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

2009
HIPAA Compliance Review Analysis And Summary of Results

September 22, 2009

Table of Contents

Introduction

During 2009 the Office of E Health Standards and Services (OESS) of the Centers for Medicare & Medicaid Services (CMS) performed reviews of five HIPAA Covered Entities (CEs) to verify compliance with "Security Standards for the Protection of Electronic Protected Health Information", found at 45 CFR Part 160 and Part 164, Subparts A and C, commonly known as the Security Rule. Historically, 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 of Civil Rights (OCR). The stance of CMS' review of "Filed Against Entities (FAE's) is based on the nature of each complaint; thereby, making each review specific to each entity and the circumstances surrounding each breach. This year for the first time, CEs for which there was no complaint also were reviewed.

The CMS, within the Department of Health & Human Services (DHHS), was responsible for enforcing and promoting compliance of the Security Rule, as it applied to HIPAA covered entities. HIPAA covered entities include health care clearinghouses, health plans, and certain health care providers.

The first review performed by CMS/OESS was of an FAE. The following four reviews were for CE's for which no complaint had been filed and no breach notification had appeared in the media. CMS had no knowledge or suspicion of any current or potential violations of the HIPAA Security Rule by these organizations. These reviews did not cover compliance with the HIPAA Transactions and Code Sets Rule, or with the Privacy Rule which is the responsibility of the Office for Civil Rights (OCR). These reviews were to gain a clearer understanding of these CEs and to verify their operational compliance with the HIPAA Security Rule, document any "Best Practices" implemented by the CE and to execute enforcement actions related to operational failures.

Using this approach, CMS assessed compliance with the Administrative, Physical and Technical Safeguards, Remote Access and Organizational, Policies and Procedures and Documentation Requirements areas of the Security Rule at each of the five CEs. Based on the complaints previously received and history, 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 off-site and an on-site analysis at the CE which included steps to assess 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 this 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 if appropriate for FAEs, discuss corrective actions taken since the incident occurred, and identify processes which protected the confidentiality, availability, and integrity of EPHI. In the case of the five CEs that were reviewed for operational compliance, CMS interviewed senior management as well as individual members of the workforce that received processed and transmitted EPHI. This action occurred to insure that the operations of each CE were thoroughly understood in order to identify the best practices in the goals noted above. 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 and discussed potential gaps in compliance with their representatives.

At the completion of the analysis, CMS provided a report which outlined any gaps. Findings or vulnerabilities in compliance identified at the CE as well as areas of 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.

As part of the reviews, remote access security and compliance was specifically targeted and found to be implemented adequately in the CEs that were reviewed. However, remote access security is believed to continue to be an issue for many CEs and is addressed in a publication on the HIPAA Security Website entitled HIPAA Security Guidance for Remote Use of and Access to Electronic Protected Health Information.

After completing reviews of five CEs, CMS performed an analysis of the compliance issues that were identified to determine areas where organizations struggled to comply with the Security Rule. These areas included:

1. Risk Analysis
2. Currency and Adequacy of Policies and Procedures
3. Security Training

4. Workforce Clearance
5. Workstation Security
6. Encryption
7. Business Associate Agreements

To help other CEs identify and address these areas, CMS has developed this document which outlines the details of these seven 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.

In preparing this paper for 2009, it was apparent that many of the findings and recommendations were similar to the 2008 Summary of Results. The majority of findings were in the area of policies and procedures, training and awareness and risk analysis. This indicates that FAEs and randomly sampled CEs have a lot in common in typical shortcomings for HIPAA Security Rule compliance. The only category of findings which was new for 2009 was for Business Associate Agreements which were found to be inadequate in several of the CEs that were reviewed this year.

There appeared to be improvement in protecting workstations and laptops, encryption and possibly workforce clearance. This indicates possible progress following the implementation of reviews and the increased general awareness of the CEs through high profile cases where data exposures led to fines and public embarrassment of other CEs.

Risk Analysis

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

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

Through this required implementation specification, the Security Rule requires Covered Entities (CEs) to conduct risk assessments to identify risks and vulnerabilities to electronic protected health information (EPHI). The standard does not dictate how CEs are to perform the risk assessment, how often the risk assessments should be performed or provide specific insight into the approach for assessing risk around EPHI. To help CEs implement this specification, CMS has provided additional guidance through paper 6 of 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.

During 2009, CMS observed the identical areas of noncompliance that were noted in the 2008 summary report:

- CEs did not perform a risk assessment;
- 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.

CEs did not have a formalized, documented risk assessment process

In 2009, with the exception of one review, CMS identified problems with most or all CE's policies and procedures including those for performing Risk Assessment. Many entities had performed risk assessments but did not have a policy requiring the creation or periodic update of these risk assessments.

CEs had outdated risk assessments

During 2009, CMS noted that many of the CEs that performed risk assessments conducted those assessments at a point greater than three years in the past. CMS noted that these organizations had not reviewed and updated the risk assessment 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. In some cases risk assessments were performed with other statutes and goals in mind and did not even address EPHI.

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 state that the existing Risk Assessment must be reviewed at least annually to ensure that the risks that had been previously identified had in fact been remediated and also that no new risks had surfaced due to changes in the environment. 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;

- 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 include particular focus 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 and Adequacy 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 this standard.

Policies, Procedures and Documentation Requirements §164.316

In addition to the policies, procedures and documentation contained throughout the Security Rule, § 164.316 sets forth specific requirements for all policies, procedures and documentation required by the Rule.

Standard §164.316(a) Policies and Procedures
The first standard, Policies and Procedures, contains several important concepts. Specifically, it requires that covered entities:

"Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in §164.306(b)(2)(i), (ii), (iii), and (iv) [the Security Standards: General Rules, Flexibility of Approach]. This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart."

Standard §164.316(b)(1) Documentation
The Documentation standard requires covered entities to:
"(i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and (ii) if an action, activity or assessment is required by this

subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment."
The Documentation standard has three implementation specifications.
1. Time Limit (Required)
2. Availability (Required)
3. Updates (Required)

Time Limit (R) - §164.316(b)(2)(i)

The Time Limit implementation specification requires covered entities to:
"Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later."

Availability (R) - §164.316(b)(2)(ii)

The Availability implementation specification requires covered entities to:
"Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains."

Updates (R) - §164.316(b)(2) (iii)

The Updates implementation specification requires covered entities to:
"Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information."

During the reviews conducted by CMS during 2009, compliance issues with the requirements of these standards and required implementation specifications as well as with the CEs' documented policies were almost universally deficient. Only one of the 5 CEs reviewed had adequate policies and procedures. Specifically, CMS observed the following conditions:

- **CEs had few and inadequate policies and procedures.**
- **CEs had policies and procedures that did not address the HIPAA Security Standards and Implementation Specifications.**
- **CE's documented procedures were inconsistent with procedures followed by CE personnel**.

CEs had few and inadequate policies and procedures.
A few CEs did not have basic policies and procedures or had some policies but were missing others in important areas. Most CEs had made an attempt to cover policies and procedures as required by the HIPAA Security Rule. However, some CEs did not understand what was required. When requested to submit security policies, some sent CMS all sorts of unstructured documents, security tips, flowcharts technical diagrams and other irrelevant material. During the reviews, the contracted reviewers often held sessions and presented examples of adequate policies and procedures in order to educate the CEs in this important area.

CEs had policies and procedures that did not address the HIPAA Security Standards and Implementation Specifications

The HIPAA Security Reviews conducted in 2009 found that several CEs had security policies and procedures that may have been written without having the goals of protecting EPHI or with no consideration of the HIPAA Security Standards and Implementation Specifications. In this case they were inadequate and produced findings.

CE's documented procedures were inconsistent with procedures followed by CE personnel. Reviews conducted during 2009 noted that often there were controls implemented that were not documented in procedures. This is probably rooted in the problem first noted in 2008 that the policies and procedures were not reviewed and updated in a timely manner and that these procedures did not result from a structured and organized process to create and review procedure.

In other cases, policy and procedures were created with good intention but were not implemented properly or as documented.

CMS observed that about half of the CE's reviewed did have formalized review and approval processes for policies and procedures. However, the ones who did have these processes still did not always produce adequate documents since many of the members of these review panels were not familiar with the HIPAA Security Rule and its implications for policy and procedure development.

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. A permanent member of the team who develops policies and procedures must be the one of the CE's designated HIPAA Security officers.

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 which complies 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 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 they identify. 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)."

HIPAA Security Guidance for Remote Use of and Access to Electronic Protected Health Information
Page 4

"Develop and employ proper clearance procedures and verify training of workforce members prior to granting remote access."

During the 2009 reviews, CMS identified compliance issues similar to those identified with Security Awareness training during the 2008 reviews regarding policies and procedures for Security Awareness Training and retaining evidence of training completion.

In addition, CMS discovered that some CEs regularly granted information systems access to new employees prior to conducting even the basic Security Training. One CE was observed to have granted access prior to the member of the workforce being hired. It is a violation of the spirit and the letter of the HIPAA Security Standard. Page 14 of Volume 2 of the HIPAA Security Series – Security Standards: Administrative Safeguards clearly states: Regardless of the Administrative Safeguards a covered entity implements, those safeguards will not protect the EPHI if the workforce is unaware of its role in adhering to and enforcing them. Many security risks and vulnerabilities within covered entities are internal. Members of the workforce cannot be expected to know how to protect EPHI when they have not been trained to recognize it, to understand the law protecting it.

Specifically, the following non-compliance issues were observed:

CEs did not have policies and procedures or those existing ones did not properly address the HIPAA Security Rule provisions for Security Training and Awareness.
Several CEs had substandard policies and procedures. Some had none that addressed Security Awareness Training. .

CEs did not 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.

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. On the other hand, one CE had weekly sessions on the work floor exploring security and privacy topics.

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 refresher 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 his 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 direct report when initial deadlines pass without completion and revocation of the user's access when final deadlines pass without completion.

4. CE senior management should be held liable for failure to train their members of the workforce in accordance with the Standards listed above.

5. Remote Access to EPHI poses a unique and specific need for Role Based Training to ensure that those members of the workforce recognize the enhanced risk of accessing and manipulating EPHI from a remote location.

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."

HIPAA Security Guidance for Remote Use of and Access to Electronic Protected Health Information
Page 4

"Develop and employ proper clearance procedures and verify training of workforce members prior to granting remote access."

The workforce clearance implementation specification instructs CEs to vet individuals with access to EPHI. This access should be restricted to only those individuals who have a reasonable and appropriate need to utilize EPHI. CMS has provided further guidance related to this implementation specification in the HIPAA Security Guidance for Remote Use of and Access to Electronic Protected Health Information. This guidance addresses developing proper procedures to perform clearance procedures on those individuals who require remote access to EPHI. In general, these clearance procedures are manifested as background investigations on personnel.

In 2009, CMS did not observe the workforce clearance issue. It is probably still an issue but by the laws of random circumstance, was not a problem for the 5 reviews conducted this year. However, in a related issue, personnel were given access to EPHI before receiving Security Awareness Training (See Section of Security Awareness Training).

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."

HIPAA Security Guidance for Remote Use of and Access to Electronic Protected Health Information
Page 5

"Require use of lock-down or other locking mechanisms for unattended laptops."

These standards stress the importance of protecting workstations that store, process, or transmit EPHI. 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 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 2009 reviews, CMS did not find the same compliance issues that were identified during the 2008 reviews. The 5 CEs which were reviewed all have good systems for protecting workstations, laptops and other computer devices from exposing EPHI. There are surely other CEs who still have issues in this area. However, it is possible that with the maturity of the industry and the high profile cases that have been made public in the last couple of years that CEs are taking this threat seriously and improving in general. Although policies and procedures for securing workstations did exist for the most part, the CEs often implemented the technology solutions before adequately reflecting the changes in these policies and procedures.

.

Encryption

164.312(a)(2)(iv)

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

HIPAA Security Guidance for Remote Use of and Access to Electronic Protected Health Information
Page 5

"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."

This implementation specification outlines the use of encryption as an additional layer of protection around EPHI. 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. 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.

During the 2009 security reviews, CMS did not observe compliance problems with encryption. This does not indicate that the problem does not exist within some covered entities but possibly indicates that there has been some progress in awareness of the need for encryption that is brought about as the result of the 2008 reviews and the Security Rule education and awareness program that had been pursued by CMS in the past few years. Without exception, all 5 CEs that were reviewed had adequately implemented security of transmissions and also of removable data storage devices and laptops.

The one FAE that was reviewed had originally had a questionable encryption implementation and was unable to prove that lost media had been encrypted. However, that entity had subsequently improved encryption and also laptop security procedures. New products on the market make automated encryption of laptops and removable media an enforceable goal. Reliance on voluntary compliance by the workforce personnel is not adequate assurance that all data will be protected.

As with all policies and procedures observed in 2009 reviews, there were weaknesses found in the formal policies and procedures which addressed the encryption of EPHI.

Business Associate Contracts and Other Arrangements

§164.308(b) (1) – Administrative Safeguards

A covered entity, in accordance with § 164.306 [the Security Standards: General Rules], may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a) [the Organizational Requirements] that the business associate will appropriately safeguard the information (Emphasis added). All covered entities must enter into a contract or other arrangement with persons that meet the definition of business associate in § 160.103. This standard is comparable to the Business Associate Contract standard in the Privacy Rule, but is specific to business associates that create, receive, maintain or transmit EPHI. To comply with this standard, covered entities must obtain satisfactory assurances from the business associate that it will appropriately safeguard EPHI.

Written Contract or Other Arrangement

§164.308(b) (4)

The Implementation Specification at §164.308(b) (4) documents the satisfactory assurances required by paragraph (b) (1) [the Business Associate Contracts and Other Arrangements] of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of §164.314(a) [the Organizational Requirements].

Business Associate Contracts or Other Arrangements

§164.314(a)(1) – Organizational Requirements

The standard, at §164.314(a)(1), provides the specific criteria required for written contracts or other arrangements between a covered entity and its business associates. The actual language used to address the requirements can be tailored to the needs of each organization, as long as the requirements are addressed. In general, a business associate is a person or entity other than a member of the covered entity's workforce that performs functions or activities on the covered entity's behalf, or provides specified services to the covered entity, that involve the use or disclosure of protected health information. A business associate may also be a covered entity.

For example, a health care clearinghouse may be a business associate and is also a covered entity under HIPAA. A software vendor may be a business associate as well; however, it is not, in that capacity, a covered entity. In both cases, the organizations could perform certain functions, activities or services on behalf of the covered entity and would therefore be business associates. (See 45 CFR § 160.103, for the definition of "business associate."). Section 164.314(a)(1)(ii) also identifies certain situations when a covered entity would not be in compliance with this standard despite the existence of a business associate contract.

This Administrative Safeguard Standard [§164.308(b)(1)] and Implementation Specification **[§164.308(b)(4)]** are critical to the protection of EPHI in the current complex world of healthcare specialization in which covered entities engage business associates or partners to provide unique and specialized services that the covered entity may not reasonably be able or care to provide. The necessity is apparent to have solid and comprehensive Organizational Policies and Procedures for the parameters under which business associates are employed and that define how the relationship with their business associates should be managed.

During the 2009 reviews, CMS observed many deficiencies with CE's Business Associate Agreements (BAAs). Usually, CEs had business associate templates, sometimes with the name of the business associate entered. However CMS found the following deficiencies:

- CEs had business associates but BAAs did not exist between the two parties
- CEs had BAAs not signed by both parties;
- CE's had BAAs that did not address:
    - BAA requirements as addressed in the HIPAA Security Rule
    - BAA requirement to develop comprehensive Risk Management Program,
    - Requirement to report vulnerabilities to the CE;
    - Requirement to report to the CE any breach in which resulted in the exposure or loss of EPHI;
    - Activities to be performed by the BA and conditions under which they were to be performed;
    - CEs authorization to perform an audit or security risk assessment on the BA and to require that corrective action plans be created to remediate the findings.

Recommended Solution:
CMS strongly recommends that all covered entities implement the following processes toward the active management of their business associates.

- Develop and implement a comprehensive policy toward the appropriate definition of the requirement for and the selection criteria for business associates;
- Develop and implement comprehensive procedures focused on the business processes that must be followed for the vetting of categories of business associates;
- Develop and implement comprehensive procedures focused on the preparation, completion, documentation and review of business associate templates to ensure that they are completed, dated and signed by both parties. Including in these procedures are provisions for periodic review (at least annually) to assure that the template is still appropriate. This procedure should also clarify and standardize the way in which the agreement is documented including the preamble, the body, the terms and conditions, and penalties;
- Develop a standard contractual template to be attached to the business associate template;
- The Contractual Document should:
    - Describe the business relationship of the business associate to the covered entity;

- Describe the services provided by the business associate under the contract;
- Flow the appropriate HIPAA Security Rule Standards and Implementation Specifications down to the business associate that are applicable to the service(s)/product(s) being provided;
- Flow the specification of the requirement for the Minimum Necessary EPHI that will be provided by the covered entity to the business associate;
- Each business associate contract should specify:
    - Start date;
    - End date;
    - Full description of the product or service to be provided;
    - Delivery terms and conditions including point of delivery;
    - Delivery specifications including supporting data (if applicable);
    - Requirements for the business associate to conduct periodic Risk Assessments and reporting the results of the Risk Assessment to the covered entity;
    - Provisions for the covered entity to conduct inspections of the business associates operations, especially as it pertains to the protection of EPHI and the confidentiality, integrity and availability afforded to the EPHI being held by the business associate (e.g., HIPAAA Security Compliance Reviews); and
    - Other provisions in accordance with vulnerabilities discovered as a function of the business associates Risk Assessment and guidance from covered entities HIPAA Security Officer (and if appropriate covered entity corporate general counsel).