2 Security Standards: Administrative Safeguards

Security Topics

1. Security 101 for Covered Entities
2. ★ Security Standards - Administrative Safeguards
3. Security Standards - Physical Safeguards
4. Security Standards - Technical Safeguards
5. Security Standards - Organizational, Policies and Procedures and Documentation Requirements
6. Basics of Risk Analysis and Risk Management
7. Implementation for the Small Provider

What is the Security Series?

The security series of papers will provide guidance from the Centers for Medicare & Medicaid Services (CMS) on the rule titled "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. The Security Rule was adopted to implement provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The series will contain seven papers, each focused on a specific topic related to the Security Rule. The papers, which cover the topics listed to the left, are designed to give HIPAA covered entities insight into the Security Rule and assistance with implementation of the security standards. This series explains specific requirements, the thought process behind those requirements, and possible ways to address the provisions.

Compliance Deadlines
No later than April 20, 2005 for all covered entities except small health plans, which have until no later than April 20, 2006.

CMS recommends that covered entities read the first paper in this series, "Security 101 for Covered Entities" before reading the other papers. The first paper clarifies important Security Rule concepts that will help covered entities as they plan for implementation. This second paper in the series is devoted to the standards for Administrative Safeguards and their implementation specifications and assumes the reader has a basic understanding of the Security Rule.

NOTE: To download the first paper in this series, "Security 101 for Covered Entities," visit the CMS website at: ***www.cms.hhs.gov/SecurityStandard/*** under the "Regulation" page.

Background

An important step in protecting electronic protected health information (EPHI) is to implement reasonable and appropriate administrative safeguards that establish the foundation for a covered entity's security program. The Administrative Safeguards standards in the Security Rule, at § 164.308, were developed to accomplish this purpose.

The objectives of this paper are to:

- ❑ Review each Administrative Safeguards standard and implementation specification listed in the Security Rule.
- ❑ Discuss the purpose for each standard.
- ❑ Provide sample questions that covered entities may want to consider when implementing the Administrative Safeguards.

Sample questions provided in this paper, and other HIPAA Security Series papers, are for consideration only and are not required for implementation. The purpose of the sample questions is to promote review of a covered entity's environment in relation to the requirements of the Security Rule. The sample questions are not HHS interpretations of the requirements of the Security Rule.

All the information presented in the Security Series is designed to further covered entities' understanding of the Security Rule concepts. The papers are not intended to be the definitive guidance for covered entity compliance. Compliance with the Security Rule will depend on a number of factors, including those identified in § 164.306(b)(2):

"(i) The size, complexity, and capabilities of the covered entity.
(ii) The covered entity's technical infrastructure, hardware, and software security capabilities.
(iii) The costs of security measures.
(iv) The probability and criticality of potential risks to EPHI."

What are Administrative Safeguards?

The Security Rule defines administrative safeguards as, *"administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information."*

The Administrative Safeguards comprise over half of the HIPAA Security requirements. As with all the standards in this rule, compliance with the Administrative Safeguards standards will require an evaluation of the

security controls already in place, an accurate and thorough risk analysis, and a series of documented solutions derived from a number of factors unique to each covered entity.

STANDARD § 164.308(a)(1) Security Management Process

The first standard under Administrative Safeguards section is the Security Management Process. This standard requires covered entities to:

> *"Implement policies and procedures to prevent, detect, contain and correct security violations."*

The purpose of this standard is to establish the administrative processes and procedures that a covered entity will use to implement the security program in its environment. There are four implementation specifications in the Security Management Process standard.

1. Risk Analysis (Required)
2. Risk Management (Required)
3. Sanction Policy (Required)
4. Information System Activity Review (Required)

NOTE: For a more detailed discussion of "addressable" and "required" implementation specifications, see the first paper in this series, "Security 101 for Covered Entities."

The Importance of Risk Analysis and Risk Management

Risk analysis and risk management are critical to a covered entity's Security Rule compliance efforts. Both are standard information security processes that have already been adopted by some organizations within the health care industry.

As stated in the responses to public comment in the preamble to the Security Rule, the Security Management Process standard and associated implementation specifications "*form the foundation upon which an entity's necessary security activities are built*." The results from the risk analysis and risk management processes will become the baseline for security processes within covered entities.

This paper provides a general understanding of risk analysis and risk management concepts and processes. CMS will include a more detailed discussion of risk analysis and risk management in paper 6 in the HIPAA Security Series titled, "Basics of Risk Analysis and Risk Management."

NOTE: Risk analysis and risk management serve as tools to assist in the development of a covered entity's strategy to protect the confidentiality, integrity, and availability of EPHI.

1. RISK ANALYSIS (R) - *§ 164.308(a)(1)(ii)(A)*

The Risk Analysis implementation specification requires covered entities to:

> *"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."*

In general, a risk analysis can be viewed as:

- ❑ The process of identifying potential security risks, and
- ❑ Determining the probability of occurrence and magnitude of risks.

Sample questions for covered entities to consider:

- ✓ How does EPHI flow throughout the organization? This includes EPHI that is created, received, maintained or transmitted by the covered entity.
- ✓ What are the less obvious sources of EPHI? Has the organization considered portable devices like PDAs?
- ✓ What are the external sources of EPHI? For example, do vendors or consultants create, receive, maintain or transmit EPHI?
- ✓ What are the human, natural, and environmental threats to information systems that contain EPHI?

2. RISK MANAGEMENT (R) - *§ 164.308(a)(1)(ii)(B)*

Risk Management is a required implementation specification. It requires an organization to make decisions about how to address security risks and vulnerabilities. The Risk Management implementation specification states that covered entities must:

> *"Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a)."*

Risk management is the process used to identify and implement security measures to reduce risk to a reasonable and appropriate level within the covered entity based on the covered entity's circumstances. The measures implemented to comply with this required implementation specification must also allow the covered entity to comply with §

164.306(a) of the Security Standards: General Rules. Covered entities will want to answer some basic questions when planning their risk management process.

Sample questions for covered entities to consider:

- ✓ What security measures are already in place to protect EPHI (i.e., safeguards)?
- ✓ Is executive leadership and/or management involved in risk management and mitigation decisions?
- ✓ Are security processes being communicated throughout the organization?
- ✓ Does the covered entity need to engage other resources to assist in risk management?

In general, a covered entity will want to make sure its risk management strategy takes into account the characteristics of its environment including the factors at § 164.306(b)(2), which are listed on page 2 of this paper. These factors will help the covered entity to determine what potential security measures are reasonable and appropriate for its environment.

NOTE: Covered entities must ensure that the risk analysis and risk management processes are on-going and dynamic processes that can change as the environment or operations change.

3. SANCTION POLICY (R) - *§ 164.308(a)(1)(ii)(C)*

Another implementation specification in the Security Management Process is the Sanction Policy. It requires covered entities to:

> *"Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity."*

Appropriate sanctions must be in place so that workforce members understand the consequences of failing to comply with security policies and procedures, to deter noncompliance.

Sample questions for covered entities to consider:

- ✓ Does the covered entity have existing sanction policies and procedures to meet the requirements of this implementation specification? If not, can

existing sanction policies be modified to include language relating to violations of these policies and procedures?

✓ Does the organization require employees to sign a statement of adherence to security policy and procedures (e.g., as part of the employee handbook or confidentiality statement) as a prerequisite to employment?

✓ Does the statement of adherence to security policies and procedures state that the workforce member acknowledges that violations of security policies and procedures may lead to disciplinary action, for example, up to and including termination?

NOTE: A covered entity's sanction policy should reinforce its security policies and procedures.

✓ Does the sanction policy provide examples of potential violations of policy and procedures?

✓ Does the sanction policy adjust the disciplinary action based on the severity of the violation?

4. INFORMATION SYSTEM ACTIVITY REVIEW (R) - *§ 164.308(a)(1)(ii)(D)*

The Security Management Process standard also includes the Information System Activity Review implementation specification. This required implementation specification states that covered entities must:

> "*Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.*"

The information system activity review enables covered entities to determine if any EPHI is used or disclosed in an inappropriate manner.

Information system activity review procedures may be different for each covered entity. The procedure should be customized to meet the covered entity's risk management strategy and take into account the capabilities of all information systems with EPHI.

Sample questions for covered entities to consider:

- ✓ What are the audit and activity review functions of the current information systems?
- ✓ Are the information systems functions adequately used and monitored to promote continual awareness of information system activity?
- ✓ What logs or reports are generated by the information systems?
- ✓ Is there a policy that establishes what reviews will be conducted?
- ✓ Is there a procedure that describes specifics of the reviews?

NOTE: The Information System Activity Review implementation specification should also promote continual awareness of any information system activity that could suggest a security incident.

STANDARD § 164.308(a)(2) Assigned Security Responsibility

The second standard in the Administrative Safeguards section is Assigned Security Responsibility. There are no separate implementation specifications for this standard. The standard requires that covered entities:

> *"Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart [the Security Rule] for the entity."*

The purpose of this standard is to identify who will be operationally responsible for assuring that the covered entity complies with the Security Rule. Covered entities should be aware of the following when assigning security responsibility:

- ❑ This requirement is comparable to the Privacy Rule standard at §164.530(a)(1), Personnel Designations, which requires all covered entities to designate a Privacy Official.
- ❑ The Security Official and Privacy Official can be the same person, but are not required to be.

- While one individual must be designated as having overall responsibility, other individuals in the covered entity may be assigned specific security responsibilities (e.g., facility security or network security).

When making this decision covered entities should consider some basic questions.

Sample questions for covered entities to consider:

- ✓ Would it serve the organization's needs to designate the same individual as both the Privacy and Security Official (for example, in a small provider office)?
- ✓ Has the organization agreed upon, and clearly identified and documented, the responsibilities of the Security Official?
- ✓ How are the roles and responsibilities of the Security Official crafted to reflect the size, complexity and technical capabilities of the organization?

STANDARD § 164.308(a)(3) Workforce Security

The third standard is Workforce Security, which states that covered entities must:

> *"Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under [the Information Access Management standard*], *and to prevent those workforce members who do not have access under [the Information Access Management standard] from obtaining access to electronic protected health information."*

Within a covered entity's environment, workforce members that need access to EPHI to carry out their duties must be identified. For each workforce member, or job function, the covered entity must identify the EPHI that is needed, when it is needed, and make reasonable efforts to control access to the EPHI. This will also include identification of the computer systems and applications that provide access to the EPHI. Covered entities must provide only the minimum necessary access to EPHI that is required for a workforce member to do his or her job.

Within Workforce Security there are three addressable implementation specifications.

1. Authorization and/or Supervision (Addressable)

2. Workforce Clearance Procedure (Addressable)
3. Termination Procedures (Addressable)

1. AUTHORIZATION AND/OR SUPERVISION (A) – § *164.308(a)(3)(ii)(A)*

Where the Authorization and/or Supervision implementation specification is a reasonable and appropriate safeguard for a covered entity, the covered entity must:

> *"Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed."*

Authorization is the process of determining whether a particular user (or a computer system) has the right to carry out a certain activity, such as reading a file or running a program. Implementation of this addressable implementation specification will vary among covered entities, depending upon the size and complexity of the workforce, and the information systems that contain EPHI. For example, in a very small provider office, all staff members may need to access all EPHI in their information system, since they may perform multiple functions. In this case, the covered entity might document the reasons for implementing policies and procedures allowing this kind of global access. If the documented rationale is reasonable and appropriate, this may be an acceptable approach.

NOTE: The Authorization and/or Supervision implementation specification provides the necessary checks and balances to ensure that all members of the workforce have appropriate access (or, in some cases, no access) to EPHI.

To determine the most reasonable and appropriate authorization and/or supervision procedures, covered entities may want to ask some basic questions about existing policies and procedures.

Sample questions for covered entities to consider:

- ✓ Are detailed job descriptions used to determine what level of access the person holding the position should have to EPHI?
- ✓ Who has or should have the authority to determine who can access EPHI, e.g., supervisors or managers?
- ✓ Are there similar existing processes used for paper records that could be used as an example for the EPHI?

Covered entities should review the authorization and supervision policies already present in the organization's current operating environment. Depending on the existing policies, covered entities may need to reinforce them, make modifications for EPHI, and/or develop corresponding documentation.

2. WORKFORCE CLEARANCE PROCEDURE (A) - *§ 164.308(a)(3)(ii)(B)*

Covered entities need to address whether all members of the workforce with authorized access to EPHI receive appropriate clearances. Where the Workforce Clearance Procedure implementation specification is a reasonable and appropriate safeguard for a covered entity, the covered entity must:

> *"Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate."*

In other words, the clearance process must establish the procedures to verify that a workforce member does in fact have the appropriate access for their job function. A covered entity may choose to perform this type of screening procedure separate from or as a part of the authorization and/or supervision procedure.

Sample questions for covered entities to consider:

- ✓ Are there existing procedures for determining that the appropriate workforce members have access to the necessary information?
- ✓ Are the procedures used consistently within the organization when determining access of related workforce job functions?

3. TERMINATION PROCEDURES (A) - *§ 164.308(a)(3)(ii)(C)*

Where the Termination Procedures implementation specification is a reasonable and appropriate safeguard for a covered entity, the covered entity must:

> *"Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) [the Workforce Clearance Procedure] of this section."*

Termination procedures must be implemented to remove access privileges when an employee, contractor, or other individual previously entitled to access information no longer has these privileges. Whether the employee leaves the organization voluntarily or involuntarily, procedures to terminate access must be in place.

The same process that is implemented for termination should also be used to change access levels if an employee's job description changes to require more or less access to EPHI. The procedures should also address the complexity of the organization and the sophistication of associated information systems.

Sample questions for covered entities to consider:

- ✓ Do the termination policies and procedures assign responsibility for removing information system and/or physical access?
- ✓ Do the policies and procedures include timely communication of termination actions to insure that the termination procedures are appropriately followed?

STANDARD § 164.308(a)(4) Information Access Management

The fourth standard in the Administrative Safeguards section is Information Access Management. Covered entities are required to:

> *"Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part [the Privacy Rule]."*

Restricting access to only those persons and entities with a need for access is a basic tenet of security. By implementing this standard, the risk of inappropriate disclosure, alteration, or destruction of EPHI is minimized. Covered entities must determine those persons and/or entities that need access to EPHI within their environment.

NOTE: The Information Access Management implementation specifications are closely related to the implementation specifications under the Workforce Security standard.

Compliance with this standard should support a covered entity's compliance with the HIPAA Privacy Rule minimum necessary requirements, which requires covered entities to evaluate their practices and enhance safeguards as needed to limit unnecessary or inappropriate access to and disclosure of protected health information. To better understand this standard, covered entities should review the minimum necessary standard of the HIPAA Privacy Rule. See 45 CFR 164.502(b) and 164.514(d).

The Information Access Management standard has three implementation specifications.

1. Isolating Health Care Clearinghouse Functions (Required)

2. Access Authorization (Addressable)
3. Access Establishment and Modification (Addressable)

1. ISOLATING HEALTH CARE CLEARINGHOUSE FUNCTIONS (R) – *§ 164.308(a)(4)(ii)(A)*

The Isolating Health Care Clearinghouse Functions implementation specification states:

> *"If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization."*

This implementation specification only applies in the situation where a health care clearinghouse is part of a larger organization. In these situations, the health care clearinghouse is responsible for protecting the EPHI that it is processing.

Sample questions for covered entities to consider:

- ✓ Does the larger organization perform health care clearinghouse functions?
- ✓ If health care clearinghouse functions are performed, are policies and procedures implemented to protect EPHI from the other functions of the larger organization?
- ✓ Are additional technical safeguards needed to separate EPHI in information systems, used by the health care clearinghouse, to protect against unauthorized access by the larger organization?

2. ACCESS AUTHORIZATION (A) - § *164.308(a)(4)(ii)(B)*

In the Workforce Security standard portion of this paper, authorization was defined as the act of determining whether a particular user (or computer system) has the right, based on job function or responsibilities, to carry out a certain activity, such as reading a file or running a program. Where this implementation standard is a reasonable and appropriate safeguard for a covered entity, the covered entity must:

> *"Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism."*

Once the covered entity has determined that the person or system is authorized, there are numerous ways to grant access to EPHI. In general, a covered entity's policies and procedures must identify who has authority to grant access privileges. It must also state the process for granting access. To create and document policies and procedures to grant access, covered entities should address the following questions.

Sample questions for covered entities to consider:

- ✓ How is authorization documented? How can it be used to grant access?
- ✓ Are the policies and procedures for granting access consistent with applicable requirements of the Privacy Rule?
- ✓ Have appropriate authorization and clearance procedures, as specified in workforce security, been performed prior to granting access?
- ✓ Are access rules specific to applications and business requirements? For example, do different workforce members require different levels of access based on job function?
- ✓ Is there a technical process in place, such as creating unique user name and an authentication process, when granting access to a workforce member?

Once a covered entity has clearly defined who should get access to what EPHI and under what circumstances, it must consider how access is established and modified.

3. ACCESS ESTABLISHMENT AND MODIFICATION (A) - § *164.308(a)(4)(ii)(C)*

Where the Access Establishment and Modification implementation specification is a reasonable and appropriate safeguard for a covered entity, the covered entity must:

> *"Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process."*

This means that a covered entity must implement and manage the creation and modification of access privileges to workstations, transactions, programs or processes. Responsibility for this function may be assigned to a specific individual or individuals, which also may be responsible for terminating access privileges for workforce members.

Covered entities must evaluate existing procedures, update them (if needed), and document procedures as necessary.

Sample questions for covered entities to consider:

- ✓ Are policies and procedures in place for establishing access and modifying access?
- ✓ Are system access policies and procedures documented and updated as necessary?
- ✓ Do members of management or other workforce members periodically review the list of persons with access to EPHI to ensure they are valid and consistent with those authorized?

STANDARD § 164.308(a)(5) Security Awareness and Training

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. This is why the next standard, Security Awareness and Training, is so important.

Specifically, the Security Awareness and Training standard states that covered entities must:

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

Security training for all new and existing members of the covered entity's workforce is required by the compliance date of the Security Rule. In addition, periodic retraining should be given whenever environmental or operational changes affect the security of EPHI. Changes may include: new or updated policies and procedures; new or upgraded software or hardware; new security technology; or even changes in the Security Rule.

The Security Awareness and Training standard has four implementation specifications.

1. Security Reminders (Addressable)
2. Protection from Malicious Software (Addressable)
3. Log-in Monitoring (Addressable)
4. Password Management (Addressable)

1. SECURITY REMINDERS (A) - *§ 164.308(a)(5)(ii)(A)*

Where this implementation specification is a reasonable and appropriate safeguard for a covered entity, the covered entity must implement:

> *"Periodic security updates."*

There are many types of security reminders that covered entities may choose to implement. Examples might include notices in printed or electronic form, agenda items and specific discussion topics at monthly meetings, focused reminders posted in affected areas, as well as formal retraining on security policies and procedures. Covered entities should look at how they currently remind the workforce of current policies and procedures, and then decide whether these practices are reasonable and appropriate or if other forms of security reminders are needed.

NOTE: Covered entities must document the security reminders they implement. Documentation could include the type of reminder, its message, and the date it was implemented.

2. PROTECTION FROM MALICIOUS SOFTWARE (A) - § *164.308(a)(5)(ii)(B)*

One important security measure that employees may need to be reminded of is security software that is used to protect against malicious software. Where this implementation specification is a reasonable and appropriate safeguard for a covered entity, the covered entity must implement:

> *"Procedures for guarding against, detecting, and reporting malicious software."*

Malicious software can be thought of as any program that harms information systems, such as viruses, Trojan horses or worms. As a result of an unauthorized infiltration, EPHI and other data can be damaged or destroyed, or at a minimum, require expensive and time-consuming repairs.

NOTE: Malicious software that successfully invades information systems can cause significant damage.

Malicious software is frequently brought into an organization through email attachments, and programs that are downloaded from the Internet. Under the Security Awareness and Training standard, the workforce must also be trained regarding its role in protecting against malicious software, and system protection capabilities. It is important to note that training must be an ongoing process for all organizations.

3. LOG-IN MONITORING (A) - § *164.308(a)(5)(ii)(C)*

Security awareness and training should also address how users log onto systems and how they are supposed to manage their passwords. Where the Log-in Monitoring implementation specification is a reasonable and appropriate safeguard for a covered entity, the covered entity must implement:

"Procedures for monitoring log-in attempts and reporting discrepancies."

Typically, an inappropriate or attempted log-in is when someone enters multiple combinations of usernames and/or passwords to attempt to access an information system. Fortunately, many information systems can be set to identify multiple unsuccessful attempts to log-in. Other systems might record the attempts in a log or audit trail. Still others might require resetting of a password after a specified number of unsuccessful log-in attempts.

NOTE: The purpose of the Log-in Monitoring implementation specification is to make workforce members aware of log-in attempts that are not appropriate.

If smaller covered entities are not using, or are not familiar with, their systems capabilities for these types of log-in attempts, they should contact their system vendor or read their application software manuals for more information. Once capabilities are established the workforce must be made aware of how to use and monitor them.

4. PASSWORD MANAGEMENT - § *164.308(a)(5)(ii)(D)*

The last addressable specification in this standard is Password Management. Where this implementation specification is a reasonable and appropriate safeguard for a covered entity, the covered entity must implement:

"Procedures for creating, changing, and safeguarding passwords."

In addition to providing a password for access, entities must ensure that workforce members are trained on how to safeguard the information. Covered entities must train all users and establish guidelines for creating passwords and changing them during periodic change cycles.

Sample questions for covered entities to consider:

- ✓ Are there policies in place that prevent workforce members from sharing passwords with others?
- ✓ Is the workforce advised to commit their passwords to memory?

- ✓ Are common sense precautions taken, such as not writing passwords down and leaving them in areas that are visible or accessible to others?

STANDARD § 164.308(a)(6) Security Incident Procedures

The next standard is Security Incident Procedures, which states that covered entities must:

"Implement policies and procedures to address security incidents."

The purpose of this standard is to require covered entities to address security incidents within their environment. Addressing security incidents is an integral part of the overall security program. Implementing the Security Rule standards will reduce the type and amount of security incidents a covered entity encounters, but security incidents will occur. Even covered entities with detailed security policies and procedures and advanced technology will have security incidents.

The Security Rule defines a security incident as, *"the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system."* Security incident procedures must address how to identify security incidents and provide that the incident be reported to the appropriate person or persons.

Whether a specific action would be considered a security incident, the specific process of documenting incidents, what information should be contained in the documentation, and what the appropriate response should be will be dependent upon an entity's environment and the information involved. An entity should be able to rely upon the information gathered in complying with the other Security Rule standards, for example, its risk assessment and risk management procedures and the privacy standards, to determine what constitutes a security incident in the context of its business operations.

There is one required implementation specification for this standard.

RESPONSE AND REPORTING (R) - § *164.308(a)(6)(ii)*

The Response and Reporting implementation specification states that covered entities must:

> *"Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes."*

Security incident procedures must describe how workforce members are to respond to an incident. This may include: preserving evidence; mitigating, to the extent possible, the situation that caused the incident; documenting the incident and the outcome; and evaluating security incidents as part of ongoing risk management.

Covered entities must be aware of any number of possible incidents that they may have to deal with. For example:

- Stolen or otherwise inappropriately obtained passwords that are used to access EPHI
- Corrupted backup tapes that do not allow restoration of EPHI
- Virus attacks that interfere with the operations of information systems with EPHI
- Physical break-ins leading to the theft of media with EPHI
- Failure to terminate the account of a former employee that is then used by an unauthorized user to access information systems with EPHI
- Providing media with EPHI, such as a PC hard drive or laptop, to another user who is not authorized to access the EPHI prior to removing the EPHI stored on the media.

A covered entity's security incident procedures must establish adequate response and reporting procedures for these and other types of events.

Sample questions for covered entities to consider:

- ✓ Are policies and procedures developed and implemented to address security incidents?
- ✓ Do the security incident policies and procedures list possible types of security incidents and the response for each?
- ✓ Do the security incident policies and procedures identify to whom security incidents must be reported?

STANDARD § 164.308(a)(7) Contingency Plan

The purpose of contingency planning is to establish strategies for recovering access to EPHI should the organization experience an emergency or other occurrence, such as a power outage and/or disruption of critical business operations. The goal is to ensure that organizations have their EPHI available when it is needed. The Contingency Plan standard requires that covered entities:

> *"Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information."*

The Contingency Plan standard includes five implementation specifications.

1. Data Backup Plan (Required)
2. Disaster Recovery Plan (Required)
3. Emergency Mode Operation Plan (Required)
4. Testing and Revision Procedures (Addressable)
5. Applications and Data Criticality Analysis (Addressable)

1. DATA BACKUP PLAN (R) - § *164.308(a)(7)(ii)(A)*

The Data Backup Plan implementation specification requires covered entities to:

> *"Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information."*

Most covered entities may have backup procedures as part of current business practices. Data Backup plans are an important safeguard for all covered entities, and a required implementation specification.

Sample questions for covered entities to consider:

- ✓ What is the EPHI that must be backed up?
- ✓ Does the plan include all important sources of data such as patient accounting systems, electronic medical records, health maintenance and case management information, digital recordings of diagnostic images, electronic test results, or any other electronic documents created or used?

- ✓ Has the organization considered the various methods of backups, including tape, disk, or CD?
- ✓ Does the backup plan include storage of backups in a safe, secure place?
- ✓ Is the organization's frequency of backups appropriate for its environment?

2. DISASTER RECOVERY PLAN (R) - § *164.308(a)(7)(ii)(B)*

The Disaster Recovery Plan implementation specification requires covered entities to:

> *"Establish (and implement as needed) procedures to restore any loss of data."*

Some covered entities may already have a general disaster plan that meets this requirement; however, each entity must review the current plan to ensure that it allows them to recover EPHI.

Sample questions for covered entities to consider:

- ✓ Does the disaster recovery plan address issues specific to the covered entity's operating environment?
- ✓ Does the plan address what data is to be restored?
- ✓ Is a copy of the disaster recovery plan readily accessible at more than one location?

3. EMERGENCY MODE OPERATION PLAN (R) - § *164.308(a)(7)(ii)(C)*

The Emergency Mode Operation Plan implementation specification requires covered entities to:

> *"Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode."*

When a covered entity is operating in emergency mode due to a technical failure or power outage, security processes to protect EPHI must be maintained.

Sample questions for covered entities to consider:

- ✓ Does the organization's plan balance the need to protect the data with the organization's need to access the data?
- ✓ Will alternative security measures be used to protect the EPHI?
- ✓ Does the emergency mode operation plan include possible manual procedures for security protection that can be implemented as needed?
- ✓ Does the emergency mode operation plan include telephone numbers and contact names for all persons that must be notified in the event of a disaster, as well as roles and responsibilities of those people involved in the restoration process?

4. TESTING AND REVISION PROCEDURES (A) - § *164.308(a)(7)(ii)(D)*

Where the Testing and Revision Procedures implementation specification is a reasonable and appropriate safeguard for the covered entity, the covered entity must:

> *"Implement procedures for periodic testing and revision of contingency plans."*

It is important to point out that this implementation specification applies to all implementation specifications under the Contingency Plan standard, including the Data Backup Plan, Disaster Recovery Plan, and Emergency Mode Operations Plan.

NOTE: Testing and revision procedures will vary in frequency and comprehensiveness.

Disaster recovery and emergency mode operations plans might be tested by using a scenario-based walk-thru (to avoid daily operations impacts) or by performing complete live tests. The comprehensiveness and sophistication of the testing and revision procedures depends on the complexity of the covered entity's organization and other factors such as size and costs. It is expected that the frequency and comprehensiveness of the procedures will vary among covered entities.

Sample questions for covered entities to consider:

- ✓ Are the processes for restoring data from backups, disaster recovery and emergency mode operation documented?

- ✓ Do those responsible for performing contingency planning tasks understand their responsibilities?
- ✓ Have those responsible actually performed a test of the procedures?
- ✓ Have the results of each test been documented and any problems with the test reviewed and corrected?

NOTE: In most environments, at a minimum, a covered entity should determine if existing contingency plans are appropriate.

5. APPLICATION AND DATA CRITICALITY ANALYSIS (A) - § *164.308(a)(7)(ii)(E)*

The last implementation specification in the Contingency Plan standard is Application and Data Criticality Analysis. Where this implementation specification is a reasonable and appropriate safeguard for the covered entity, the covered entity must:

> *"Assess the relative criticality of specific applications and data in support of other contingency plan components."*

This implementation specification requires covered entities to identify their software applications (data applications that store, maintain or transmit EPHI) and determine how important each is to patient care or business needs, in order to prioritize for data backup, disaster recovery and/or emergency operations plans. A prioritized list of specific applications and data will help determine which applications or information systems get restored first and/or which must be available at all times.

STANDARD § 164.308(a)(8) Evaluation

It is important for a covered entity to know if the security plans and procedures it implements continue to adequately protect its EPHI. To accomplish this, covered entities must implement ongoing monitoring and evaluation plans. Covered entities must periodically evaluate their strategy and systems to ensure that the security requirements continue to meet their organizations' operating environments.

The Evaluation standard has no separate implementation specifications. The standard requires covered entities to:

"Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operations 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 [the Security Rule]."

NOTE: On-going evaluation of security measures is the best way to ensure all EPHI is adequately protected.

The purpose of the evaluation is to establish a process for covered entities to review and maintain reasonable and appropriate security measures to comply with the Security Rule. Initially the evaluation must be based on the security standards implemented to comply with the Security Rule. Subsequent periodic evaluations must be performed in response to environmental or operational changes that affect the security of EPHI. The on-going evaluation should also be performed on a scheduled basis, such as annually or every two years. The evaluation must include reviews of the technical and non-technical aspects of the security program.

Sample questions for covered entities to consider:

- ✓ How often should an evaluation be done? For example, are additional evaluations performed if security incidents are identified, changes are made in the organization, or new technology is implemented?
- ✓ Is an internal or external evaluation, or a combination of both, most appropriate for the covered entity?
- ✓ Are periodic evaluation reports and the supporting material considered in the analysis, recommendations, and subsequent changes fully documented?

STANDARD § 164.308(b)(1) Business Associate Contracts And Other Arrangements

The last standard in the Administrative Safeguards section is Business Associate Contracts and Other Arrangements. The organizational requirements related to this standard are discussed in more detail in § 164.314(a) of the Rule, which is covered in paper five of this series titled "Security Standards – Organizational, Policies and Procedures and Documentation Requirements." The Business Associate Contracts and Other Arrangements standard states that:

"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)."

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.

This standard also addresses a few situations in which a business associate contract is not needed.

As stated at § 164.308(b)(2), the Business Associate Contracts and Other Arrangements standard does not apply with respect to:

"(i) The transmission by a covered entity of EPHI to a health care provider concerning the treatment of an individual.

(ii) The transmission of EPHI by a group health plan or an HMO or health insurance issuer on behalf of a group health plan to a plan sponsor, to the extent that the requirements of § 164.314(b) and § 164.504(f) apply and are met; or

(iii) The transmission of EPHI from or to other agencies providing the services at § 164.502(e)(1)(ii)(C), when the covered entity is a health plan that is a government program providing public benefits, if the requirements of § 164.502(e)(1)(ii)(C) are met."

In addition, § 164.308(b)(3) states, *"A covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the standards, implementation specifications, and requirements of this paragraph and §164.314(a)."*

The standard has one implementation specification.

WRITTEN CONTRACT OR OTHER ARRANGEMENT (R) – *§ 164.308(b)(4)*

Covered entities are required to:

"Document 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].”

Sample questions covered entities may want to consider:

- ✓ Have all business associates been identified? Business associates may include clearinghouses, medical billing services, vendors of hardware and software, external consultants, lawyers, transcription contractors, or others who have access to EPHI.

- ✓ Have existing business associate contracts created and implemented for compliance with the Privacy Rule, which involve EPHI, been reviewed to determine if Security Rule requirements are addressed?

- ✓ To minimize additional work efforts, can existing business associate contracts, which involve EPHI, be modified to include Security Rule requirements?

In Summary

All of the standards and implementation specifications found in the Administrative Safeguards section refer to administrative functions, such as policy and procedures that must be in place for management and execution of security measures. These include performance of security management process, assignment or delegation of security responsibility, training requirements, and evaluation and documentation of all decisions.

Resources

The remaining papers in this series will address other specific topics related to the Security Rule. The next paper in this series covers the Physical Safeguards section. These are the safeguards required to protect electronic systems, equipment and the data they hold, from threats, environmental hazards and unauthorized intrusion, as well as the measures necessary to restrict physical access to EPHI.

Covered entities should periodically check the CMS website at www.cms.hhs.gov under "Regulations and Guidance" for additional information and resources as they work through the security implementation process. There are many other sources of information available on the Internet. While CMS does not endorse guidance provided by other organizations, covered entities may also want to check with other local and national professional health care organizations, such as national provider and health plan associations for additional information.

Need more information?

Visit the CMS website often at www.cms.hhs.gov under "Regulations and Guidance" for the latest security papers, checklists, and announcements of upcoming events.

Visit the Office for Civil Rights website, http://www.hhs.gov/ocr/hipaa, for the latest guidance, FAQs and other information on the Privacy Rule.

Security Standards Matrix (Appendix A of the Security Rule)

ADMINISTRATIVE SAFEGUARDS			
Standards	**Sections**	**Implementation Specifications (R)= Required, (A)=Addressable**	
Security Management Process	§ 164.308(a)(1)	Risk Analysis	(R)
		Risk Management	(R)
		Sanction Policy	(R)
		Information System Activity Review	(R)
Assigned Security Responsibility	§ 164.308(a)(2)		
Workforce Security	§ 164.308(a)(3)	Authorization and/or Supervision	(A)
		Workforce Clearance Procedure	(A)
		Termination Procedures	(A)
Information Access Management	§ 164.308(a)(4)	Isolating Health Care Clearinghouse Functions	(R)
		Access Authorization	(A)
		Access Establishment and Modification	(A)
Security Awareness and Training	§ 164.308(a)(5)	Security Reminders	(A)
		Protection from Malicious Software	(A)
		Log-in Monitoring	(A)
		Password Management	(A)
Security Incident Procedures	§ 164.308(a)(6)	Response and Reporting	(R)
Contingency Plan	§ 164.308(a)(7)	Data Backup Plan	(R)
		Disaster Recovery Plan	(R)
		Emergency Mode Operation Plan	(R)
		Testing and Revision Procedures	(A)
		Applications and Data Criticality Analysis	(A)
Evaluation	§ 164.308(a)(8)		
Business Associate Contracts and Other Arrangements	§ 164.308(b)(1)	Written Contract or Other Arrangement	(R)

PHYSICAL SAFEGUARDS			
Standards	**Sections**	**Implementation Specifications (R)= Required, (A)=Addressable**	
Facility Access Controls	§ 164.310(a)(1)	Contingency Operations	(A)
		Facility Security Plan	(A)
		Access Control and Validation Procedures	(A)
		Maintenance Records	(A)
Workstation Use	§ 164.310(b)		
Workstation Security	§ 164.310(c)		
Device and Media Controls	§ 164.310(d)(1)	Disposal	(R)
		Media Re-use	(R)
		Accountability	(A)
		Data Backup and Storage	(A)
TECHNICAL SAFEGUARDS			
Standards	**Sections**	**Implementation Specifications (R)= Required, (A)=Addressable**	
Access Control	§ 164.312(a)(1)	Unique User Identification	(R)
		Emergency Access Procedure	(R)
		Automatic Logoff	(A)
		Encryption and Decryption	(A)
Audit Controls	§ 164.312(b)		
Integrity	§ 164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information	(A)
Person or Entity Authentication	§ 164.312(d)		
Transmission Security	§ 164.312(e)(1)	Integrity Controls	(A)
		Encryption	(A)
ORGANIZATIONAL REQUIREMENTS			
Standards	**Sections**	**Implementation Specifications (R)= Required, (A)=Addressable**	
Business associate contracts or other arrangements	§ 164.314(a)(1)	Business Associate Contracts	(R)
		Other Arrangements	(R)
Requirements for Group Health Plans	§ 164.314(b)(1)	Implementation Specifications	(R)

POLICIES AND PROCEDURES AND DOCUMENTATION REQUIREMENTS			
Standards	**Sections**	**Implementation Specifications (R)= Required, (A)=Addressable**	
Policies and Procedures	§ 164.316(a)		
Documentation	§ 164.316(b)(1)	Time Limit	**(R)**
		Availability	**(R)**
		Updates	**(R)**