Shipman & Goodwin LLP

# HIPAA Security Alert

## EXECUTIVE GUIDANCE

July 2008

## HIPAA SECURITY COMPLIANCE

**How would your organization's senior management respond to CMS or OIG inquiries about health information security issues at your facility?**

**Does your organization have the documentation to demonstrate the existence of sufficient security protections or procedures that have been implemented?**

**If asked, do your employees understand their security-related responsibilities?**

These are just a few of the questions that senior management may be asked by CMS or the OIG during a HIPAA security audit of your facility. CMS has begun to conduct HIPAA security audits of hospitals to assess compliance with the HIPAA security regulations implemented in April 2005. Based upon initial findings, CMS has found that many providers are ill prepared in this area. At the moment, the security audits seem to be directed at gathering information and providing examples for the industry on where problems with data security arise and where security was addressed effectively, as opposed to being oriented toward the imposition of penalties and sanctions. This enforcement approach can change at any time.

Whether or not your facility undergoes a HIPAA security audit, there are potential costs and liabilities that would stem from any major failure or infiltration of a health care provider's electronic records systems. A security breach can involve claims for breach of privacy and raise the need to address exposure to identify theft of patients, security incidents involving electronic patient records and billing systems can also potentially compromise every aspect of a facility's core operations and expose a facility to expensive repair and rebuilding costs as well as costs associated with interruption in billing cycles or accessing records needed to provide care.

The basis of all of the Security Rules is the general mandate for providers to implement reasonable administrative, physical and technical safeguards to ensure the confidentiality, integrity and accessibility of electronic protected health information that it creates, receives or transmits.

For providers that may have made limited use of electronic record systems or otherwise never fully considered the Security Rules previously, now is a good time to undertake a HIPAA Security compliance effort, as regulatory interest in and inquiries into security aspects of provider operations is likely to continue to grow. For providers that developed plans, policies and procedures to address the Security Rules in 2005, it is a good time to undertake that portion of the Security Rules that calls for periodic re-assessment of the security compliance program, and to consider whether security policies, procedures and measures are adequate in light of new technology or services that may have been introduced since 2005 and consider new information about security threats and ways to address them that may be available.

For either approach, it is useful to use the Security Rules themselves as the guiding principles, coupled with use of the OIG and CMS audit lists to provide additional considerations when implementing the standards. CMS has made extensive educational materials about the Security Rules available on its website, including providing a framework for engaging in a risk assessment and providing specific risk management suggestions for use of remote access devices. The CMS materials and audit checklists can be found at http://www.cms.hhs.gov/SecurityStandard/.

The balance of this article will review the general requirements of the Security Rules and present sample considerations in addressing these standards based on the guidance materials provided by CMS.

## A. Overview of the HIPAA Security Rules.

The Security Rules as a general matter require providers to do the following:

- **Ensure the confidentiality, integrity and availability** of Electronic Protected Health Information ("EPHI") that the provider creates, receives, maintains or transmits;
- **Protect against reasonably anticipated threats or hazards** to the security or integrity of the information;
- **Protect against reasonably anticipated unauthorized uses or disclosures** of EPHI under the privacy rules; and
- **Ensure workforce compliance** with the security standards.

Providers are expected to implement administrative, physical and technical safeguards as outlined in the Security Rules to achieve the above. The Security Rules are a set of standards, and each standard should be considered a required aspect of the Security Rules. Many of the standards contain implementation specifications, which describe a method to use for meeting a standard. The implementation specifications are identified as either "Required" or "Addressable". A **"Required"** implementation specification must be implemented. For implementation specifications listed as **"Addressable"**, however, providers may consider whether the specification is reasonable and appropriate for that provider's environment, as long as there is documentation of the provider's consideration and decision-making for that item. "Addressable" should not be taken to mean optional, however. If a provider entity opts not to implement one of the addressable specifications, it is expected to implement an alternative measure if such measure would be reasonable and appropriate to the provider's environment. All assessments and decisions made around the addressable specifications should be well documented.

None of the Security Rules dictate any particular technology solution. Rather, a provider may decide which security measures allow it to reasonably and appropriately implement a standard, taking into account the size and complexity of the entity, the breadth of its technical infrastructure and security capabilities, the cost of various security measures, and the probability and criticality of certain risks to EPHI. Every provider should pay particular attention, however, to security measures associated with portable media and remote access to EPHI, as these areas may present greater risk of security violations and are of particular concern to CMS and the OIG.

Compliance with the Security Rules specifically requires periodic re-evaluation of the measures taken to address security and documented policies and procedures and consideration of whether modifications or updates are advisable in light of changes in a provider's organization or operations, such as introduction of new technologies or increased use of remote access, or changes in available security technologies and their cost.

## B. Administrative Safeguards.

Despite the fact that many providers perceive security compliance as belonging within their IS department, about half of the Security Rules standards involve administrative, not technical, standards. This fact suggests that providers should approach EPHI security as an entity-wide endeavor, rather than a task left to IS personnel only, and should consider all aspects of their systems use, such as who obtains rights to access systems and for what purposes, where systems are physically placed and how workforce use of systems is monitored in addition to the technical protections built into the system.

There are nine core administrative safeguard standards, and there are multiple implementation specifications for many of the standards. The administrative safeguards all involve the development of administrative actions, policies and procedures around the implementation of security measures and managing the provider's workforce in relation to EPHI.

The following list describes the administrative safeguards required by the Security Rules and the associated implementation specifications (noted in italics), including whether a specification is "required" or "addressable", and some considerations to make for each in undertaking a compliance effort:

1) Security Management Process – Providers must have policies and procedures to prevent, detect, contain and correct security violations.

a) *Risk Analysis (Required)* – Providers must conduct an assessment of potential risks to confidentiality, integrity and availability of EPHI.

b) *Risk Management (Required)* – Providers must implement security measures sufficient to reduce identified risks to a reasonable and appropriate level.

c) *Sanction Policy (Required)* – Providers must apply sanctions against workforce members who fail to comply with security policies and procedures.

d) *Information System Activity Review (Required)* – Providers must have procedures to regularly review records of information system activity, such as audit logs, access reports and security incident tracking reports. (Note: Reviews should promote awareness of activity that could suggest a security incident).

These specifications require providers to make an assessment of how EPHI flows within its organization and identify all systems and hardware involved in storing or accessing EPHI. What threats (i.e. human, natural and environmental) exist to information on those systems? How is senior management involved in risk mitigation decisions? What security measures are already in place, and are they communicated throughout the organization where appropriate? What controls exist on vendors or consultants that handle the organization's EPHI? Do existing sanction policies and procedures for workforce apply to violations of security procedures? Do employees understand the consequences of security procedure violations? Do existing systems permit audit and activity review? What, if any, audit logs or access reports get generated? Are whatever steps that are being taken documented?

CMS' list of items it might request in a security audit related to this standard includes an entity-wide security plan, documentation of a risk analysis and risk management plan,

an inventory log of media and devices that contain EPHI, an inventory of all information systems, including network diagrams of hardware and software used to store EPHI, a list of Primary Domain Controllers and servers, and a workforce sanction policy.

2) *Assigned Security Responsibility* – Providers must identify a security official responsible for the development and implementation of policies required by the Security Rules. Providers should ask whether there is any documentation of the security official who has been identified for this role and of other staff members who are responsible for general HIPAA compliance. Are roles and responsibilities for information security clearly defined?

3) *Workforce Security* – Providers need to implement policies and procedures to ensure that all members of its workforce have appropriate access to EPHI, and to prevent those who don't from accessing it. Note that although each implementation specification here is "addressable", providers must demonstrate some way they address the overall standard and document those decisions.

a) *Authorization and/or Supervision (Addressable)* - Procedures for authorization/ supervision of workforce members who work with EPHI (i.e. whether a particular user has right to carry out a certain activity – this may build on existing policies governing who can access PHI).

b) *Workforce Clearance Procedure (Addressable)* – Procedures to address that a workforce member's access to EPHI is appropriate.

c) *Termination Procedures (Addressable)* – Procedures for terminating access to EPHI when employment ends or changes.

Providers should consider how workforce members access rights to information systems is determined, whether job descriptions are associated with varying level of access, whether procedures for determining workforce access to systems are consistently applied, who can authorize access to systems and what processes exist to terminate access to systems if employment ends or an individual's job responsibilities change. CMS' audit request list requires a review of policies or procedures that address establishing and terminating system access, authentication methods used to identify authorized users, and requires the maintenance of a list of all user accounts for active and terminated employees, and information about employee background checks and confidentiality agreements.

4) Information Access Management – Providers must implement policies and procedures for authorizing access to EPHI that are consistent with HIPAA's Privacy Rule, such as restricting access to only include those with a need for access. The two implementation specifications for this standard are:

a) *Access Authorization (Addressable)* – Policies and procedures should identify how access is granted and who has authority to grant access privileges.

b) *Access Establishment and Modification (Addressable)* – Policies and procedures that establish, document, review and modify user's right of access to workstation, program or process.

Considerations here are similar to those for workforce security. Are there system access policies that address how access is established and modified? Do access rights bear any relationship to authorized users of PHI under the Privacy Rule? Does management review lists of employees with access rights to ensure they are consistent with authorized users? How is system use being monitored?

5) Security Awareness and Training – Providers must implement a security awareness and training program for all workforce members, including management. The following addressable implementation specifications must at least be considered by providers under this standard, and adopted if they are reasonable and appropriate to the provider's environment:

a) *Security Reminders (Addressable)* – Implement periodic security updates and document security reminders implemented.

b) *Protection from Malicious Software (Addressable)* – Implement procedures for guarding against, detecting and reporting malicious software. Training can address workforce role in protecting against malicious software (i.e. caution with email attachments) and system protection capabilities.

c) *Log-In Monitoring (Addressable)* – Training to address how users log onto systems and protect passwords. Implement procedures for monitoring log-in attempts and reporting discrepancies.

d) *Password Management (Addressable)* – Procedures for creating, changing and safeguarding passwords.

Providers should consider what kind of security training workforce currently receives. Are employees given instructions about password protection and prohibitions on sharing passwords? Is there a written policy for password management? CMS' audit request list includes a request for examples of training courses or communications to staff on security issues.

6) Security Incident Procedures – Providers must implement policies and procedures to address security incidents. Providers must have procedures to identify and respond to suspected or known security incidents, mitigate harmful effects, and document security incidents and outcomes. Security incidents include events such as stolen passwords, corrupted back-up tapes, virus attacks, theft of media with EPHI and unauthorized access by a former employee whose rights were not terminated timely.

Providers should consider whether workforce would understand how to identify an incident as relating to security and how to report it. Do procedures exist that contemplate possible security incidents and how to respond if they occur? A CMS audit may include a request for security violation monitoring reports.

7) Contingency Plan – Providers need to establish (and implement as needed) policies and procedures for responding to an emergency that damages systems that contain EPHI (i.e. fire, vandalism, system failure). The required implementation specifications under this standard are:

a) *Data Backup Plan (Required)* – Procedures to create and maintain retrievable exact copies of EPHI.

b) *Disaster Recovery Plan (Required)* – Procedures to restore any loss of data.

c) *Emergency Mode Operation Plan (Required)* – Procedures to enable continuation of critical business processes for protection of the security of EPHI while operating in emergency mode (i.e. due to power outage or technical failure).

Providers should consider whether back-up plans include backup of all important sources of data, whether recovery or emergency mode plans are known by appropriate individuals and accessible when needed, and whether there has been identification of people to be notified in the event of a system emergency and who is involved in the restoration process. Information about data backup and disaster recovery plans should be producible in the event of an audit. Additionally, there are two addressable specifications:

d) *Testing and Revision Procedures (Addressable)* – Periodic testing and revision of contingency plans (i.e. at a minimum to determine if existing contingency plans are appropriate).

e) *Applications and Data Criticality Analysis (Addressable)* – Assess relative criticality of specific applications and data (i.e. identify software applications and determine how important each is to patient care or business needs to prioritize need for data backup and other above contingency plan components).

Although these are addressable standards, one of the items on CMS' audit list is a request for an analysis of information systems, applications and data groups according to their criticality and sensitivity.

8) Evaluation - Providers are required to perform a periodic technical and nontechnical evaluation of its security policies and procedures based upon the Security Rule standards and in response to environmental or operational changes to consider how the requirements of the Security Rule are being met. For this, providers should consider whether security evaluations are being conducted currently, and whether simply time or certain events (i.e. security incident, new technology purchase) will trigger the conduct of an evaluation. Any evaluations being conducted should be documented (i.e. evaluation reports, analysis of whether changes are recommended). Keep in mind that evaluation does not necessarily mean the entire security program needs to be evaluated each time; providers can select particular areas of focus for different evaluations.

9) Business Associate Contracts – Providers must ensure that business associates that create, receive, maintain or transmit EPHI agree to the required security provisions in their business associate agreements. Providers should confirm that their form business associate agreements contain the required security terms, and review older, signed agreements to see if an updated form is needed to add these terms. CMS indicates on its audit list that it may request a list of contractors with access to EPHI and copies of business associate agreements.

## C. Physical Safeguards.

The physical safeguards under the Security Rules all relate to the physical measures, policies and procedures that are used to protect the provider's information systems and related buildings and equipment from natural and environmental hazards and from unauthorized intrusion. Some of these standards may be incorporated into and addressed under the policies developed under some of the administrative safeguard standards.

1) Facility Access Controls – Providers' policies and procedures must limit physical access to electronic systems and the facility(ies) where systems are housed, while ensuring that properly authorized access is allowed. The implementation specifications for this standard are:

a) *Contingency Operations (Addressable)* – Establish procedures that allow facility access in support of restoration of lost data under the disaster recovery and emergency mode of operations plans.

b) *Facility Security Plan (Addressable)* – Policies and procedures to safeguard the facility and equipment from unauthorized physical access, tampering and theft.

c) *Access Control and Validation Procedures (Addressable)* – Procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision (i.e. procedures that determine which workforce members have access to certain locations based on their function).

d) *Maintenance Records (Addressable)* – Procedures to document repairs and modifications to the physical components of a facility which are related to security (i.e. hardware, walls, doors and locks).

Does the provider's contingency plan identify procedures for facility access in the event of an emergency, such as loss of power and which personnel are allowed to enter the facility to perform data restoration? What controls are implemented to prevent unauthorized physical access to areas and equipment in the facility (i.e. surveillance cameras, locked doors, restricted area signs, ID badges, visitor badges, security service)? Do procedures identify methods to control or validate employee access to facilities (ID badges, key cards)? Do procedures identify roles or job functions authorized to access software programs for testing and revision? Are there policies or procedures that specify how to document repairs or modifications to physical components of the facility related to security?

2) Workstation Use - Providers must implement policies and procedures to specify how various classes of workstations that can access EPHI are to be used. Providers should consider whether procedures specify how to place and position workstations to allow viewing only by authorized individuals. Do procedures use additional security measures to protect workstations with EPHI, such as privacy screens, password protected screen savers or requirement to log off a workstation before leaving? Do policies address workstation use for users that access EPHI remotely? CMS' audit list asks for documentation of guidelines for each class of workstation (on site, laptop and home system usage).

3) Workstation Security – Providers must implement physical safeguards for all workstations that access EPHI to restrict access to authorized users. Providers should ask

how workstations are physically protected from unauthorized users and whether there is documentation of safeguards used in its policies and procedures for workstation use. Have all types of workstations been identified (i.e. laptops, PDAs)?

4) Device and Media Controls – Providers must implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain EPHI into and out of the facility, and the movement of these items within the facility.

a) *Disposal (Required)* – Polices and procedures must address the final disposition of EPHI and hardware or media on which EPHI is stored (i.e. degaussing, destruction of media).

b) *Media Re-Use (Required)* – Providers must implement procedures for removal of EPHI from electronic media before media is made available for re-use.

c) *Accountability (Addressable)* – Maintain a record of the movements of hardware and electronic media and any person responsible therefor.

d) *Data Backup and Storage (Addressable)* – Create a retrievable, exact copy of EPHI when needed before movement of equipment (Note: This standard can be addressed through the overall Data Backup Plan mentioned above).

Providers must consider whether its procedures address the disposal of EPHI and hardware or media used to store EPHI, including which personnel are authorized to dispose of EPHI or electronic media and whether specific technology is used to make hardware or electronic media unusable. Does the provider have procedures for the removal of EPHI from electronic media before re-use, and do those procedures specify when EPHI must be permanently deleted or only reformatted to make files inaccessible? Is there a process that tracks all hardware and electronic media (i.e. tapes, disks, digital memory cards) being used? Does it permit identification of individual devices by serial number or other mechanism? Is a record kept of movements of media containing EPHI? Do data backup procedures include situations for creating a copy of EPHI before equipment is moved? Could the provider produce an inventory log of the owner and movement of media and devices that contain EPHI?

## D. Technical Safeguards.

The technical safeguards of the Security Rules refer to the technology and the policies and procedures for its use that protect EPHI and control access to it.

1) Access Control – Providers must implement technical policies and procedures for systems that maintain EPHI to allow access only to those persons or software programs that have been granted access rights under the provider's information access management policies referred to in the administrative safeguard standards. Again, there is some overlap with these standards and those standards described under the administrative safeguards. Implementation specifications are:

a) *Unique User Identification (Required)* – Providers must assign a unique name and/or number for identifying and tracking user identity.

b) *Emergency Access Procedure (Required)* – Providers must establish and implement as needed procedures for obtaining necessary EPHI during an emergency. (Note: This should already be addressed under the contingency plan mentioned above.)

c) *Automatic Logoff (Addressable)* – Implement electronic procedures that terminate a session after predetermined time of inactivity.

d) *Encryption and Decryption (Addressable)* – Implement mechanism to encrypt and decrypt EPHI whenever deemed appropriate.

Providers should confirm that each workforce member has a unique user identification and that the identification can be used to track activity within the information systems that contain EPHI. They should also confirm that emergency plans have considered who needs access to EPHI in the event of an emergency and that policies are in place to provide access. Providers should consider whether there should be an automatic logoff feature on systems that access EPHI. Consideration should be given to whether there are some communications of EPHI for which encryption is appropriate. For instance, a provider's analysis about whether or not to employ encryption technology several years ago may be different when security policies are re-evaluated today, as the provider's use of electronic transmissions of EPHI and affordability of the technology may have changed.

A CMS or OIG audit may contain many requests around technical aspects of the provider's systems, including requests for policies and procedures concerning remote access activity, wireless networks, Internet usage, authentication and encryption mechanisms and termination for inactive computer sessions. Audit requests may also involve server configuration, patch management for systems storing EPHI, and use of antivirus software.

2) Audit Controls – Providers are required to implement hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI. Providers should examine the audit control capabilities of existing information systems with EPHI, and consider whether those controls permit the provider to comply with

administrative policies developed for the Information System Activity Review specification under the Security Management Process standard above.

3) Integrity – Providers must implement policies and procedures to protect EPHI from improper alteration or destruction. There is one addressable implementation specification for this standard, which is to consider use of electronic authentication mechanisms, or mechanisms to corroborate that EPHI has not been altered or destroyed in an unauthorized manner. Again, as an addressable standard, if these methods are not employed the provider should document why it made the decision it did and whether an alternative method for data integrity is being used.

4) Person or Entity Authentication – Providers must implement procedures to verify that a person or entity seeking access to EPHI is the one claimed, such as through use of a PIN or password, smart card or key, or use of a biometric mechanism (i.e. fingerprint, voice). Providers should document authentication methods currently being used, and consider whether other methods are available that would be reasonable and appropriate.

5) Transmission Security – Providers must implement technical security measures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network. There are two addressable implementation specifications to be considered for this standard: (a) Integrity Controls; and (b) Encryption. Providers should evaluate how often it is required to transmit EPHI and what security measures are currently used. Are the security measures to protect EPHI in transmission from unauthorized access or from being modified during transmission appropriate? Based on the provider's risk analysis, is encryption reasonable and appropriate to implement for some transmissions? A regulatory audit may request information about transmission mechanisms used to ensure data integrity during transmission, including portable media transmissions.

## E. Policies, Procedures and Documentation.

Other standards in the Security Rules require providers to (1) have business associate agreements with required security provisions for business associates that handle EPHI; (2) implement reasonable and appropriate written policies and procedures to comply with the standards and implementation specifications of the Security Rules; (3) maintain written records of activities and assessments for which documentation is required under the Security Rules;

(4) retain all documentation for 6 years from creation or the date it was last in effect (whichever is later); (5) make documentation available to persons responsible for implementing the procedures; and (6) review and update documentation periodically.

## F. Conclusion:

No matter where a provider is in its development of security management processes, it is a good time to take stock of how well those processes address the standards of the HIPAA Security Rules and how well the organization would be able to respond to regulatory inquiries about its security policies and procedures. Be sure as steps are taken to address security that there is documentation of any decisions made, that plans are developed based on risk assessments and that policies and procedures are implemented. In some cases, one provider policy may address multiple standards and implementation specifications under the Security Rules.

If not already engaged, senior management needs to be aware of the need to address security issues, what is being done and what resources or support may be needed to address security more effectively. Also, be sure that workforce members are trained to understand their security-related responsibilities and the institutional policies that have been implemented. Finally, the issue of security risk analysis, auditing and monitoring is an ongoing process in your organization that must be continually evaluated.

## Questions or Assistance?

If you have any further questions regarding the HIPAA Security Rules, please feel free to contact either Joan Feldman or David Mack.

**Joan Feldman**
(860) 251-5104
jfeldman@goodwin.com

**David Mack**
(860) 251-5058
dmack@goodwin.com



SHIPMAN & GOODWIN LLP

COUNSELORS AT LAW