacy rule. 4. Ensure compliance with the security rule by its workforce." [4]

When preparing for the HIPAA rule many companies will not have to start from scratch. To help with this, most companies can reflect on their current policies to check for the possibility of revising current policies to account for the new HIPAA requirements. Companies normally have many different types of policies already in place. Some examples of these policies are but are: Acceptable Use, Remote Access, User Account/Password, Firewall, and Network Policies. [1]

Many companies of today have already achieved an acceptable secure environment for their company. Only revisions to the company's current security policy will be needed to incorporate the new HIPAA rule. However, if there is a need to start fresh with a security policy then the six-step process as stated in NetworkWorldFusion is a good place to start. These six steps are: perform a risk analysis, create a security policy, implement proactive security measures, implement reactive security measures, make and test a business continuity/disaster recovery plan and maintenance. [2]

Effects of HIPAA on AUP

HIPAA affects AUP and many other policies directly. However, AUP dovetails with HIPAA. Both stress and support the importance of privacy. HIPAA strictly restricts the distribution of private health information without written consent. Incorporating HIPAA into an AUP is much like that of incorporating new rules into a revised AUP. For any type of implementation of security policies a top-down approach must be taken if the policy is to be taken seriously. With the issuing of the revised AUP, it will be the responsibility of the upper management to pass the correct information down to everyone. The upper management will also boost security awareness and ensure everyone abides by the new policy. [7]

There is a growing importance for having intact and up to date security policies. With the growing number of policies one can become lost within all the paperwork. Companies may begin to streamline their policies. There is no need for excess elaboration on passwords or sending private data electronically when you can streamline this into one policy, AUP. Companies can elaborate or add on a different section dealing with the extra needs to compliment the HIPAA policy. There are a few general goals of an AUP: clarification of Internet use, protect company against liability, avoid security threats, and encourage effective use of their resources. All four of these goals can be modified to better suit a company or a particular policy. A few specific items that may need to be altered to comply with HIPAA are the user accounts, passwords, encryption, access list and firewalls. A current company policy may state that all management has user names and strong passwords. Strong passwords consisting of at least 8 characters and contains 3 of the following four: upper case letters, lower case letters, numbers, and special symbols. The working staff such as Nurses may all have a general username and password that they share. This is something that can be revised within the AUP to state that everyone that must access a computer will have a specific user name and password. This will hold each person accountable for his or her actions. Instead the business will be held accountable if it cannot prove who committed the prohibited act.

One of the biggest issues to keep in mind is not to reinvent the wheel when its' not necessary. HIPAA rules don't actually contain much information about what technologies or security solutions organizations should use other than defining transaction codes and formats. Tweaking the current AUP may be all that's necessary for the beginning stages of going HIPAA compliant. [3]

Conclusion

The purpose of this paper was to introduce Acceptable Use Policy and the Health Insurance Portability and Accountability Act. It was also to introduce how these two coincide with one another. Revising for the new law HIPAA can actually be a smooth transition if previous policies are reviewed and revised first to account for this. Revising the older AUP can limit the amount of paper work and confusion many workers will have in keeping the different policies separate.

References and Citations

Websites, Books, and Journals

[1] Andress, Mandy. "An overview of security policies". 08 May 2002 http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci822681,00.html

[2] Spohn, Darren. "HIPAA and the small business". 08 March 2004 http://www.nwfusion.com/cgi-bin/mailto/x.cgi

[3] Frantz, Ken, "How Much Security Is Enough When It Comes to HIPAA?", Journal of Health Care Compliance, July-August 2003, Vol. 5, No. 4, pages 47 – 48.

[4] Pumo, Beth, "Now That the HIPAA Security Rule Is Final, Where Do You Go from Here?", Journal of Health Care Compliance, September-October 2003, Vol. 4, No. 5, pages 46 – 48.

[5] Principles And Practice of Information Security. Linda Volonino & Stephen R. Robinson. Pearson Education, Inc. 2004

[6] Principles of Information Security. Michael E. Whitman & Herbert J. Mattord. Course Technology Inc. 2003

[7] Network Magazine: June 2003 "A top-down approach for security", http://www.networkmagazineindia.com/200306/is15.shtml