Security Guidelines
The Impact of CMS in the Insurance Industry

Coty Pearson
July 30, 2004
GSEC Practical Assignment
Version 1.4b option 1

Table of Contents

Abstract

Every day companies are being evaluated and audited on their security guidelines and procedures. Many companies are not sure against which guidelines they are actually being measured. In the health insurance industry, some health insurance carriers manage both public and private contracts. By holding public contracts, this automatically holds them to the highest standards. There are several guidelines and standards to which they must adhere in order to maintain compliance with Federal and State agencies. Determining what standard to align with in creating a stable security guideline is becoming more difficult, yet exciting.

Centers for Medicare & Medicaid Services (CMS) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) are the driving force behind the push for security in the insurance industry. Determining the guidelines of CMS and HIPAA help the insurance industry determine appropriate levels of security. CMS follows the HIPAA and ARS guidelines when auditing or assessing a health insurance carrier. Understanding ARS and HIPAA can help one to align with the highest of standards in the insurance industry.

Introduction

CMS business partners are located at many sites throughout the United States. Some CMS business partners perform both the Claims Processing and the Claims Data Processing work for CMS. (As part of the Certification and Accreditation (C&A) process) A technical certification assessment process, called the System Test and Evaluation (ST&E), has been developed to ensure CMS data center's sensitive information in all forms is protected appropriately.

A CMS business partner is a corporation or organization that contracts with CMS to process, or support the processing of, Medicare fee-for-service claims. Insurance carriers that maintain public contracts for Medicare beneficiaries have to ensure compliance with CMS. Annual audits must be performed to ensure all security guidelines are being met and a higher rating of security must be upheld. The higher rating was chosen since loss or change of CMS information could have a negative impact on CMS and compromise the privacy of Medicare beneficiaries.

Choosing the appropriate security guidelines with which to align with is very critical. CMS uses the ARS guideline, which was created with FISMA and HIPAA in mind. The ARS guideline is what an insurance carrier maintaining public contracts should adhere to; this would help affirm compliance with CMS. I plan to discuss CMS guidelines and legislation affecting CMS, Access Controls of the ARS, and the auditor's process of assuring compliance.

Legislation Affecting CMS

CMS has noticed the information being passed between agencies and businesses are at greater risk in our time. Technology is growing at a rampant rate and so are the skills and number of hackers. With more hacking tools becoming widely available and easier to use, governance's had to be passed to maintain a level of security. CMS had to ensure that the privacy of sensitive information was being upheld. Any business partner with CMS must adhere to the governances as well. There are many laws that have been passed with which government agencies must adhere to. There are currently twenty-four Acts that have been passed with which government agencies must comply. CMS, as a government agency has tried to create a security guideline with all in mind, but heavily influenced by FISCAM, OMB Circular A-130, IRS 1075, HIPAA, and FISMA.

Federal Information Systems Control Audit Manual (FISCAM) was used in the past by CMS when doing financial internal audits and audits of business partners.

FISCAM had four phases:

1. Planning Phase
2. Internal Control Phase
3. Testing Phase
4. Reporting Phase

In the planning phase, the entity would provide details to the auditors (a contracted company hired by CMS) of their infrastructure. The auditors would determine which systems would be at risk and focus on those systems for the audit. The auditors must provide the audited entity with a plan of what type of audit and details of the audit being performed. Once the entity has agreed, the auditors move on to the testing phase and begin evaluations of the systems. FISCAM had six controls to the general evaluation and testing phase: Security program and management for the entity, access controls, maintaining a change control for application development, system software, segregation of duties, and service continuity. (United States General Accounting Office, FISCAM p.22) The testing and evaluation phase for application controls helps ensure that all transactions are valid and being handled efficiently. FISCAM was headed in the right direction but was left too broad, therefore open to interpretation.

Office of Management and Budget (OMB), Circular A-130 was mandated to manage the resources of federal information systems. “OMB was required to help manage and help other agencies set their own security guidelines due to the Paper Reduction Act.” (Panetta) OMB tries to help manage the development of security guidelines for other agencies to operate more efficiently.

IRS 1075 was written to protect Federal Tax Information and Returns. There is a section in the IRS 1075 that pertains to computer security. This “requires any party that houses any Federal Tax Information or Return Information to follow the Common Criteria of security.” (Internal Revenue Service, p. 20) Following NIST or ARS guidelines, should provide adequate protection.

Health Insurance Portability and Accountability Act of 1996 (HIPAA) was passed to “ensure privacy, accountability, and integrity when dealing with any form of private health or sensitive information.” (Department of Health & Human Services, HIPAA p.7) This Act was passed with several different guidelines and deadlines to which an agency dealing with this type of Private Information must adhere. This Act had a significant impact on all state, federal, local, and private agencies dealing with private and sensitive health information. This topic alone is very in depth. The intentions of this act were primarily to distinguish what the requirements were in dealing with private health information (PHI). CMS is not the only one that must adhere to HIPAA, private insurance agencies, doctors, and hospitals all must comply with HIPAA. This Act, if not followed, can result in stiff penalties.

Federal Information Security Management Act of 2002 (FISMA) will eventually require all government systems to align with a set of NIST guidelines. Although this Act is not a key driver it is on the horizon. This Act should be taken into consideration when considering security guidelines.

CMS's Acceptable Risk Safeguard (ARS)

The health insurance carriers that are business partners with CMS are driven to higher levels of security and performance than other carriers. The health insurance industry that is not Medicare related does not have as stringent guidelines to follow for security. CMS's security guideline, ARS, dictates how your infrastructure is designed and how your security is deployed. Regardless of what type of health insurance carrier you are, you should have stringent guidelines to protect the members private health information. Most companies tend to do what they need to do and not what they ought to do. CMS requires you to do what you ought to do. The ARS is an outline of security levels that should be met for information security controls. The security controls that will be summarized range from physical security to disaster recovery.

"Past experiences of government agencies and business partners coupled with industry standards compiled the ARS." "The ARS was developed with a defense in depth approach, least privilege access." (Department of Health & Human Services, ARS p. 1) Employees should be given as little security access as possible to start. If the job requires the to have more access, then the access should be granted.

To follow the ARS a determination of what security level each of the systems measure. To do this, one would have to follow CMS's Information Security Levels. Knowing what types of applications are being housed on the systems will help determine what level of security must be followed.

Physical Security Standards

Physical Security Standards are in place to ensure the protection of physical resources, and the information these resources contain." (Department of Health & Human Services, ARS p. 3) Depending on your level of security depends on how you limit access by the public or unauthorized individuals. Lower security guidelines may only be required to have locks on the doors and windows. If the entity is measured at a high standard, not only would the facility need to be secure, but the data centers as well. This security could be implemented by controlling access through physical authentication devices. Some physical authentication devices are combination door locks, biometrics devices, and smart cards. "Maintenance personnel only should be allowed access to HVAC systems, telephone infrastructure, and network closets. Authenticating physical devices should also restrict this access." (Department of Health & Human Services, ARS p. 3) Cameras should monitor computer room access and a record of access should be kept. "If a system requires repair off-site, all storage media should be removed and unusable media destroyed. On-site repairs should be performed in a protected and monitored environment." (Department of Health & Human Services, ARS p. 4) All servers should have backup power redundancy. "Security personnel should monitor control alarms and remedial action taken in the event of an alert." (Department of Health & Human Services, ARS p. 5) A policy and backup contingency plan must be written for all control alarms. The policy should contain levels of alerts and levels of reporting for the alerts. If there is damage to the surrounding environment, damage must be reported and corrective action taken. To prevent unauthorized access to the network through the physical layer, all unused ports should be disabled.

Personnel Security Standards

Personnel access should be given based on the role of the employee. Personnel should only be given physical access to the areas that are required to carry out the responsibilities of the job. Access should be granted on a need to know basis only. Less access is best. This is a difficult area for which to set standards due to the many different roles that there could be. For example, a claims processor should not have access to the network closet to change which port they are plugged into. Each employee should be dealt with on a case by case basis.

Organizational Practice Security Standards

Organizational practice means security standards are implemented at an organizational level. There are several different standards that should be met at an organizational level. To start, every job duty and role of the user must be defined. The responsibilities of the user must be understood and written to protect both employer and employee. There should be policies written for acceptable use to prevent any misunderstanding. Suggested policies for acceptable use would be: Internet use, corporate email use, password, security, privacy and network use. With every acceptable use policy there should be action items that would take place if a violation of the policy occurred.

Each computer or system that contains PHI or has network access should have a warning banner. You should also clearly display the banner at all entry points and public facing web sites. This banner should state that the person logging in must follow the security policies that are set by the organization. The banner should notify the user that they may be monitored and any violation could have legal penalties. A display should also appear once the users are authenticated to the network allowing them to accept or deny a privacy policy. By accepting the privacy policy the user could continue to utilize the system on the network. If the user denies the privacy policy, record should be made, network access stripped, and corrective action taken. The organization should also implement an encryption standard that has a minimum of 128-bit for all Intranet and extranet applications containing PHI.

Password policies for a system with a high level of security system should require a minimum password length of eight characters. The password must contain at least one each of numeric, alphanumeric, and special characters. The password should be set to expire and force the users to change the passwords at least every sixty days. “The users should not be allowed to reuse a password that they have previously used in the past six passwords.” (Department of Health & Human Services, ARS p. 9) Following this policy cause them to create unique non-identifying passwords that are not easy to crack. The administrator should have a unique and modified login ID and follow the same password guidelines.

Information Sensitivity Assessments (ISA) should be prepared for all systems. The assessment should take place in the design phase of a new project. “The ARS controls the schematics of the systems and equipment under this standard.” (Department of Health & Human Services, ARS p.8) One must adhere to CMS guidelines and procedures for testing, updating, and managing your system. “Documentation should also be available for the systems purpose and configurations.” (Department of Health & Human Services, ARS p. 11) Any change to these systems should be documented in a change control environment.

Security Management Standard

In order to manage information security and security programs effectively one must have a Security Management Standard. This standard should outline security training for all personnel on basic security issues. Management measures to ensure security should also be taken. Once an employee is terminated, the employee should be escorted out of the building and denied any access to the facility indefinitely. Terminated employees network access should be taken away to ensure that the systems or information is not compromised.

If a contractor is required to write a business application or work on a system, the contractor should sign a confidentiality statement if working with any PHI is a possibility. Contractors should be given limited access and rights to the system. In order to select a contractor, one must have looked at several other contracting firms and presented why this contractor was chosen. The appropriate management must approve the decision and all CMS security policies must be followed.

If you feel that a system could be compromised because of an employee or situation of an employee, rights should be reviewed and restricted prior to notification. This should be approved by the Information System Security Officer (ISSO). Some of the circumstances could occur during or after a performance review of the employee, or because of irrationality of the employee. These are normally circumstances that you would not have to be dealt with on a day to day basis.

"Remote offices of the organization should follow all of the CMS guidelines." (Department of Health & Human Services, ARS p. 16) The infrastructure of the interconnection between the remote site and the parent site should be approved and meet all guidelines of CMS.

If something indicates that PHI or a system has been compromised one must report it appropriately. The compromise should be handled as an incident and must be handled within the company and then reported to CMS. A procedure should be in place for incident response handling. Once a determination has been made that there was a compromise, being careful collecting the data is crucial. The notification of a compromised system or PHI should be escalated through a chain in an organization and the forensics of the incident handed over to the appropriate team. Ensure that the information that has been collected from the compromised machine was rightfully obtained in order to taken legal action.

Certification & Accreditation Standards

In order to become a CMS business partner one must pass Certification and Accreditation at least every year. "In this process the company must assign security responsibilities of the systems to staff that is experienced in the technology or platform of the systems." (Department of Health & Human Services, ARS p.17) An Information Security Risk Assessment (RA) should be performed on each system containing Medicare information. "Documentation should be developed to list the risk and safeguards of the system." (Department of Health & Human Services, ARS p.17) The safeguards are countermeasures of the risk. This could help eliminate incidents from even happening.

The prospected or renewing business partner must also have a contingency and disaster recovery plan. This plan should be current and fully tested. Testing should take place any time there is a major system change and scheduled once a year. Every since 9/11 everyone has realized even the unimaginable can happen to you. You must be prepared for emergencies or disasters or you may not be able to recover from them. If you have proper contingency planning and disaster recovery you should be able to be restored at another location with little or no loss to revenues and system information.

Network Security Standards

Network security standards are very important. This is the hardware and infrastructure that will keep your Major applications (MA) and General Support Systems (GSS) secure and available. Preventive measures should be taken to reduce the risk of unauthorized access. Implementing the proper network security and setting adequate perimeters around your trusted network should reduce the risk of exposing systems through compromising technology like wireless or modems. The perimeter should be guarded by stateful inspection firewalls. The firewall could be either software or hardware based. Rules are set on the firewall that states what traffic it will allow and deny. The firewall designates what ports are accessible to external sources coming in to the trusted network. The firewall should review all packets that are received and ensure that they are approved based on the rules that are set. If a packet is not approved it will be dropped. There should be an application proxy in place that will allow the application to be served up to the proxy. When a request comes in for a page on the companies web site, instead of the user going to the web server and getting the page, the proxy will get the page and return it to the user. The user will never leave the proxy.   The company should implement a DMZ structure utilizing the firewall. The DMZ should have a firewall in front of the company to separate the Internet and their trusted network. Then another firewall should be in place to separate the internal domain from the external domain. The DMZ normally consists of domain controllers and web servers. The web servers should house external web sites only. If the site has the functionality to access back end information from legacy systems or internal applications, the internal firewall should only allow the proxy server to go and get that information. Only a one way trust should be set up between your external and internal domains. This structure keeps external users from accessing information on the internal domain.

Desktop modem installations by users should be prohibited by policy. An alternative to desktop modems would be for the company to have a remote access server (RAS). RAS would be able to serve many employees and would allow proper staff knowledgeable in the technology to properly secure the remote access.

Hand held personal computers should be restricted from being plugged into computers accessing the network. Network information should not be stored on handheld personal computers. Personal or company information should not be allowed to be synchronized with any handheld device.

System Access Security Standards

Upon initial setup of the system, recommended lock down methods should occur to strengthen the security of the operating system or platform. The default administrators' account should be renamed with a unique login ID. This unique login ID should not have anything identifiable with the person setting up the box. If there are default user accounts that are not being used they should be disabled. Any default accounts that are being used by the system or application should be renamed. For example, if one is running IIS, the IUSR and IWAM accounts could be used to hack into an application. If you rename this account it is harder for the attacker to find which account has the properties of the IUSR or IWAM account. Don't forget to change the description of these accounts and document what the changed accounts function is. The access control list (ACL) should be configured to only allow read rights to the public, and only where necessary. They should not be able to look at system files and objects. Services are enabled by default, browse through the services and disable any services that are not required to run the server. If at a later time it is necessary to house an application that will need one of the disabled services, the service can then be enabled. If it is not required that a system or an application have access to a file system, that access should be disabled. If there is a protocol that the server is not utilizing that protocols should be disabled. Leaving the protocols enabled only adds to the number of access points an attacker could use.

Administrative rights with full access could be dangerous if given to someone that is not fully trained on the platform. The existence of too many administrators could lead to changes being made that may overwrite a change another administrator was making. This is why change control and communication is very important. A segregation of duties among the administrators should help eliminate this from happening. For example, one could still have one administrator with full access but then allow the other administrators limited rights. The administrative user group should be monitored any time you feel you may have a system breach, when requested by auditors/management, or at least every seven days. Monitoring this group would ensure that unauthorized administrators have not been added to the group. Logging of administrative activities should be enabled on all servers.

Once a user has a failed a predefined number of logon attempts the user account should be locked out. The security level defined for your systems determines the length of lock out. If the system has a low security level lockout would be for five minutes after five failed attempts. A moderate security level would disable access for ten minutes after three failed logons. If there were three of these cycles, it would lock out the account and require reset by an administrator. A medium security level would disable access for fifteen minutes after three failed logons. If there were three of these cycles, it would lock out the account and require reset by an administrator.

Virus scanning software should be installed and actively scanning. Low security level requires scanning of critical system files once a week and at boot time. Moderate security level requires that the software be installed and configured to run every twenty-four hours and at system boot. The software must be configured to do a full scan. High security level must be configured the same as moderate level, but scheduled to scan every twelve hours.

"System boot access must be denied for removable media, unless the media is required." (Department of Health & Human Services, ARS p.26) System BIOS settings should be locked with an approved password that falls under the organizational password requirements.

"If a user has a mainframe session that has been inactive for fifteen minutes, the user would be disconnected from the mainframe." (Department of Health & Human Services, ARS p.26) This prevents someone walking by with less access and using the inactive users' computer to access legacy systems on the mainframe that they may not be authorized to view. If the user had used the desktop locking feature it would not be a risk, but a safeguard.

"System maintenance must be performed to install any vendor hotfixes, patches, service packs, and virus definition files. Once the vendor has supplied one of these security measures, they must be tested in a test environment. If the test is successful, an installation is required within seventy-two hours of release. If the test fails, a sufficient work around must be performed within the seventy-two hour release time. " (Department of Health & Human Services, ARS p.27)

VPN links must be established through the VPN client. This would allow remote access if necessary. If remote access is not necessary, do not perform this task. VPN traffic must be encrypted at the organizational encryption standard (128-bit). Additional security should also be used to ensure the person using the VPN is a valid user. Some other security controls would be password combination or biometrics. Remote administration can also be available through VPN link and should also follow the same standards for any remote VPN connection.

"Remote access through a modem should be set up with the call back capability." (Department of Health & Human Services, ARS p.29) The remote server must be able to verify the source and ensure it is a valid location. It is preferred that the Medicare Data Connection Network (MDCN) be used. If the application being accessed remotely requires authentication the user would be assigned a user ID. If the person accessing were a contractor or vendor, the account would be set to expire every six months.

Application Security Standards

An application that is being published through SSL must be set to require the minimum 128-bit encryption determined by the organizational practice. If this setting is not configured the user could connect at a lower encryption level. The application should also be configured to use authentication methods that are approved under the organizational practices and follow the standard guidelines. Using a certificate and authenticating to the application provides a higher level of security.

All mail, including attachments, should be sent encrypted. Any information that is related to the company or CMS is considered high risk and also requires a digital signature. CMS does not allow any PHI that is Medicare related to be passed over the internet unless the information is fake/test data used for data center programming or in communication with CMS.

"In order for a business partner to utilize persistent cookies approval must be acquired through Department of Health and Human Services (DHHS)."(Department of Health & Human Services, ARS p.31) A persistent cookie collects and stores information on the clients' computer and is accessed by the server using CGI scripts. The cookies could be storing anything from browsing habits to personal information that may have been entered on a form.

Data Security Standards

"Data security standards should be used for data in transit and rest." (Department of Health & Human Services, ARS p.32) These additional security requirements should be used in conjunction with the other security requirements in the ARS. "Data security standard is written to protect both electronic and hard copy data. All data in rest and transit should be encrypted and protected through ACL's. When the data is being transmitted the data should be sent through secure communication that adheres to the Network security standard as well." (Department of Health & Human Services, ARS p.32)

A schedule should be in place for system backups. Partial or incremental backup will run daily. It is recommended that a full backup be performed every other day. The media that is written to with data during a back up must be labeled with name, date, time, type of backup and put in the correct cycle of the backup schedule. The label must be externally visible on the media. All magnetic media must be stored in a secure location. If the media will be disposed of, proper sanitizing of the media is required. The media should not be able to have information recovered during any forensics.

Any paper information that is dispersed must be done with management approval. "During transport of the hard copy it must remain in a secure location. The document should be marked with its security level. If the hard copy will no longer be used it must be finely shredded and securely disposed of." Department of Health & Human Services, ARS p.33) Monitoring of this process is recommended if this process is contracted out to a vendor. The vendor will normally put secure holding bins in secure areas to place hard copy data into the bin when ready for disposal. All bins always remain locked and have a small slot to place the hard copy in. Once a week the data should be picked and securely transferred to the vendors facility for monitored disposal.

Vulnerability Assessment Security Standards

Vulnerability assessment security standards define standards of deploying intrusion detection systems (IDS) in your network. This standard will outline how you should be collecting information on possible intrusions or network abuse, reporting the information, and proper incident handling of the evidence.

IDS should be deployed in your network on the realm of the DMZ. IDS is in place to monitor and detect any type of suspicious root activity or request, suspicious HTTP request, failed logon attempts, backdoors, stack smashing code, enumeration, suspicious FTP, etc. These are activities that could be used in a hacking attempt on your system. The IDS would provide the ability, when monitoring, to catch that activity when it starts. Alerts should be configured to notify the administrator. An active IDS system would allow you to kill that traffic immediately. A passive IDS would only log that information it is up to the administrator to continue collecting the correct information for a forensics case. Once a case is compiled with all the information, legal action could be pursued. Just because one has an IDS device does not mean that it should be your only guide. One should continue to monitor system event logs for suspicious activity as well. If it is found that a system has been compromised, the administrator should take immediate action. Correction of the vulnerability or removing system from the network should help mitigate further risk.

It is critical that authenticity of the data is confirmed. If the information has been changed this could compromise the integrity of the entity holding the information as well as CMS. File comparisons should be performed for the data and ACL's. Any changes should be sent to the administrator to monitor.

Self-penetration testing should be performed on a routine basis. The testing should take place no less than quarterly. In addition to the vulnerability penetration testing the organization should perform an overall evaluation yearly. All findings in the penetration test should be documented and corrective action taken and documented.

Auditing and Logging Security Standards

Proper and standardized logging and auditing should be in place to affirm consistency and accuracy. Proper auditing and logging is a requirement if inspection of the system becomes necessary during a compromise. Proper auditing and logging also helps to ensure that segregation of duties is being upheld.

Auditing should be turned on to log any type of account management information such as successful/failed logons, changes to local security policies, etc. System management functions should also be logged, such as reboot, shutdown, etc. These logs must be kept on the system for 90 days and old logs archived for one year. This policy should be followed for system and application logs.

To further assure that data is not modified inappropriately any modifications or deletion of critical files should be logged and monitored. Accessing of the file should be logged to ensure that authorized users only are accessing the files.

Monitoring of perimeters is required, such as firewalls. The firewall must be configured to log scans, packet modifications, system management errors, user management, and packet denials.

An automated method to review logs should be in place to review system, application, and perimeter logs. The utility should allow you to look for suspicious or abusive activities on your network. This method of reviewing logs works well in conjunction with monitoring IDS logs. While reviewing logs it is found that PHI or financial information has been released against standards, a record must be made. The record must contain the name of the sender and recipient, date, and time.

Behind the Scenes of an Audit

CMS requires yearly evaluations of their business partners to ensure they are in compliance with all governance's that pertain to the insurance industry and personal information. CMS contracts the audit process to third party consultants. CMS, the business partner, and the consultant group all work together to compile a list of what will be audited. This list is determined based on risk or level of information that is being housed on each server or application. If the application or server houses or accesses any Medicare information, it must be looked at during the audit.

The consultant group composes a script after all information has been gathered. The script contains all systems that will be evaluated and how they will be penetrated. The script will list all types of vulnerability assessment tools they plan to use and how in depth they will go for on each scan. The consultant group can go as far as owning the entire system, uploading hacking tools, or DOS with the business partners permission. Once the script is completed, CMS and the business partner must approve the script before the audit begins.

It is apparent audit day has arrived when all of the system administrators and management are running around frantically. Well, actually, it should not be like that at all. One's security should not begin when the auditors arrive; it should be part of your every day practice. It might be wise to think of security as practice because it will never truly be achieved. New vulnerabilities are introduced every day; one must be willing to quickly adapt to change in order to stay abreast of the changes. An audit should not be considered dreadful but a learning experience. The process should be taken very seriously, but it needs to be kept in perspective. The auditors are not there to make one look bad, they are only there to ensure that one has the most stringent security in place that fits the environment. The audit may begin as a penetration test against all outward facing sites and entry points. During this penetration test, they are also making sure that one is meeting all of the requirements that are set in the ARS. Some of the methods that are used in this phase of penetration testing could be port scans, password guessing, testing to ensure all known vulnerabilities have been patched. After the external scan, the internal scans begin. The internal scans are normally more in depth because they are given all of the information regarding the systems they will be assessing. The same methods are also used for the internal scan. A vulnerability scan is also performed on each system. For those of you who have run vulnerability scans on your own systems know that this could bring many false positives to the surface.

After the penetration and assessments are completed, the auditors meet with the business partners to discuss the findings. The findings are the results or their testing. At this time one is able to contest any of the findings that are presented to you. One must be able to provide documented evidence of either why it is not necessary or unadvisable to implement in your environment, or that it is implemented or in the process of being implemented. For example, if the auditors show that you are missing MS03-007. You would have the opportunity to research this finding. In your research you would find that this patch only applies to Windows Server 2000 SP3 and earlier. Your system is running SP4. The patch is included in the service pack upgrade; therefore, it is a false positive. One needs to go through all of the findings and then one has a set amount of days to answer the findings. In answering the findings, one must document that it is false or that one has taken corrective action. Not taking corrective action will lead to repeat findings the next year, which can cause CMS to reconsider ones value as a business partner. You should have a main point of contact that ensures all of the groups with findings are answered in the appropriate time frame.

The final report is composed once the time frame for the answers has expired. The final report of the findings is presented to the business partner and CMS by the consultant. Even though the time has expired to answer, one should still take corrective action on any of the findings that have been presented. These are vulnerabilities, if they were not aware before, they are now. Again, not taking corrective action will only lead to repeat findings the next year. In the past, companies have had a difficult time making the cultural change of seeing the auditors as a momentary annoyance, leaving the company to get back to what they feel is real work after the auditors leave. As we know this is not the case, and, they are seen more as a partner. They are here to do the same thing as the system administrators: They are here to make sure that CMS is secure, and the system administrators are here to make sure their companies are secure.

Conclusion

All insurance carriers must follow HIPAA guidelines. CMS adds another layer of requirements to its business partners. It causes its business partners to adhere to more stringent security guidelines. CMS has a greater impact on insurance carriers that maintain government contracts because it sets them at the same standard as CMS. All insurance carriers, Private or Government ought to have a strict regimen in ensuring privacy of its members. It is good business to be able to ensure your customers privacy and offer security. Companies that are not contracted by the government have seen that there is a need to align with a set of security guidelines. Many companies, for their security guidelines, have adopted the ISO17799. It is a full-bodied security program; the ARS would fit in this security guideline set as well. It would be a good recommendation to align with the ISO17799, ARS, and NIST.

CMS currently appears to be behind the times with Internet activity. CMS currently does not allow any PHI to be transmitted over the Internet. This requirement does not seem to have affected the private insurance carriers. CMS may never allow PHI over the Internet, I hope that in the future CMS will come up with a combination of security levels to ensure that the mail containing PHI is passed securely to the intended party. This would allow business partners to send secure PHI over the Internet. I think that a feasible measure would be to pass any mail containing PHI to a secure server, and act similar to WebDAV. The mail would be sent to a secure holding with a unique path with username and password to allow the recipient to come and pick the message up on a secure channel. Private health insurance companies are allowed to send PHI over the Internet if it meets the requirements that are set forth in the HIPAA guideline for electronic mail.

CMS has not directly impacted the Insurance Industry from a private business perspective. However, CMS has definitely impacted insurance carriers that maintain public contracts. Because insurance companies with public contracts are striving for more stringent security guidelines and safeguards, it is driving private insurance carriers to also strive for that type of security excellence. Often companies with public contracts also maintain private contracts. Public carriers are excelling in the security and technology field largely due to all of the requirements of CMS. Insurance companies that maintain public contracts are being recognized for their advancement in technology and security. Public carriers are pulling private carriers up to their standards. This has been an indirect effect from CMS and all the mandating forces that govern CMS. Setting security guidelines for the insurance industry is no longer part of a future requirement. The requirements have become part of today. To continue in the insurance business today, one should begin to live and breathe security.

References

Northcutt, Stephen. "Passive Vulnerability Scanners". Cyber Defense April 2004. (2004): 14-18.

Sturdevant, Cameron. "Privacy is good business". EWEEK October 13, 2003 (2003): 67.

Department of Health & Human Services, Centers for Medicaid & Medicare Services. *"CMS Information Security and Privacy Legislation Resource".* Version #2. February 25, 2003. http://csrc.nist.gov/fasp/FASPDocs/program-mgmt/legislative_resource.pdf. (July 22, 2004).

Panetta, Leon E. "Circular A-130". No. 2. http://clinton1.nara.gov/White_House/EOP/OMB/html/omb-a130.html. (July 22, 2004).

U.S. Department of Homeland Security, "Federal Information Security Management Act". 2002. http://www.fedcirc.gov/library/legislation/FISMA.html. (July 22, 2004).

Department of Health & Human Services, Centers for Medicaid & Medicare Services. "CMS Information Security Acceptable Risk Safeguards". Version 1.1. March 14, 2003. http://csrc.nist.gov/fasp/FASPDocs/risk-mgmt/ars.pdf. (July 22, 2004).

United States General Accounting Office, Accounting, & Information Managemet Division. "Federal Information Systems Control Audit Manual Volume I: Financial Statement Audits". GAO/AIMD-12.19.6. 2001. http://www.gao.gov/special.pubs/ai12.19.6.pdf. (July 22, 2004).

Internal Revenue Services. "Tax Information Security Guidelines for Federal, State, and Local Agencies". OMB No. 1545-0962. Rev 3/99. http://www.irs.gov/pub/irs-pdf/p1075.pdf. (July 22, 2004).