Plan Sponsor’s Guide to the HIPAA Security Rule

Compliments of Aetna

We want you to know™
We live in a world with ever increasing Internet and e-mail access, networking capabilities, and automation of data, including health information. These advances bring you efficiencies, but also elevated concerns about the privacy, security and integrity of your employees’ health information.

Fortunately, when the Health Insurance Portability and Accountability Act (HIPAA) was passed by Congress and signed into law in 1996, it included Administrative Simplification guidance (Title II, Subtitle F) that includes standards for health information privacy and security.
Background on HIPAA

When HIPAA was originally passed in 1996 and for many years thereafter, most of the focus was centered on certain health insurance-related issues such as federal health care fraud and abuse laws, limitations on exclusions for pre-existing conditions, availability of health insurance coverage for small employers, and the rights of individuals to apply for health coverage when they lose their existing group coverage.

Within the last several years, however, more attention has shifted to the five components of the Administrative Simplification section of HIPAA. The five components are: Privacy, Electronic Transactions, Code Sets, Unique Identifiers, and Security. Each of the Administrative Simplification components has its own compliance date.

Employers that sponsor group health plans, health care providers, and insurers have in recent years been particularly aware of the sweeping effect of the Privacy Rule, paying close attention to the need to undertake specific tasks in order to be in compliance with the Privacy Rule by its April 14, 2003 deadline.

The HIPAA Privacy Rule governs the use and disclosure of Protected Health Information (PHI) for those “covered entities” defined as health plans, health care clearinghouses and health care providers who transmit health information electronically. The Privacy Rule covers PHI that is transmitted or maintained in any form or medium (e.g., electronic, paper and oral communications).
The HIPAA Security Rule — The Next Phase in HIPAA Administrative Simplification Compliance

The compliance date for the new HIPAA Security Rule is April 21, 2005. (Small health plans will have until April 21, 2006 to implement.) The Security Rule requires covered entities to institute administrative, technical, and physical safeguards to protect individually-identifiable health information when it is in electronic form ("electronic protected health information" or "ePHI").

The HIPAA Security Rule primarily impacts health care providers and insurers, but also affects employers that sponsor group health plans. While the Security Rule does not directly regulate employers, the requirements do apply to self-funded group health plans. If you have not done so already, we urge you to consult your professional/legal advisors for guidance on how the Security Rule impacts you and what, if anything, you need to do to comply.

Privacy refers to the right of an individual to control his or her personal health information and to not have it divulged or used by others against his or her wishes. The Privacy Rule covers PHI.

Security applies to safeguards put in place to protect the integrity, availability and confidentiality of personal health information. The Security Rule covers ePHI.

The focus on security and integrity includes precautions for such things as network firewall breakthroughs, e-mail and computer viruses, and compromised passwords. All of
these can lead to computer “crashes” or overloading critical computer servers, which, in turn, can disrupt the flow of health information or affect the integrity of health information, by corrupting data that is being transmitted. Organizations must protect against these outside breaches as well as put safeguards in place to protect against internal carelessness or malicious individuals who may take advantage of system vulnerabilities to access and misuse personal health information.

The Responsibility of Covered Entities

To comply with the HIPAA Security Rule, a covered entity must apply reasonable and appropriate administrative, technical and physical safeguards to:

- Ensure the confidentiality, integrity and availability of any ePHI it creates, receives, maintains or transmits;
- Protect against any reasonably anticipated threats or hazards to the security or the integrity of ePHI;
- Protect against reasonably anticipated unauthorized uses or disclosures of ePHI; and
- Ensure compliance by its workforce.

The Security Rule also requires a covered entity to review its current security policies, procedures and safeguards against the Rule’s requirements and decide upon and implement risk management measures proportional to the risks it faces.
Similarities Between the HIPAA Security Rule and the HIPAA Privacy Rule

The HIPAA Security Rule was designed to complement the HIPAA Privacy Rule, and, therefore, has adopted much of the same terminology and definitions used in the Privacy Rule. In addition, many of the Security Rule requirements mirror those of the HIPAA Privacy Rule — the following are some notable examples:

- **Security Official** — A covered entity must designate a security official responsible for developing and implementing its security policies and procedures.

- **Security Policies and Procedures** — A covered entity must inventory, evaluate and, as needed, develop new security policies and procedures and/or amend existing policies and procedures to reflect the requirements of the HIPAA Security Rule.

- **Security Awareness and Training** — A covered entity must train its employees on its security policies and procedures.

- **Health Plan Documentation** — A health plan’s documents must contain appropriate and reasonable security standards for the plan, and the plan sponsor must agree to abide by these standards before the plan may disclose ePHI to the plan sponsor.

- **Business Associate Agreements** — A covered entity must have a written contract with each “business associate” that contains certain prescribed assurances regarding the business associate’s security practices.
Simplifying Business Associate Agreements

A covered entity does not have to have separate Business Associate Agreements to meet the HIPAA Privacy Rule and the HIPAA Security Rule. Instead, you can update each applicable Business Associate contract amendment to include provisions that require the Business Associate to implement security safeguards for ePHI. For new Business Associate relationships, you can create a contract that includes the Business Associate provisions required by both the HIPAA Privacy Rule and the HIPAA Security Rule.

Note, health plans are considered the Business Associate of those self-funded plans for which they perform services that involve the use of PHI and ePHI (e.g., claims administration, utilization management, disease management, etc.).
How Employers Can Comply with the HIPAA Security Rule

Frequently Asked Questions and Answers

By: Mark Lutes
mlutes@ebglaw.com

The following set of Frequently Asked Questions and Answers, relating to the issues plan sponsors must deal with, is provided as a courtesy by the Law Firm of Epstein Becker & Green, P.C., in Washington, D.C.
What is the HIPAA Security Rule? When is its Implementation Date?

The Security Rule is a companion to the HIPAA Privacy Rule that became effective April 14, 2003. The Security Rule became final last year and all but small plans must implement the rule’s requirements by April 21, 2005. Small group health plans (those with receipts of $5 million or less) have until April 21, 2006 to implement it.

How does the scope of the Security Rule compare to that of the Privacy Rule?

The Privacy Rule covered all individually identifiable health information that was not exempt and thus was deemed “protected” (“PHI”). It has one general statement about the security of PHI — that a covered entity is to use “appropriate” administrative, physical and technical safeguards.

The Security Rule is a little narrower insofar it requires that the safeguards only be applied to electronic protected health information (“ePHI”), although it is more prescriptive than the Privacy Rule as to how the organization is to assess risk to the ePHI and document that it has instituted appropriate safeguards.

ePHI is covered by the rule whether it is “at rest” in a storage device (e.g., hard drive, CD or tape) or “in transit” (e.g., over Internet, dial-up, EDI or FTP). Some information that is not considered to be in electronic form includes data transmitted in person-to-person telephone calls, by copy machines, by fax machines, or using voice mail.
Do employers have responsibilities under the HIPAA Security Rule?

Not directly. The obligations fall on the employer’s group health plan (“GHP”). However, employers are often the administrators of the GHP and, in that capacity, will want to arrange for the GHP’s compliance. Also, if, as discussed in more detail below, an employer receives ePHI in other than summary form from the GHP, an HMO or a health insurer, it will need to both amend the GHP’s plan documents to provide that the ePHI is appropriately safeguarded and will need to act to implement those safeguards.

Will the typical insured plan sponsor have these responsibilities?

The typical insured plan sponsor will not need to amend its GHP documents because it will only be receiving either enrollment and disenrollment ePHI or ePHI in summary form that will be used only for obtaining premium bids and for “plan settlor” functions — e.g., modifying, amending or terminating the plan. However, the insured employer, acting as a GHP administrator, may wish to help the insured GHP comply with the rule with respect to the ePHI it maintains or transmits.

What ePHI is it typical for an insured or self-funded GHP to hold or transmit?

The full range of ePHI is generally maintained and transmitted by a self-funded plan’s business associates on the plan’s behalf. Moreover, an insured or self-funded GHP might, for example, determine that it holds data related to beneficiary questions — coverage questions and claims status questions. The GHP
might also determine that it maintains or transmits enrollment or disenrollment data. While the enrollment and disenrollment data is viewed, for Privacy Rule purposes, as not, by itself, requiring the institution of a privacy notice and other features of a privacy program administration, the maintenance or transmission of that data is not exempt from the scope of the Security Rule. An insured or self-funded GHP might also trigger Security Rule obligations by maintaining claims data that would, for Privacy Rule purposes, be judged to be subject only to the limitations placed on the disclosure and use of “summary health information.”iii Finally, self-funded plans will frequently have claims appeal data.

What is the basic thrust of the Security Rule?

The rule requires the GHP to put in place appropriate “administrative” (e.g., policies and procedures, risk assessment, training), “physical” (e.g., facility access controls, workstation safeguards) and “technical” (e.g., log-in and audit controls) to safeguard the “confidentiality, integrity and availability” of the GHP’s ePHI against reasonably anticipated risks.

The rule details the process for performing a risk assessment and applying safeguards to the risks identified through eighteen standards that include forty-two specifications. Certain specifications are considered “required” although only in the context of mitigating a reasonably anticipated risk. Other specifications are deemed “addressable.” An addressable specification can be implemented or the GHP could choose not to do so if it documents why it is not appropriate to its environment.
Can the GHP be compliant without a risk assessment?

No. While many safeguards need not be adopted if the plan documents appropriate circumstances, it is impossible to create the appropriate documentation without a risk assessment. A GHP is not expected to eliminate all security risk — but it is required to understand the risks and reduce the risks to what it deems to be an acceptable level.

A risk assessment need not be undertaken by third party consultants. The plan administrator can undertake the assessment using the methodologies propounded by the National Institute of Standards and Technology ("NIST"), the International Standards Organization ("ISO"), or other standards organizations. The NIST resource guide for implementing the security rule is at http://hipaa-compliance.info.

GHPs will want to be cautious about the creation of third party risk analysis by consultants interested in selling particular services or technology. The report of a consultant, recommending such technologies, might require the plan to document why those technologies are in fact not appropriate safeguards given its risk profile.
What approaches to risk assessment should be considered?

GHPs will wish to compare the merits of “qualitative” risk analysis (assets requiring protection assigned exposure levels relative to each threat) with “quantitative analysis” (objective numerical values assigned to components of risk and loss). The difficulties of assigning dollar values to the loss expectancy associated with each threat to the confidentiality, integrity and availability of ePHI may commend qualitative or modified qualitative methodologies to GHPs.

What should the result of the risk assessment be?

Based on risks identified, decide how and (if applicable) whether to implement additional administrative, physical and technical safeguards. The GHP must respond to each risk but can use a flexible approach. Do not presume that the remediation will require major capital expenditures. Presume that remediation will require additional conceptualization of security safeguards and documentation of same.

What are typical administrative safeguards?

The risk analysis itself (which should be re-performed as threat configurations change) is a fundamental administrative safeguard. Assigning security responsibility to an individual is also fundamental. Implementing policies as to workforce security, application of sanctions to workforce members that fail to comply with procedures and regular review of information system activity (audit logs, access reports and security incident reports) are also core needs.
What are typical physical safeguards?

Physical safeguards that are addressed in response to a risk assessment need include facility access controls, a facility security plan, work station controls, and device and media controls.

What are typical technical safeguards?

Unique user identification and emergency access controls are required. Automatic log-off, encryption and decryption are addressable safeguards. Audit controls which record and examine system activity will also typically be part of a technical safeguard program. Electronic mechanisms can also be employed to corroborate that data has not been altered or destroyed.
What are the legal risks/penalties for non-compliance?

The general HIPAA penalties are likely to apply — e.g., civil penalties of $100 per violation for up to $25,000 per standard per year. Criminal penalties (fines and imprisonment) apply to “knowing misuse.”

However, other negative consequences could also occur:

- FTC or state attorney general actions based on “unfair or deceptive acts or practices” in information handling;
- tort claims based on failure to adhere to these new standards of care;
- and/or adverse publicity due to strong media interest in data privacy/security.

The legal liabilities for employers might also include claims of breach of fiduciary duty (grounded in ERISA) relative to GHP assets. Stock companies’ risks could include shareholder action alleging failure to cause adoption of, or supervision of reasonable protection for, corporate assets. External auditors may also fault the company for failure to institute appropriate controls for this exposure, as required by the Sarbanes Oxley legislation.
Are insured GHPs largely exempt?

The Privacy Rule exempted from most documentation obligations those insured plans that receive PHI only in the form of summary health information. In contrast, the Security Rule contains no such exceptions. Therefore, GHPs, even if insured, seem to have the obligation to do a risk assessment and document the safeguards applicable to the ePHI they have — most commonly enrollment and disenrollment information. The other common instance wherein the insured GHP might be deemed to have risk analysis and other compliance responsibilities is when it or its agents maintains or transmits ePHI in the context of beneficiary advocacy.

Is the GHP only responsible for safeguarding the ePHI it holds?

Section 164.502(e) of the Privacy Rule and Section 164.308(b) of the Security Rule each state that the Covered Entity may allow another entity to create or receive PHI on its behalf “if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information.” Both rules call for those assurances to be documented in a contract. A stand alone version of such a contract is commonly called the “business associate agreement” although the required covenants can be included in agreements that contain terms and conditions unrelated to privacy or security.

One might hypothesize that self-funded plans have an ERISA duty of care with respect to their delegation of the handling of ePHI to an administrator. However, the Security Rule itself does not clearly establish a duty of inquiry for the plan. Section 164.314 of the Security Rule simply restates the
Privacy Rule’s admonition that a covered entity is not in compliance if it “knew of a pattern of activity or practice” that constituted a breach of the business associate’s obligation under the agreement and it failed to take reasonable steps to cure the breach or, if the cure was unsuccessful, to terminate the relationship if feasible or report to the Secretary if termination was not feasible.

**What “business associate” covenants related to security must the GHP obtain from its vendors?**

The business associate must covenant that it will implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the ePHI it creates, receives, maintains or transmits on behalf of the GHP and that it will “ensure” that its agents, including subcontractors, do the same. The business associate must also covenant to report to the covered entity any security incident of which it becomes aware. Finally, the agreement must authorize the GHP to terminate the business associate’s handling of ePHI if the GHP becomes aware that the business associate has violated a material term of these covenants.
Must the GHP obtain “business associate” covenants from the plan sponsor with respect to its handling of ePHI on behalf of the Plan?

Such covenants generally need not be obtained from the plan sponsor. However, unless the plan sponsor only receives enrollment or disenrollment information from the plan and any other ePHI it receives is in the form of summary health information and is used only for obtaining premium bids or modifying, amending or terminating the plan, the GHP’s plan documents must be amended to specify that the plan sponsor “will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted” by it on behalf of the GHP.

How should these changes to the Plan documents be made?

Employers will want to work with counsel, benefits consultants and others who advise them on health plan issues to make HIPAA conforming changes to their plan documents and to give appropriate notice of such changes or to create plan documents if none currently exist. Self-funded plans will want to coordinate these efforts with any third parties performing their administration.

Where should my company/plan start?

1. Coordinate among employee benefit and information system personnel to identify the ePHI that the plan receives or transmits and perform a risk analysis with respect to each application that houses or transmits ePHI.
2. Your analysis should address the risks to the confidentiality, integrity and availability of the ePHI on each application utilized by or in support of the GHP as well as the current safeguards addressing those risks. It should focus on critical risks and consider the probability of such risks.

3. Use the results of the risk analysis to add additional administrative, physical and technical safeguards to reduce critical and probable risk to an acceptable level. Remember that the Security Rule does not require that the GHP eliminate risks to the ePHI — only that it formally assess those risks on a periodic basis and appropriately apply available resources to respond to reasonably anticipated risks.

4. Formally document the GHP’s policies, procedures and risk management decisions. Repeat the exercise on a regular basis — particularly where the applications used by the GHP have changed or the company undergoes change as a result of merger or acquisition. Monitor change in “best practices” for electronic security and incorporate such change into risk remediation choices and plans.

5. If ePHI other than summary health information is reviewed or if the plan sponsor’s uses exceed plan settlor functions, consult your advisers and amend plan documents to specify that the plan sponsor “will reasonably and appropriately safeguard” the ePHI.

By Mark E. Lutes, mnlutes@ebglaw.com

i The information furnished herein is of a general educational nature and does not constitute legal advice. Each plan sponsor should consult with counsel as to the particulars of its situation.

ii We include a paper discussing the approaches at http://hipaa-compliance.info

iii For purposes of the Rule, “summary health information” is information that summarizes the claims history, claims expenses, or types of claims experienced by beneficiaries of the group health plan from which identifiers have been deleted.

This set of Frequently Asked Questions is provided by Epstein Becker & Green, P.C. for general information purposes; it is not and should not be used as a substitute for legal advice. Copyright 2004© Epstein Becker & Green, P.C. All Rights Reserved.
We at Aetna hope you find this information helpful.

This information summarizes selected elements of the HIPAA Security Rule, but does not include a full statement of these or related regulations. Please remember that this information is not intended as legal advice and that plan sponsors should consult their own professional/legal advisors regarding compliance with the Security Rule.

If you would like further details or have questions about Aetna’s compliance with the HIPAA Security Rule, please contact your Aetna account executive or account manager.

For more information about Aetna please visit our website at www.aetna.com.

“Aetna” is the brand name used for products and services provided by one or more of the Aetna group of subsidiary companies. The Aetna companies that offer, underwrite or administer benefit coverage include Aetna Life Insurance Company. While this material is believed to be accurate as of the print date, it is subject to change.