Global Information Assurance Certification Paper

HIPAA Compliance:
Cost-Effective Solutions for the Technical Security Regulations
Tautra Romig, v1.2f

The Health Insurance and Portability and Accountability Act (HIPAA) became law in 1996. It was passed in response to the concerns about the confidentiality of personal medical information. The proposed standards contain administrative, physical, and technical security measures that are to help ensure the privacy of patient medical records.

The HIPAA regulations are far-reaching and will require vast resources of time and money. According to Gartner Group, at least 75 percent the time and money spent on achieving HIPAA compliance by 2004 will represent between 100 percent and 150 percent of their efforts and costs for the Y2K software modifications. The regulations that have already been published address the format and coding of information (Transactions and Code Sets) and the privacy of health information. The Department of Health and Humans Services (HHS) is said to be planning to publish the Administration Simplification security regulations as early as the beginning of 2002.

As each part of the HIPAA regulation is published, covered entities will have just over two years to comply. To be considered compliant, a covered entity must satisfy each of the regulations in a reasonable and appropriate manner. The regulations were drafted to be technology-neutral, thus allowing an entity to design their own unique solutions that it believes will satisfy the legislation. Due to the overlapping design of the regulations, it is possible to satisfy more than one requirement with a single solution. By finding the areas of the regulations where this occurs, a company can save money and labor costs.

While HIPAA is comprised of many different regulations, the objective of this document is to suggest cost-effective solutions to the proposed Technical Security Mechanisms regulation. The scope includes suggestions for a combined Windows NT and UNIX environment. Please note that there are numerous variations of each operating system, and certain techniques outlined in this paper might not be available or may function differently depending on the configuration of a company's systems.

Proposed HIPAA Technical Security Mechanisms for Data in Transit

There are a number of items covered by the HIPAA Technical Security Mechanisms Rule but in general, it can be divided into three subject areas: data authentication, data encryption, and external network protection. If a covered entity transmits protected health information (PHI) over a network, it must have the following security mechanisms in place:

- Integrity controls
- Message authentication

- Alarm
- Audit trail
- Entity authentication
- Event reporting

If the provider communicates with others via a network, it must also utilize one of the following implementation features:

- Access controls
- Encryption

It is possible to comply with more than one of the requirements simultaneously. For example, a company's solution for the Encryption requirement may also help to satisfy the Integrity Control regulations.

Integrity Controls

Integrity controls assist in ensuring that information has not been altered during transmission. If using a Windows platform, digital signatures can be utilized. MS Exchange and MS Outlook are able to support digital signatures with the use of the Secure Mime protocol. Digital signatures can also be used with Internet Explorer (IE) version 5.0 and above. IE can also use the standards protocols of Secure Sockets Layer (SSL) and Transport Layer Security (TLS) to ensure message integrity.

In UNIX, if one is using FTP for communications, some from of encryption should be in place. There are three basic types of encryption; hash functions, symmetric (private key encryption), and asymmetric (a combination of public and private key encryption). An administrator should choose an encryption package that best fits their environment. There are also third-party programs that combine SSL and TCP services.

While using encryption with FTP provides increased security, there are few additional points to consider. By default, login attempts when using FTP are not logged. This can allow hackers to crack passwords without detections. By simply enabling logging of FTP attempts, it can help identify unauthorized intrusion. FTP also allows users to initiate sessions on any host on the network. Administrators should consider granting restricted permissions for FTP use.

Message Authentication

By using message authentication, a company can provide a level of assurance through validation of a sender's message. An important primary step is to assign user specific network IDs and passwords. This is a basic element of defense in depth. Using unique user IDs as part of the authorization process serves as an additional hurdle for intruders before they can access your network.

Generally, employees should be strongly warned against sharing accounts and passwords.

Companies should also limit or even prohibit users from giving send-as permissions in the e-mail system. If an employee is granted permissions to another user's mailbox, by default they have the ability to send messages posing as the other party.

Assigning a range of TCP/IP addresses for specific departments or building floors can help towards validating a sender's message. If the sender's IP address does not reside within the pre-determined range of addresses, it could be an indication of a security issue.

When using FTP for communications on a UNIX platform, an encryption package should be used. This also helps to satisfy the above-mentioned Integrity Control requirement of HIPAA. Another authentication tool is the *tcpdump* program, which reads network traffic. It can be set to monitor specifically indicated values, such as unauthorized traffic on a specific port. The logs should be monitored and backed-up on a regular basis.

Alarms

The HIPAA regulations mandate that alarms be set to notify the appropriate individuals in the event of a security incident. The "Reasonable and Appropriate" stipulation in HIPAA will dictate what alarms are configured for each company's specific environment. Whether using Windows or a UNIX platform, alarms can be set for precise events. Possible events for which to set alarms are:

- *A specific number of failed logins.* A systems administrator might also want to monitor successful logins in addition to unsuccessful logins. By monitoring successful logins, it can provide evidence that a user did indeed gain access after numerous failed logins.
- *When a user is granted Domain Administrator privileges on a Windows system.* Only a very few users should have this level of access. A user account with such a high level of access can be very detrimental if it falls into the wrong hands.
- *If a user logs in as root on a UNIX system.* In only very rare occasions should anyone have access to the system using *root*. Best practice is to create alternate, less powerful superuser accounts instead of allowing such unrestricted access as with *root*.
- *When the contents of specific log files are reaching maximum capacity.* The UNIX command, *audomon* monitors the amount of remaining free space on the file system. By default, it will send a message to the administrator that the file will soon reach its maximum size. However, it is generally best to be notified before the file system is full.

Audit Trails

HIPAA requires medical records to be held for six years or more. During that time, several practitioners and other medical staff will need access to those records. By constructing an audit trail, a company can monitor the access activity of specific medical files.

Log files are the mechanism by which to record audit trails. Jonathan Tomes, a noted HIPAA expert states, a "record of who did what, from which terminal, on what machine, when, with what objective and whether successful or not should be maintained". Properly documenting

logs in this way is crucial for corrective and/or legal action, as it reveals the sequence of events of the incident in question.

In any environment, choosing not to monitor non-critical files can help save space on the network. Also, using a centralized monitoring system can help reduce the labor cost of monitoring.

In a Windows environment, an administrator should consider the following:

- *Enabling Event Auditing is done within User Manager.* Various events to consider monitoring are: authentication, creation/deletion of sensitive information, access rights administration, and any additional actions that might affect the security of the system.
- *Save the logs on a separate system or disk on a regular basis.*
- *Use a third party monitoring and filtering tool.* There are several to choose from and they vary in scope and price.

If your company operates on a UNIX platform, several tools are included in the operating system or available at no cost, including: (The file paths listed below are unique to the Linux platform.)

- **/var/run/utmp** The *utmp* file records who is currently logged on the system. As users logout, their entries are automatically removed. Confirm that only root can access these files.
- **/var/run/wtmp** This records all successful logins and logouts, and displays the user ID, the machine name, and the time and origin of the activity.
- **/var/run/btmp** Bad login attempts are logged in the *btmp* file. Only root should have access to these files.
- **/var/adm/sulog** This records all successful and failed attempts to become another user.
- **Syslog** The *syslog* utility manages system messages and includes a hostname, a timestamp, the program name, and the body of the communication. It also provides for centralized reporting which can be quite a time saver.
- **TCP Wrappers** This tool supplies access control for most Internet services, and can also log connection activity. Monitored services include *telnet* and *ftp*.

Entity Authentication

The HIPAA regulations require that covered entities can authenticate the identity of other users with whom they communicate electronically. Whether you run Windows or a version of UNIX, there are several best practice points to cover in regards to Entity Authentication:

- Require unique user IDs and complex passwords.
- Set passwords to expire at least every two months.
- Create a formal process to grant user accounts.
- Create a formal process to disable user accounts immediately upon an employee's termination.

- Employ digital certificates if applicable.

User accounts are the last line of defense in protecting your network. Regardless of how well you secure your systems, all the policies and procedures in the world will not help if your users share their personal account information!

Event Reporting

Since HIPAA requires the protection of patient health information, event reporting plays a fundamental role of complying with the regulations. Recording specific events that occur on a network is part of the HIPAA requirements that can be concurrently satisfied when the auditing and alarm requirements are met.

By using the Event Viewer in Windows, administrators can check for abnormal activity. According to Microsoft, Windows has the "ability to audit and report on a variety of system and security events". An administrator might consider monitoring the following with Event Viewer:

- Logons and logoffs
- Directory access
- Access to the critical files and folders

With so many events to monitor, this process can be quite labor intensive. Therefore, it is advised to monitor only the files that contain patient identifiable information. In UNIX, many of the same commands that are used to create audit trails can be used for event reporting:

- /var/run/utmp
- /var/run/wtmp
- /var/run/btmp
- /var/adm/sulog

The retention time for the logged event reports depends on the sensitivity of the monitored files. The more critical the protected information is, the longer the reporting logs should be retained. Each company has the ability to determine what is reasonable and appropriate in this regard.

The proposed HIPAA security regulations will make the protection of patient information everyone's responsibility. Network administrators will have to correctly configure their systems, install security patches, and keep current with the latest security vulnerabilities. Employees will have to choose strong passwords and be conscious of social engineering. Complying with HIPAA will also necessitate substantial technical resources. Both Windows and UNIX have built-in mechanisms, which if enabled, would help to comply with a variety of HIPAA regulations. Since the cost burden of complying with the regulations will be entirely up to the covered entities, utilizing cost-effective solutions will be of the utmost importance. By using the technical resources already available on their systems, a company can greatly reduce the cost of complying

with HIPAA.

REFERENCES

Boran, Steve. *The Security Cookbook.* URL: http://www.boran.com/security/

Department of Health and Human Services. Administration Simplification. April 12, 2000. URL: http://aspe.os.dhhs.gov/admnsimp/nprm/sec09.htm

Duncan, Matthew. *Gartner Group HIPAA Survey 2Q01 Results: Spending and Consulting Use,* September 6, 2001.

Microsoft. *A White Paper: Health Information Security*, February 2001. URL: http://www.microsoft.com/business/health

Phoenix Health Systems. "HIPAAdvisory". URL: http://www.hipaadvisory.com/

Public Law 104-191, AUG 21, 1996, Health Insurance Portability and Accountably Act of 1996 URL: http://aspe.hhs.gov/admnsimp/nprm/sec09.htm

SANS Institute. *GIAC LevelOne Security Essentials*. June 2001.

Tomes, Jonathan. *The Compliance Guide to HIPAA and the HHS Regulations*, Veterans Press, Overland Park, KS, 1999.