CMS

CENTERS for MEDICARE & MEDICAID SERVICES

HIPAA Compliance Review Analysis and Summary of Results

Centers for Medicare & Medicaid Services (CMS)
Office of E-Health Standards and Services (OESS)

Reviews 2008

Table of Contents

Introduction

During 2008, CMS performed reviews of ten Health Insurance Portability and Accountability Act of 1996 (HIPAA) Covered Entities (CEs) to verify compliance with "Security Standards for the Protection of Electronic Protected Health Information (ePHI)," found at 45 CFR Part 160 and Part 164, Subparts A and C, commonly known as the Security Rule. CMS initiated these reviews based on complaints filed against the entities, identification of potential Security Rule violations through the media, or recommendations from the Department of Health and Human Services (HHS) Office for Civil Rights (OCR). Each CMS review is specific to the CE based on the nature of each complaint. Using this approach, CMS assessed compliance with select areas of the Security Rule at each of the ten CEs. Based on the complaints, CMS's particular focus for these reviews included, but was not limited to, the following areas:

- Risk analysis and management;
- Security training;
- Physical security of facilities and mobile devices;
- Off-site access and use of ePHI from remote locations;
- Storage of ePHI on portable devices and media;
- Disposal of equipment containing ePHI;
- Business associate agreements and contracts;
- Data encryption;
- Virus protection;
- Technical safeguards in place to protect ePHI; and
- Monitoring of access to ePHI.

Each review involved an on-site analysis at the CE which included an assessment of compliance with multiple areas of the Security Rule. Prior to each site visit, CMS provided an information request list outlining the initial documents required for the review. A list of the type of information that might be requested is available on the CMS website as "Information Request for On-site Compliance Reviews". Please note that the posted information request document is not a comprehensive list of applicable investigation/review areas nor does it attempt to address all non-compliance scenarios.

During the reviews, CMS conducted interviews with individuals at the CEs. The goal of these interviews was to understand the nature of the incident, discuss corrective actions taken since the incident occurred, and identify existing or new processes which protected the confidentiality, availability, and integrity of ePHI. In addition, CMS examined documented policies and procedures which supported the security of ePHI. For selected key processes, CMS conducted analysis to assess whether the processes were operating effectively and as intended. To maintain visibility of the process, CMS provided regular status reports to the CE throughout the review, and discussed potential gaps in compliance with their representatives.

At the completion of the analysis, CMS provided a report which outlined identified gaps in compliance and provided technical assistance to help the CE increase their overall level of security around ePHI. Areas of technical assistance included suggestions for improving security controls beyond the purview of the specific reported incidents.

After completing reviews on ten CEs, CMS performed an analysis on the identified compliance issues to determine areas where CEs appeared to struggle to comply with the Security Rule. These areas included:

1. Risk Assessment
2. Currency of Policies and Procedures
3. Security Training
4. Workforce Clearance
5. Workstation Security
6. Encryption

To help other CEs identify and address these areas, CMS has prepared this report which outlines the details of these six overarching compliance issues and provides recommended solutions as a guide to help increase compliance with these select areas of the Security Rule. Please note that, as with the sample information request, this document is not a comprehensive list of applicable investigation/review areas nor does it attempt to address all non-compliance scenarios.

Risk Assessment

164.308(a)(1)(ii)(A)

Risk analysis - "Conduct accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI) held by the covered entity."

Through this implementation specification, the Security Rule requires Covered Entities (CEs) to conduct a risk assessment to identify risks and vulnerabilities to ePHI. The standard does not dictate how CEs are to perform the risk assessment or provide specific insight into the approach for assessing risk around ePHI. To help CEs implement this specification, CMS has provided additional guidance through a paper in the security series, titled "Basics of Risk Analysis and Risk Management." Although this approach is not required, it defines steps to address the key tenets of an effective analysis of risk. CEs are expected to analyze their environment and assess potential risks and vulnerabilities which may affect the confidentiality, integrity, and availability of ePHI. The risk assessment process lays the groundwork for CEs to build their policies and procedures around addressing these risks.

CMS observed significant variations in the methodology and performance of risk assessments. Specifically, CMS observed the following conditions during the reviews:

- CEs did not perform a risk assessment;[1]
- CEs did not have a formalized, documented risk assessment process;
- CEs had outdated risk assessments; and,
- CEs did not address all potential areas of risk.

CEs did not perform a risk assessment

CEs did not understand the key elements of an effective risk assessment. CEs did not conduct a documented analysis targeted at risks to the confidentiality, integrity, and availability of ePHI. In some cases although management had identified certain risks within the organization, no formally documented risk assessment covering ePHI risks throughout the organization existed.

CEs did not have a formalized, documented risk assessment process

CEs did not have a risk assessment process for identifying and addressing risks to the confidentiality, integrity, and availability of ePHI.

CEs had outdated risk assessments

Many of the CEs that performed risk assessments conducted those assessments at a point between August 1996, when Congress enacted HIPAA, and the point when the law required CEs to comply with the Security Rule (either April of 2005 or 2006 depending on the size of the CE).

[1] "The Global State of Information Security 2008" noted that only 57% of survey respondents from the healthcare provider industry said that their organization conducts enterprise risk assessments at least once a year.

CMS noted that these organizations had not reviewed and updated the risk assessment since their initial analysis to reflect the changes in their environments.

CEs did not address all potential areas of risk

CEs did not include all applicable areas or systems within their organization in the risk assessment process. In general, these organizations either did not maintain an accurate inventory of systems which stored, processed, and transmitted ePHI or did not properly identify the applicability of components of the organization.[2]

Recommended Solutions

In order to increase compliance with the Security Rule, the following solutions are recommended:

1. CEs should develop and formally document a policy requiring the completion of a periodic risk assessment covering all systems and applications which store, process, or transmit ePHI. The policy should require that these risk assessments be completed at least every three years or whenever there is a significant change in the environment, including, but not limited to:

   - Introduction of new systems;
   - Significant upgrades to existing systems;
   - Retirement or disposal of systems;
   - Physical relocation of IT assets;
   - Introduction of new lines of business; and,
   - Reorganization of the CE's management or business structure.

2. CEs should develop and formally document supporting procedures for conducting risk assessments. One of the key initial steps in the risk assessment process is to identify the systems which store, process, or transmit ePHI. CEs must also identify components of the organization which handle ePHI and the physical location of IT assets that contain ePHI. Lack of an accurate inventory of systems and an understanding of business use of ePHI will prevent the CE from establishing an effective risk assessment process.

   After CEs have an accurate inventory of systems and an understanding of the business use of ePHI, the CE should develop procedures outlining steps to:

   - Identify the criticality of the system and its data;
   - Identify threats to the system;
   - Identify vulnerabilities on the system;
   - Analyze the controls that have been implemented, or are planned for implementation;
   - Identify the probability that a vulnerability may be exploited;
   - Identify the impact of a successful threat exercise;

[2] "The Global State of Information Security 2008" noted that only 38% of survey respondents from the healthcare provider industry maintained an accurate inventory of where they stored patient data.

- Assess the level of risk;
- Identify additional controls to mitigate identified risks; and,
- Document the results of the risk assessment.

Section 3 of NIST SP 800-30, “Risk Management Guide for Information Technology Systems” provides guidance on the steps to conduct an effective risk assessment. Additionally, "Basics of Risk Analysis and Risk Management," a part of CMS's security series, provides risk assessment guidance for CEs to improve their level of compliance with the Security Rule.

For guidance regarding the process of identifying criticality, NIST has developed SP 800-60, "Guide for Mapping Types of Information and Information Systems to Security Categories," which outlines steps to categorize the data on the system and information system itself, and Federal Information Processing Standards (FIPS) Publication (Pub) 199, "Standards for Security Categorization of Federal Information and Information Systems" which outlines steps to categorize the information system.

3. CEs should conduct a formal, documented risk assessment for systems and applications which store, process, or transmit ePHI. This assessment should comply with the policies and procedures developed in accordance with Recommendations 1 and 2. The resulting risk assessment should be approved by management. The approver should not be the individual responsible for completing the risk assessment or involved with the day to day operation of the assessed system. CEs should retain evidence of this approval, within the document itself if possible.

4. After CEs complete their risk assessment, they should identify corrective actions for any weaknesses they identify during the process. These plans should identify steps to mitigate the residual risks identified in the risk assessment.

5. CEs should re-perform the risk assessment, following established policies and procedures, every three years or whenever there is a significant change in the environment. Although this re-performance should assess all areas of risk, CEs should be certain to focus specifically on areas in which they have implemented corrective actions since the previous risk assessment. Additionally, CEs should focus scrutiny on new or modified systems and facilities.

Currency of Policies and Procedures

164.308(a)(8)

Evaluation – "Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule, and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart."

Through this standard, the Security Rule emphasizes the importance of continued effectiveness of security processes driven by documented policies and procedures. The purpose of this standard is to ensure that CEs continue to comply with the Security Rule and maintain the confidentiality, integrity, and availability of ePHI. There are no implementation specifications for this standard, so the Security Rule allows for flexibility in the approach that CEs may use to address it.

During the reviews, CMS identified compliance issues with the requirements of this standard as well as with the CEs' documented policies. Specifically, CMS observed the following conditions:

- CEs did not review and approve security policies and procedures within the time frame that their policy required;
- CEs did not document evidence of their review and approval of policies and procedures; and,
- CE's documented procedures were inconsistent with procedures followed by CE personnel.

CEs did not review and approve security policies and procedures within the time frame that their policy required

Most CEs had a documented policy which required periodic review and approval of security policies and procedures, though the definition of "periodic" varied between organizations. Despite these policies, CMS noted that CEs did not complete the review and approval process within the time frame they defined. Through the failure to complete these reviews, management had little assurance that the documented processes were operating effectively, complied with the organization's regulatory and operating environment, or matched current processes carried out by CE employees. For additional details on this latter point, please see the section entitled "CE's documented procedures were inconsistent with procedures followed by CE personnel" within this report.

In general, the lack of a formalized review and approval process was the primary cause for the failure of CEs to maintain current policies and procedures. The processes that were in place at CEs varied between internal groups and these groups had not documented these disparate processes. Additionally, individuals with specific responsibilities related to the policies at the CEs were often unaware of the requirement to review and approve policies and procedures.

CEs did not document evidence of their review and approval of policies and procedures
Often, issues with outdated policies were compounded by a lack of documented review, even in cases where a review may have occurred. Some CEs were able to provide informal evidence of review, such as email messages; however, this varied among organizations.

Again, this issue often stemmed from the lack of a formalized review and approval process. Additionally, CEs did not identify a tool or mechanism to document review and approval of policies and procedures. Frequently, organizations lacked something as fundamental as a standardized format for documenting policies and procedures.

CE's documented procedures were inconsistent with procedures followed by CE personnel
At some CEs, CMS noted that the process executed by the organization's personnel did not match the documented procedure. In general, the process had evolved and the documentation had not followed. Although not as common, there were also instances where the documented procedure represented the correct process but individuals charged with carrying out the process had not followed the documented steps.

In cases where the policy lagged behind the process, CEs were often out of compliance with their periodic review policy. In cases where individuals carried out a process incorrectly, these individuals often were unaware of the documented procedure.

Recommended Solutions
In order to increase compliance with the Security Rule, the following solutions are recommended:

1. CEs should develop and formally document a policy requiring that management periodically review policies and procedures. This policy should outline the maximum timeframe between reviews as well as require management review when there is a significant change to systems or the environment.

2. CEs should develop and formally document a procedure for conducting periodic reviews of policies and procedures. This procedure should allow management to conduct these reviews in a timely manner, compliant with the CE's documented policy for frequency of this type of review. The process should outline the steps for management to:

   - Identify policies and procedures for which they are responsible for reviewing;
   - Gather the most recent versions of these policies and procedures;
   - Assess the currency of the documented policy or procedure against the organization's operational and regulatory environment;
   - Implement updates to the policy or procedure as necessary;
   - Document evidence of their review and approval; and,
   - Disseminate the updated policy or procedure throughout the organization.

If possible, this process should be standardized for all departments or groups which are responsible for maintaining policies and procedures.

3. CEs should develop a standard format for documenting policies and procedures. This format should accommodate multiple types of documents, but should maintain information on revisions to the document, the dates of each revision, the individual who revised the document, the date of the most recent approval of the document, and the individual who approved it.

4. CEs should evaluate their process for disseminating and adopting updated policies and procedures to determine if employees are aware of updates. As part of this process, CEs should develop tools to manage policies and procedures as well as aid management with their review. If possible, organizations should deploy tools to centrally manage and distribute policies and procedures. Ideally, these tools should allow individuals to register for automated notifications when management updates policies or procedures. In addition, updates to organization-wide policies and procedures should be communicated to all employees. These updates should be reiterated in refresher security awareness training.

5. CEs should conduct periodic evaluations, either internally or by engaging a third party, to assess the effectiveness of policies and procedures and their compliance with the Security Rule. CEs can perform this assessment through a number of methods including interviews, process walkthroughs, and/or assessment of the actual results of these processes. Larger organizations should consider a formalized review conducted by internal audit. Smaller organizations should consider less formal means of evaluation or engagement of a third party. The individuals who conduct these evaluations should not be the same as those responsible for carrying out the process and should maintain a reasonable level of competence to properly perform the assessment.

Security Awareness and Training

164.308(a)(5)(i)

Security awareness and training - "Implement a security awareness and training program for all members of its workforce (including management)."

Through this standard, the Security Rule emphasizes the importance of security training for the entire workforce, including management. Additionally, CMS **HIPAA Security Guidance for Remote Use of and Access to Electronic Protected Health Information** (page 4) recommends that CEs
"Develop and employ proper clearance procedures and verify training of workforce members prior to granting remote access."
Specifically, the Security Rule requires awareness training for all personnel. Regardless of the safeguards a CE implements, those safeguards will not protect the ePHI if the workforce is unaware of its role in adhering to and enforcing them. Many CE's security risks and vulnerabilities, as identified and analyzed in their risk assessments, are internal threats, both accidental and malicious.[3] This is why security awareness training is so important.

During the reviews, CMS identified compliance issues with the requirements of this standard as well as with CEs' own documented policies. Specifically, CMS observed the following conditions:

- CEs did not have formally documented policies related to training;
- CEs did not track and retain evidence of training completion;
- CEs did not conduct security awareness training prior to granting user access; and,
- CEs did not conduct security refresher training on a regular basis.

CEs did not have formally documented policies for training
CMS noted that CEs did not formally document policies for initial security awareness training and annual security awareness refresher training. In most cases however, CMS did note that an undocumented process was in place requiring the completion of initial and refresher security awareness training.

CEs did not track and retain evidence of training completion
CMS noted that CEs had a formal or informal process in place requiring employees to take security awareness training, either prior to receipt of system access for new hires or at least annually for existing employees. However, the CEs could not provide evidence that every employee completed the training within the required time frame.

[3] "The Global State of Information Security 2008" noted that of 34% of respondents say that employees are the likely source of incidents over the next 12 months. This is higher than that of former employees (16%) and hackers (28%).

CEs did not conduct security awareness training prior to granting user access
CMS noted weaknesses in CEs' security awareness training and account provisioning processes. Specifically, CMS noted instances where new hires were granted access to systems that stored, processed, and transmitted ePHI prior to completing initial security awareness training.

CEs did not conduct security refresher training on a regular basis
CMS noted that some CEs did not have a process for providing annual security awareness refresher training to individuals with access to ePHI.

Recommended Solutions
In order to increase compliance with the Security Rule, the following solutions are recommended:

1. CEs should develop and formally document policies for the development, administration, and monitoring of initial and annual security awareness training courses. The policies should require that all newly hired employees complete initial security awareness training prior to gaining access to ePHI. This requirement should include employees and temporary workers as well as contractors and vendors, if not previously arranged through a Business Associate agreement.

   Additionally, the policy should require that any individual with access to ePHI complete security awareness refresher training at least annually.

   Further, the policy should require that management review and revise both the initial and refresher security awareness training courses at least annually to ensure currency with the organization’s environment. Additionally, as CEs identify new risks through the risk assessment process, they should incorporate these potential threats in the trainings to further awareness.

2. CEs should develop and formally document a procedure for initial and refresher security awareness training. This procedure should be coordinated with the account provisioning/management process. The procedure should require verification that new users have completed initial security awareness training prior to granting them access to ePHI and require security awareness training on an annual basis thereafter. Additionally, processes should be designed, documented, and put in place to monitor compliance. To support this process, CEs should develop tools for monitoring compliance. If possible, CEs should deploy an automated tracking system to capture key information regarding program activity (e.g., individuals' completion dates). The tracking system should capture this data at a high level, so that CEs can use such information to provide enterprise-wide analysis and reporting regarding awareness, training, and education initiatives.

To effectively implement this recommendation, CEs must tightly integrate the initial hiring process with the account provisioning process. They must also integrate the training compliance monitoring process with the account management process.

3. CEs should develop and formally document procedures to monitor course completion and escalate issues involving users who have not completed their annual security awareness training timely. Specifically, pre-determined sanctions should be applied to those individuals who are not in compliance with this requirement. These sanctions may include notification of the user's supervisor when initial deadlines pass without completion and revocation of the user's access when final deadlines pass without completion.

Workforce Clearance

164.308(a)(3)(ii)(B)

Workforce clearance procedure – "Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate."

The workforce clearance implementation specification instructs CEs to determine if access of a workforce member to ePHI is appropriate[4] This access should be restricted to only those individuals who have a reasonable and appropriate need to utilize ePHI. CMS has provided further guidance specific to access to ePHI using tools or devices outside the physical boundaries of the organization, in the CMS **HIPAA Security Guidance for Remote Use of and Access to Electronic Protected Health Information.** We recommend that CEs "Develop and employ proper clearance procedures and verify training of workforce members prior to granting remote access." This guidance addresses developing proper procedures to perform clearance activities on those individuals who require remote access to ePHI. In general, these clearance procedures are manifested as background investigations on personnel.

During the reviews, CMS identified compliance issues with the requirements of this implementation specification. Specifically, CMS observed the following condition during the reviews:

- CEs granted access to ePHI prior to completing background investigations.

CEs granted access to ePHI prior to completing background investigations.
Most CEs required completion of a background investigation on all employees who handled ePHI. In general, these background investigations were handled as part of the new hire process. The breakdown occurred when the CE had not completed the background investigation by the time employment began. Many CEs processed access requests within the first few days of employment. As such, organizations granted access to ePHI prior to the completion of a background investigation.

Recommended Solutions
In order to increase compliance with the Security Rule, the following solutions are recommended:

1. CEs should identify positions which require background investigations based on risk. Using the risk assessment as a starting point, CEs should identify positions with access to ePHI and determine if access by an individual whose potential background investigation may not return

[4] "The Global State of Information Security 2008" noted that 61% of survey respondents from the healthcare payers industry conducted personnel background checks.

clean would pose a "reasonably anticipated use or disclosure of such information."[5] The listing of positions which require a background investigation should be maintained and periodically reviewed based on organizational or environmental change.

2. CEs should develop policies and procedures for performing background investigations. The policy should incorporate the listing of positions that must complete a background investigation and include:

    - Details regarding the results required for employment;
    - A requirement to complete the investigation prior to gaining access to ePHI; and,
    - The types of checks the CE will perform to verify the appropriateness of an employee's access.

    After the policy is in place, CEs should develop and formally document a procedure to support implementation of the policy. The procedure should outline the steps for completing the investigation, retaining evidence of the results, and integrating the completion with the account provisioning process. To protect individuals from privacy concerns, CEs should not submit a request for access until the background investigation is complete and clear.

3. CEs should consider implementing a reinvestigation process for positions they identify as high risk. This process should mirror that of the initial background investigation with modifications for sanctions if the results violate policy. After implementation, CEs should develop a policy which outlines how often they will complete the reinvestigations.

4. CEs should require background investigations from vendors and third parties who have access to ePHI. This should be part of the requirements established in Business Associate Agreements with these vendors and third parties.[6]

[5] Health Insurance Portability and Accountability Act of 1996, Part 164, Subpart C, Section 306(a)(3) (2003)

[6] "The Global State of Information Security 2008" noted that 68% of respondents from the healthcare payer industry are either "somewhat" or "not at all" confident in their partners' information security practices.

Workstation Security

164.310(b)

Workstation use - "Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information."

164.310(c)

Workstation security – "Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users."
These standards stress the importance of protecting workstations that store, process, or transmit ePHI. Additionally CMS has issued the **HIPAA Security Guidance for Remote Use of and Access to Electronic Protected Health Information**. On page four, the guidance recommends that CEs "Require use of lock-down or other locking mechanisms for unattended laptops." Because of the increased use of laptops and other portable devices and the ease with which threat sources can gain access to these devices' data, preventing these systems from "walking away" is critical in protecting ePHI. An effective risk assessment is paramount in identifying the potential risks and vulnerabilities to the workstations and other tools within the CE's environment. Additionally, these controls are not limited to laptops or other devices designed for use outside of the CE's facilities. CEs must consider risks in these facilities and identify any reasonable and appropriate controls to protect the confidentiality, integrity, and availability of EPHI.

During the reviews, CMS identified compliance issues with the requirements of these standards as well as with CEs' own documented policies. Specifically, CMS observed the following conditions:

- CEs did not have a formalized, documented policy or process for verifying the security of workstations;
- CEs were not complying with their policies and procedures for securing workstations; and,
- CEs did not deploy the necessary tools to implement documented policies.

CEs did not have a formalized, documented process for verifying the security of workstations
CMS noted that policies and procedures for securing the workstations existed; however, there was no documented process to outline the steps for management tests of compliance with their policies and procedures.

CEs were not complying with their policies and procedures for securing workstations
CMS noted that the process executed by organizations' personnel did not match the documented policy or procedure. In general, the process had evolved and the documentation had not

followed. There were instances where the documented procedure represented the correct process but individuals charged with carrying out the process had not followed the documented steps.

CEs did not deploy the necessary tools to implement documented policies
CMS noted that organizations had documented policies and procedures for physically securing laptops and other portable systems; however, they had not provided employees with a means to implement these policies or procedures.

Recommended Solutions
In order to increase compliance with the Security Rule, the following solutions are recommended:

1. CEs should develop a policy outlining workstation classifications and the types of physical security controls the CE requires for each class of workstations. This policy should take into consideration the results of the risk assessment to identify threat sources and potential environments where workstations exist.

2. CEs should develop a policy for performing security walkthrough. This policy should identify a specific timeframe for performing the reviews, the types of reviews the CE will perform, and the scope of the walkthroughs (e.g. facility locations or specific areas of single facilities). CEs should consider identifying sensitive areas in their facilities which require additional scrutiny.

3. CEs should develop procedures for the types of walkthroughs they perform in their environment. These procedures should specify the steps for performing walkthroughs as well as documenting the results of each. This documentation should include details regarding who performed the walkthrough, the date the individual performed the walkthrough, and the results of the process.

4. CEs should evaluate the results of the walkthroughs. The results can then be used to identify areas where the CE may need to deploy additional employee training or physical security controls.

5. CEs should outline physical security requirements in initial and refresher security awareness training. The training should specifically outline employees' responsibility for securing workstations, laptops, and other portable devices.

Encryption

164.312(a)(2)(iv)

Encryption and decryption - "Implement a mechanism to encrypt and decrypt electronic protected health information."

This implementation specification outlines the use of encryption as an additional layer of protection around ePHI. Additionally on page five of the CMS **HIPAA Security Guidance for Remote Use of and Access to Electronic Protected Health Information**, we recommend that CEs

"Require that all portable or remote devices that store EPHI employ encryption technologies of the appropriate strength. . . Deploy policy to encrypt backup and archival media; ensure that policies direct the use of encryption technologies of the appropriate strength."

Because of the proliferation of portable devices and media, the risk of loss or theft of ePHI has increased. Although this implementation specification is addressable, strong encryption provides additional assurances over the protection of ePHI, even in cases where portable devices are lost or stolen.[7] The combination of CMS's recommendation in the remote use guidance, the increasing number of incidents involving lost portable devices, and the decreasing cost of encryption solutions has resulted in an environment where encryption may not be optional under the mantra of reasonable and appropriate.

CMS observed one of the common corrective action plans after an incident involving a lost or stolen portable device was to encrypt ePHI. However, CMS continued to observe the following conditions during the reviews:

- Encryption was not implemented on all workstations and laptops;
- Encryption was not implemented on the transmission of data which contained ePHI; and,
- Strong encryption was not consistently implemented.

Encryption was not implemented on all workstations and laptops

CMS noted that CEs either did not implement encryption on workstations and laptops or did not encrypt all of these systems.

Encryption was not implemented on the transmission of data which contained ePHI

CEs were at varying levels of compliance with regard to encryption of ePHI in transit. Some organizations had developed systems to optionally encrypt email at an employee's request. Most organizations who implemented these types of mechanisms used web-based secure mail for

[7] "The Global State of Information Security 2008" noted that of respondents from the healthcare payer industry, 46% encrypt databases, 54% encrypt file shares, and 62% encrypt backup tapes. However, only 28% encrypt removable media and encryption of laptops has decreased in the last year, down to 51%. In addition, 50% of respondents from the healthcare provider industry utilized laptop encryption.

delivery. Many organizations continued to use legacy transmissions methods for transferring ePHI, such as FTP, which did not include encryption mechanisms.

Strong encryption was not consistently implemented
CEs who implemented encryption did not always implement strong encryption, especially on wireless networks which transmitted ePHI.

Recommended Solutions
In order to increase compliance with this element of the Security Rule, the following solutions are recommended:

1. CEs should develop an accurate inventory of laptops, workstations, and other portable devices or media. Failure to establish an accurate inventory usually results in the lack of assurance that CEs have encrypted all devices which require this protection. Maintenance of this inventory should be integrated with the procurement process for new systems and devices.

2. CEs should develop and formally document policies requiring encryption of ePHI. The policy should address situations where encryption is required. These situations should be identified based on risk. In addition, the policy should outline the minimum level of encryption required for ePHI at rest and in transit.

3. CEs should implement an encryption solution on all workstations and laptops which store, process, or transmit ePHI. Because of the ease with which electronic data moves between systems, CEs should also consider extending these protections to all workstations and laptops. The software should provide a whole disk encryption solution using strong encryption technology. If possible, the solution should be validated as compliant with Federal Information Processing Standards (FIPS) Publication (Pub) 140-2, "Security Requirements for Cryptographic Modules" or leverage encryption modules which validate as compliance.

4. CEs should identify requirements for encryption of portable devices and media as necessary. If ePHI is stored on USB keys, backup tapes, PDA, Blackberries, iPods, or other portable devices, the data on this media should be encrypted. CEs should also consider implementing policies specifically forbidding ePHI on these types of devices; however, CEs must then consider approaches to prevent this information from moving to these devices. Such a decision will be dependent on the work of the employees, and the need to be able to access data from a portable device, particularly in the clinical arena, given the advent of electronic health records and personal health records which are designed to be accessed from anywhere at any time.

5. CEs should implement strong encryption on wireless networks, if they are used to transmit ePHI. Wireless networking technology continues to evolve, as does the security around these networks. Because of longstanding identified weaknesses in WEP and recently identified in

WPA using TKIP[8], organizations must research encryption methods which reasonably and appropriately protect ePHI in transit. These mechanisms should be revisited as wireless security evolves.

6. CEs should communicate encryption requirements to the workforce through policies, initial security awareness training, and periodic refresher training. Training should include information on employee responsibilities as they relate to encryption, and should be updated based on new threats to encrypted data. For example, research out of Princeton University[9] shows that attackers can compromise whole disk encryption keys and decrypt drives without a password by finding the encryption key in residual memory. Changes in the threat environment introduce additional risk which CEs must identify and mitigate. For additional details regarding identifying risk, please see the section entitled "Risk Assessment" within this document.

7. After CEs implement encryption, they should update their system baselines and build procedures to reflect the deployment of the encryption solutions.

[8] Beck, Martin and Erik Twes. "Practical attacks against WEP and WPA". 8 Nov. 2008. 17 Nov. 2008

[9] Details of this research, a demonstration of the vulnerability, and recommended corrective actions are available at http://citp.princeton.edu/memory/.