HIPAA
The Privacy and Security Provisions

ON THE FRONT LINES
OF WORKPLACE LAW™

HIPAA
THE PRIVACY AND SECURITY PROVISIONS

TABLE OF CONTENTS

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) created a new and complicated set of requirements for group health plans and their vendors. HIPAA was designed to improve the portability of health insurance coverage, reduce health care costs by standardizing certain health care transactions, and increase the security and privacy of health care information.

Starting with plan years beginning on or after July 1, 1997, group health plans were required to comply with HIPAA's portability, special enrollment and nondiscrimination provisions. Basically, these "Title I" HIPAA requirements made health coverage more portable for people changing jobs by restricting the extent to which health plans could exclude coverage of preexisting conditions. That first wave of HIPAA requirements also mandated that plans allow certain mid-year enrollments, and prohibited discrimination based on health status, such as a history of high health claims.

By contrast, the Privacy Rules and Security Rules contained in HIPAA Title II, which became effective later, created a complex regulatory scheme evidenced by hundreds of pages of guidance and regulations issued by the United States Department of Health and Human Services (HHS), the Federal agency which oversees Title II. This booklet focuses on these regulations and the steps that employers, their group health plans, plan insurers, and business associates should take to comply with HIPAA's Privacy and Security requirements.

As with any brief overview of a complex subject, this is no substitute for competent legal counsel. Rather, our goal is to provide a clear explanation, in non-technical language, of the highlights of this important area of the law. For answers to specific fact situations or for more thorough legal guidance, consult an attorney.

Introduction

HIPAA's Title II is deceptively referred to as "Administrative Simplification." Nothing could be further from the truth. In fact, Title II sets out detailed new standards controlling Privacy issues, establishing Security rules, and setting out uniform standards for electronic transactions.

A. Privacy Rules

The Privacy rules were designed to protect "individually identifiable" health information, and required all "covered entities" to be in compliance by April 14, 2004. The phrase "covered entities" refers to health insurance companies, health care providers that conduct certain transactions electronically, health care clearinghouses, and group health plans. The American Recovery and Reinstatement Act of 2009 (ARRA) expanded HIPAA to apply directly to business associates. Business associates are required to be in compliance by February 17, 2010. Business associates are persons or entities that perform certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provide services to, a covered entity.

B. Security Standards

Hand-in-hand with HIPAA's Privacy requirements, the Security standards regulate the integrity and confidentiality of protected health information in electronic form and required all covered entities to be in compliance by April 21, 2006. Business associates are required to be in compliance by February 17, 2010.

C. Standards For Electronic Transactions (SFETs)

SFETs are intended to improve efficiency and reduce health care costs by standardizing the electronic transfer of certain information between and among covered entities and business associates. SFETs primarily represent software challenges.

Coverage

The Privacy and Security regulations severely restrict the flow of Protected Health Information (PHI) between health plans, their sponsors, and business associates. However, every benefit plan or employer is not covered by the Privacy and Security rules, and every piece of health information is not PHI. The regulations directly govern only "covered entities," which do not include employers. They also define PHI and electronic PHI, or ePHI, and closely control its allowable uses and disclosures. Before considering how to meet HIPAA's requirements, you must identify 1) relevant covered entities and business associates; 2) who, if anyone, in your organization comes into contact with PHI or ePHI; and 3) how and when employees or other representatives use or disclose PHI or ePHI.

A. Identifying Covered Entities

Doctors, hospitals, pharmacies and in some cases on-site clinics (health care providers), billing, processing and repricing entities (health care clearinghouses), and group health plans are all covered entities under HIPAA. Although employers are not covered entities, they are nevertheless concerned with HIPAA compliance if they sponsor a group health plan. Since the distinction between a group health plan and its sponsor may be little more than a piece of paper, and since the health plan will not likely have employees of its own, the employer sponsor will have to ensure that its plan or plans comply with HIPAA's requirements.

Unless a health plan has fewer than 50 participants and is self-insured and self-administered, it is covered by HIPAA. Furthermore, the broad definition of "group health plan" encompasses not only medical plans, but also dental and vision plans, health care flexible spending accounts (FSAs) and some employee assistance plans (EAPs). Not all employee welfare benefit plans are covered because not all provide or pay for medical care. For example, life and disability plans are not covered by HIPAA's rules. Workers' compensation plans are also excluded from HIPAA.

As you develop HIPAA compliance strategies, be careful not to overlook plans such as FSAs, dental, vision and EAPs. An employer who sponsors more than one plan may want to designate them collectively as an Organized Health Care Arrangement (OHCA), which will create compliance efficiencies such as using a joint HIPAA Privacy Notice.

B. Identifying Business Associates

A "business associate" is a person or entity that performs certain functions or activities that involve the use or disclosure of PHI or ePHI on behalf of, or provides services to, a covered entity. A member of the covered entity's workforce is not a business associate. A covered health care provider, health plan, or health care clearinghouse can be a business associate of another covered entity. The Privacy Rule lists some of the functions or activities, as well as the particular services, that make a person or entity a business associate, if the activity or service involves the use or disclosure of PHI or ePHI. The types of functions, or activities that may make a person or entity a business associate include payment or health care operations activities, as well as other functions or activities regulated by the Administrative Simplification Rules.

Business associate functions and activities include claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management; and re-pricing. Business associate services are legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, and financial.

Examples of business associates include:

- a third party administrator that assists a health plan with claims processing;
- a CPA firm whose accounting services to a health care provider involve access to protected health information;
- an attorney whose legal services to a health plan involve access to protected health information;

- a consultant that performs utilization reviews for a hospital;
- an independent medical transcriptionist that provides transcription services to a physician; or
- a pharmacy benefits manager that manages a health plan's pharmacist network.

C. PHI And ePHI

PHI is individually identifiable health information that has not been excluded from HIPAA coverage. PHI may be in any form or medium, including but not limited to electronic (ePHI). Individually identifiable health information is protected if it is 1) created or received by a covered entity, 2) relates to an individual's past, present or future medical care, and 3) is either identifiable as to an individual or there is a reasonable basis to believe that it could be.

D. "Employment Records" Excluded From Coverage

Significantly, "employment records" are excluded from the definition of PHI, although the regulations do not define what constitutes an employment record. In fact, depending upon its origin or use, the same piece of information can be protected PHI or an unprotected employment record. As a rule of thumb, documents that do not flow to or from a covered entity are not PHI. For example, in the hands of an employer, pre-employment drug screens, sick leave requests and fitness-for-duty examinations are employment records not subject to HIPAA although the records may be subject to other privacy laws. Likewise, records that an employer obtains from an employee or a health care provider for purposes of complying with the Americans with Disabilities Act or the Family and Medical Leave Act are not PHI in the hands of the employer.

Obviously, the legal fiction that distinguishes an employer/plan sponsor from its group health plan can lead to significant confusion when company employees such as human resources personnel have access to information that could be PHI, non-PHI, or both, depending upon the source. Despite this dilemma, one thing is certain: if an employer/plan sponsor

receives PHI/ePHI from a covered group health plan, the employer will have to deal with the morass of Privacy requirements. And, PHI in the hands of an employer's health plan will be subject to HIPAA's detailed Privacy laws. Fortunately, the sponsor of a fully-insured plan may be able to shift much of this burden to the plan insurer if it can operate its health plan without receiving PHI/ePHI.

In understanding and complying with the Privacy and Security regulations, keep in mind the law's over-arching goals. With respect to group health plans, HIPAA seeks to 1) prevent PHI/ePHI from being used in any employment decisions; and 2) allow individual plan participants to exercise their rights freely, without interference. Therefore, in addition to complying with the detailed requirements of the Privacy and Security rules, you should continually assess whether your actions are consistent with the overall goals of the regulations.

E. Preemption Of State Laws

Preemption is a legal term that refers generally to instances in which federal law overrides any conflicting state law. Although recent court decisions have made some inroads, the Employee Retirement Income Security Act of 1974 (ERISA) broadly overrides all state laws that purport to govern employee medical plans or other covered benefits.

Unlike ERISA, HIPAA's preemption rules are not straightforward. The Privacy rules preempt all contrary state laws, unless the state laws provide greater protection for individuals and their PHI. Nevertheless, before it is deemed to provide greater protection, the contrary state law must survive ERISA preemption as well. Therefore, if a state privacy law survives ERISA preemption and provides greater protection than the HIPAA Privacy regulations, the state privacy law will prevail, but not otherwise.

There are some exceptions to the general HIPAA preemption rule where state laws will not be preempted, such as laws preventing fraud and abuse, laws maintaining state regulation of insurance and health plans, and laws permitting states to continue reporting health care delivery and costs. Preemption

is a complicated issue, and you should generally consult with counsel for assistance.

F. Recordkeeping

Although rarely mentioned, recordkeeping is a core HIPAA responsibility. Covered entities and business associates are required to keep all records necessary to ensure that they have complied with the HIPAA requirements, and to cooperate with HHS in any investigation or compliance review. Generally, records must be retained for six years from the date the record was generated or last in effect, whichever is later.

Avoiding Or Limiting The Full Compliance Burden

Full HIPAA compliance (discussed later) is clearly onerous. Fortunately, there are instances in which less than full compliance is acceptable.

First, although self-insured plans bear a greater overall compliance burden than fully-insured plans, any employer/plan sponsor may receive PHI for the limited plan administration purpose of tracking enrollment and disenrollment without assuming additional obligations.

Second, the employer or business associate may receive information that has been cleansed of individually identifiable information and, depending upon its form and use, avoid significant compliance burdens. The most common form of cleansed information a business associate or employer/plan sponsor may choose to receive from the plan is “summary health information.”

Receiving only summary health information may be a viable solution for some, but if this option is chosen, you must recognize that 1) the definition of summary health information is very precise, and failure to meet it may nullify efforts to avoid the full compliance burden; 2) summary health information may be used only for limited purposes; and 3) if you later receive PHI, you may still have to fulfill significant compliance obligations.

A. What is Summary Health Information?

Summary health information is information summarizing the claims history, expenses, or types of claims experienced by individuals, and from which all of the following information has been deleted:

- names;
- geographic subdivisions smaller than a state (including addresses, cities, counties or parishes, although the first five digits of a zip code may be retained);
- all elements of dates (except year) directly related to an individual (including birth date, admission or discharge dates, date of death, and all ages over 89 and elements of dates, including year, which indicate age. Ages and elements may be aggregated into a single category of age 90 or older);
- telephone numbers;
- fax numbers;
- e-mail addresses;
- Social security numbers;
- medical record numbers;
- health plan beneficiary numbers;
- account numbers;
- certificate/license numbers;
- vehicle identifiers and serial numbers, including license plate numbers;
- device identifiers and serial numbers;
- web Universal Resource Locators (URLs);
- internet protocol (IP) address numbers;
- biometric identifiers, including finger and voice prints;

- full face photographic images and any comparable images; and
- any other unique identifying numbers, characteristics, or codes (except that the covered entity may assign a means of record identification to allow de-identified information to be re-identified by the covered entity), provided the codes used are not related to information about the individual and not capable of being translated to identify the individual, and the covered entity does not disclose the means for re-identification.

B. Uses Of Summary Health Information

An employer or business associate choosing to receive summary health information may use it only for the limited purposes of modifying or terminating the plan or for seeking bids for coverage. If you receive PHI, or use summary health information beyond the prescribed purposes, you may become subject to HIPAA's other Privacy and Security burdens.

C. Alternatives To Summary Health Information

An employer/plan sponsor or business associate of a fully-insured plan may avoid some compliance responsibilities by receiving a "limited data set," which also carries a specific definition and may be used only pursuant to a data use agreement, or by using "de-identified information," which likewise has a very specific definition but is not subject to the Privacy and Security regulations because this information is no longer PHI/ePHI. Consult your attorney before deciding whether to use either of these options.

Major Compliance Categories For Privacy

If it cannot avoid the full HIPAA compliance burden by receiving and using cleansed information as described above, the plan sponsor of a group health plan and its business associate will have significant obligations which may include:

- allowing individuals to exercise their individual rights;

- providing a Privacy Notice;
- adhering to use and disclosure requirements;
- fulfilling administrative requirements;
- amending the plan document; and
- executing business associate agreements.

Each is discussed in more detail below. In addition to complying within these categories, no one may retaliate against individuals who exercise their HIPAA Privacy rights, and they may not require individuals to waive their rights. They must also honor requests for confidential communication of participants' PHI.

A. Individual Rights

HIPAA requires that individuals must be able to access their PHI and request corrections. Decisions on requests to amend records must be made within 60 days (with a single 30-day extension if the covered entity/business associate informs the requestor in writing of the reasons for the delay and provides a date upon which the request will be determined). If the amendment is accepted, the covered entity/business associate must make the amendment, inform the requestor of this fact, and inform others of the amendment if the covered entity/business associate either knows they have the unamended information, or if the requestor identifies them.

Individuals also have a right to an accounting of disclosures of their PHI/ePHI other than disclosures made for treatment, payment, or health care operations, disclosures to the individual, or disclosures made pursuant to the individual's authorization during the prior six years. Effective January 1, 2014, individuals may also request disclosures of "electronic health records" related to treatment, payment or health care operations. However, the time period in this request may not be longer than the prior three years. An electronic health record is an electronic record of health-related information on an individual that is created, gathered, managed and consulted by authorized health care clinicians and staff.

For purposes of HIPAA, "payment" is an activity undertaken by a health plan to determine or fulfill its responsibility for provision of benefits, or to obtain or provide reimbursement for health care. This includes eligibility and coverage determinations, as well as adjudication of health benefit claims, among other activities. "Operations" means activities compatible with or directly related to treatment or payment, such as internal quality oversight review, credentialing, legal services, auditing functions, general administration, underwriting and other activities related to the creation, renewal or replacement of a contract of health insurance or health benefits, as well as other functions.

Participants also have the right to request restrictions on the use or disclosure of their PHI/ePHI, and to request confidential communications of PHI/ePHI. Despite this right, a covered entity or business associate is not required to grant such a request. Effective February 17, 2010, however, the Plan must agree to a request for restrictions if the disclosure is to a health plan and for the purpose of payment or health care operations and the disclosure relates to a health care expense for which the individual has already paid. Finally, written policies must exist to support the exercise of all individual rights.

B. Privacy Notice

Individuals must be informed of their rights and the covered entity's Privacy practices through a written "Privacy Notice." As is the case with most HIPAA Privacy requirements, the content and format of the Privacy Notice are painstakingly set forth in the regulations. A fully- insured plan is not automatically responsible for distributing the Notice; that burden generally falls upon the insurer. However, if the plan will disclose summary health information to the plan sponsor, that disclosure must be included in the Notice. Also, self-insured plans and any plans that receive more than summary health information or use summary health information for more than the narrow allowable purposes, are primarily responsible for providing the Privacy Notice.

It is a good idea to mail the Notice to the covered employee's home. New enrollees must receive a Notice on or before enrollment, and all participants must be reminded of the existence of the Notice at least once every three years.

Additionally, if a covered entity maintains a website that describes its services or benefits, a copy of the Notice must be displayed on the website. Privacy Notices may be sent electronically, but only if the individual first consents to receive the Notice in that fashion.

C. Use and Disclosure Requirements

Covered entities and business associates must obtain specific "authorizations" for most uses and disclosures of PHI other than those allowable uses discussed above, such as enrollment/disenrollment tracking or treatment, payment or health care operations. An authorization must describe its particular purpose(s) and the subject information may not be used or disclosed for purposes beyond the authorization. Authorization forms are required to contain numerous express elements, and execution of an authorization by an individual must be informed and voluntary.

Authorizations must be completed in writing, and the individual must receive a copy of the signed form. The form must be clear and unambiguous. Business associates, employers, and others may rely upon the authorization for as long as it is in force, but the individual may revoke it at any time. Significantly, in most cases an employer may not condition enrollment in the health plan upon execution of an authorization.

One of the most common instances in which an employer or business associate may need to obtain an authorization occurs when a plan participant seeks the employer's help in resolving a question related to a health plan claim or benefit. Individuals are, or course, free to share their own PHI directly with anyone. But an insurance company cannot use or disclose PHI with the employer or business associate unless it has obtained a valid authorization from the individual, or unless the employer/plan sponsor has amended the plan document and certified its compliance with the amendments (described in more detail below).

The regulations create a "Minimum Necessary Use" standard which requires covered entities and business associates to take reasonable efforts to limit use and the disclosure of PHI to the minimum necessary to accomplish the reason for each use, disclosure or request. This concept is intended to prevent situations such as disclosure of a patient's entire medical record when a small portion of the record will fulfill the purpose underlying the need for information. A minimum necessary policy is among those that entities should establish under the next set of requirements, Administrative Safeguards.

D. Administrative Requirements

Covered entities and business associates must implement various Privacy policies and procedures. Among other things, these requirements include naming Privacy officials, training pertinent employees regarding Privacy policies and procedures, establishing a complaint process and developing sanctions for employees who violate the Privacy rules.

The covered entity and business associate must also implement administrative, technical and physical safeguards to protect PHI. This includes adopting policies and even such steps as locking doors and file cabinets. The rules require employers and business associates who handle PHI to establish firewalls between employees who receive PHI and those who do not have access to it. This includes appropriate written policies, procedures and measures to address violations.

E. Plan Document Amendment and Employer Certification

If a sponsor receives PHI or uses summary health information beyond the prescribed limited purposes, the plan document must be amended to describe, among other things, what information the employer may receive, the classes of employees who will receive it, and the safeguards which will be implemented to protect the information received. The amendment must also limit the use of such information to plan administration purposes, provide a mechanism for resolving non-compliance, and require the plan sponsor to honor

individual rights, report any inconsistent acts to the plan, make records available for audit, require its business associates to observe the same restrictions, return or destroy PHI received, if feasible, and certify compliance with all plan amendments.

As with the other requirements associated with HIPAA Privacy, the mandatory plan amendments are described in detail by the regulations. The employer/plan sponsor's certification of compliance with the plan amendments, while perhaps superfluous in substance, represents yet another formality necessary to achieve compliance.

F. Business Associate Agreements

When a covered entity such as a health plan uses another entity, such as a third party administrator (TPA), to help it perform functions covered by the Privacy regulations, the rules require the covered entity to obtain assurances that the third party will protect PHI that it uses or discloses on behalf of the plan. The covered entity obtains such assurances through execution of a "business associate agreement," another document for which the HHS has provided detailed guidance.

The Department's rules set forth the minimum provisions that must appear in business associate agreements. Effective February 17, 2010, a business associate using PHI in performing services to its client, the covered entity, is also responsible for insuring a business associate agreement is in place.

Applying The Privacy Rules

A. To Employers/Plan Sponsors

As sponsors of an employee group health plan, employers face varying levels of compliance obligations, depending primarily upon three factors:

- is the plan fully-insured;
- does the plan provide PHI or summary health information to the plan sponsor; and

- does the plan sponsor use summary health information beyond its limited purposes.

Your answers to these questions will determine what steps you must take to comply with the Privacy rule. Various combinations of answers may create slightly different results, but the self-insured or insured dichotomy is the best starting point for this analysis. We refer you to the HIPAA Privacy Decision Tree in Appendix A.

1. Fully-Insured Plans

As a general rule, fully-insured plans have the lightest compliance burden. If the employer receives only summary health information from the plan and uses it only for amending the plan and seeking premium bids, the employer need not undertake the responsibilities described under any of the five major HIPAA compliance categories listed above.

However, the plan's insurer must provide a Privacy Notice to participants, and the plan must allow them to exercise their rights and honor requests for confidential communication. Most importantly, employers must be careful that they do not receive PHI/ePHI or use summary health information beyond the prescribed purposes, thus incurring a much greater compliance burden.

If the sponsor of a fully-insured plan uses summary health information beyond the purposes allowed in the regulations, it must amend its plan document to set forth those purposes, including all of the descriptions and assurances described above. The sponsor must also certify to the plan that it will comply with the amendments. If the sponsor chooses to receive PHI/ePHI (generally, anything more than summary health information), it must undertake compliance within all of the major categories listed above, including plan amendment and the other administrative requirements.

2. Self-Insured Plans

Self-insured plans are more likely to result in the plan sponsor's exposure to PHI/ePHI, so the HIPAA compliance burden is

greater, beginning with the requirement of providing a Privacy Notice. Sponsors of self-insured plans must also ensure that the plans comply with HIPAA's use and disclosure requirements, administrative safeguards and individual privacy rights requirements. If the Plan Sponsor receives information beyond summary health information or uses summary health information beyond the prescribed purposes, it must also comply with the detailed requirements for certification and amending the plan document.

B. To Business Associates

As of February 17, 2010, the Privacy (and Security) rules apply directly to business associates. Business associates who use, create or maintain PHI or ePHI must perform a HIPAA compliance analysis, train employees with access to PHI/ePHI, ensure business associate agreements are in place, and develop Privacy and Security policies and procedures.

The HIPAA Security Rule

The Security Rule covers the administrative, technical and physical security measures that covered entities and business associates are required to take with regard to electronic storage and transmission of electronic Protected Health Information (ePHI). Many of the Security standards work in concert with the Privacy Rule that took effect before the Security Rule.

The final Security Rule provides general principles and an implementation process, rather than detailed mandates or prescribed technologies. The Security Rule also allows covered entities and business associates to evaluate and determine how to apply many of the Security standards based on the facts of each situation. The intent of the Security Rule is best summarized in the preamble where HHS stated, "we have focused more on what needs to be done and less on how it should be accomplished."

The deadline for most plans to comply with the Security Rule was April 20, 2005, but small plans (those with less than $5 million in receipts during their last fiscal year) had an extra year to comply. On February 17, 2010, as part of the American Recovery and Reinvestment Act of 2009 (ARRA), business associates became directly subject to requirements of the HIPAA Security Rule.

The Security Rule establishes guidelines for the minimum requirements to ensure confidentiality, security and integrity of electronically stored and transmitted health information. The Security Rule does not provide specific instruction on how covered entities or business associates should safeguard ePHI. However, it does provide a process of evaluation that covered entities and business associates could use to determine what would constitute "appropriate safeguards."

The overriding theme of the Security Rule is flexibility. The preamble of the Security Rule states that each organization must analyze its own situation and work within the constraints of its situation and resources.

A. What Information Is Subject To The Security Rule?

The Security Rule requires covered entities and business associates to safeguard and protect PHI maintained or transmitted in electronic form (ePHI). Additionally, as part of the Security Rule, HHS updated the definition of PHI to clarify that PHI includes information that is transmitted by electronic media, maintained in electronic media or maintained in any other form or medium.

The term "electronic media" is defined as 1) electronic storage media, including computer hard drives and any removable/transportable digital memory medium such as magnetic tape or disk, or digital memory card, 2) transmission media used to exchange information already in electronic storage media, for example, extranet, leased lines, dialup lines, private networks, and 3) the physical movement of removable/transportable electronic storage media. Further, the Security Rule clarifies that certain transmissions, such as paper-to-paper faxes, person-to-person telephone calls, video

teleconferencing and/or messages left on voice mail are not "electronic media" and, accordingly, are not subject to the safeguards required under the Security Rule.

Because HHS moved the definitions of electronic media and PHI to the general definition section in the HIPAA regulations, these definitions apply to all of the HIPAA Administrative Simplification regulations–i.e., Security, transactions and code sets, and Privacy regulations.

B. Who Must Comply With The Security Rule?

The Security Rule provisions apply to three categories of covered entities. These three categories are the same as those under the Privacy Rule. Therefore, if an entity is a covered entity under the Privacy Rule, it is a covered entity under the Security Rule. The three categories of covered entities under the Security Rule are:

- health plans;
- health care clearinghouses; and
- health care providers that transmit certain health claims transactions electronically.

Prior to February 17, 2010, the HIPAA Security Rule only applied indirectly to business associates that performed services for covered entities, if the services involve PHI/ ePHI through the business associate agreement. As of February 17, 2010, however, the Security Rule applies directly to business associates.

The Security Rule attempted to synchronize with the Privacy Rule by requiring that all business associate agreements provide that the business associate will: 1) implement administrative, physical and technical safeguards to protect ePHI it creates, receives, maintains or transmits on behalf of the covered entity; 2) ensure that any agent or subcontractor to whom it provides the covered entity's ePHI agrees to implement safeguards to protect the ePHI; 3) report to the covered entity any security incidents of which it becomes aware; and 4) authorize termination of the agreement by the covered entity, if the covered entity determines that the

business associate has violated material terms of the agreement.

C. "De-Identified" Information

Although not addressing the issue to any great degree, the preamble to the Security Rule notes that de-identified information is not covered by the Security Rule because it is no longer ePHI.

How Is The Security Rule Structured?

The Security Rule requirements are called "standards." Each standard offers a generalized Security requirement and is followed in most cases by "implementation specifications." The implementation specifications identify what the covered entity or business associate must do to meet a standard and each one is either a "required specification" (R) or an "addressable specification" (A). The Security Rule contains both required and addressable implementation specifications and a security standards matrix (attached as Appendix B) that designates the specifications with either an "R" or an "A." A "required specification" must be implemented as stated in the regulations. For example, backup data plans and disaster recovery plans are required standards.

For an "addressable specification," the covered entity and business associate are given more options. They must decide to do one of the following: 1) address the specification directly, 2) implement an alternative that covers the same general concept identified in the standard, 3) do a combination of both, or 4) do nothing.

The decision made by the covered entity/business associate must be based upon a security risk assessment and if the covered entity/business associate chooses to use an alternative solution, or decides to do nothing, the basis for that decision must be documented in writing. Included in the documentation should be the covered entity's/business associate's decision, the rationale behind the decision, and an explanation of how the standard is being met. Cost can be

used as a factor in these decisions, but the preamble to the Security Rule notes that adequate Security measures still must be implemented.

Major Compliance Obligations for Security

The Security Rule specifies that covered entities and business associates must meet four general Security requirements:

- ensure the confidentiality, integrity and availability of all ePHI the covered entity or business associate creates, receives, maintains or transmits;
- protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
- protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the Security Rule; and
- ensure compliance by the workforce.

These requirements must be met by applying the standards found in the Security Rule. The Security Rule standards are grouped under three headings: administrative safeguards, physical safeguards, and technical safeguards. The covered entity/ business associate will know what measures are reasonable and appropriate by engaging in a risk analysis and then implementing measures to handle the risks identified.

Essentially, the covered entity/business associate must engage in a risk analysis to determine how to comply with the Security Rule standards. Compliance with the standards will be determined based on the effectiveness and feasibility of the measures in ensuring the confidentiality, integrity and availability of ePHI.

A. Administrative Safeguards

The administrative safeguards are actions, policies and procedures to manage the selection, development, implementation and maintenance of Security measures to

protect ePHI and to manage the conduct of the covered entity's/business associate's workforce in relation to the protection of the information. Specifically, the administrative safeguards must address the following areas:

1. Security Management Process

Implement policies and procedures to prevent, detect, contain and correct security violations. There are four enumerated implementation specifications, all of which are required. These include a) a risk analysis to detect the potential risks and vulnerabilities, b) risk management to implement Security measures to reduce risks and vulnerabilities, c) a sanction policy to apply appropriate sanctions against workforce members who fail to comply with the policies, and d) information system activity review to examine records of information system activity, such as audit logs, access reports and security incident tracking reports.

2. Assigning Security Responsibility

Identify a security official to develop and implement policies and procedures.

3. Workforce Security

Develop policies and procedures to ensure appropriate workforce access to ePHI and to prevent unauthorized access by those who should not have access to the information.

4. Information Access Management

Implement policies and procedures for authorizing access to ePHI. This includes isolating health care clearinghouse functions if they are part of a larger organization.

5. Security Awareness and Training

Implement a Security awareness and training program for all members of the workforce (including management) with access to ePHI. The amount of training is to be determined by the organization.

6. Security Incident Procedures

Implement policies and procedures to address security incidents. This includes identifying and responding to suspected and known security incidents.

7. Contingency Plan

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 containing ePHI. This requires developing and implementing a backup data plan, a disaster recovery plan and an emergency-mode operation plan.

8. Evaluation

Perform a periodic technical and non-technical evaluation, based initially on the standards, to see the extent to which the entity's Security policies and procedures meet the requirements of this section. The covered entity or business associate may make a business decision to obtain external certification, but is not required to do so to comply with the standard.

B. Physical Safeguards

Each covered entity/business associate is required to address the following physical safeguards standards that concern the physical protection of data systems and data from intrusion and from environmental or natural hazards. The physical safeguard standards are as follows:

1. Facility Access Controls

Implement policies and procedures to limit physical access to electronic information systems and the facilities in which they are housed, while ensuring that properly authorized access is allowed. These controls would include the following implementation features: disaster recovery, emergency mode operation, need-to-know procedures for personnel access and sign-in requirements for visitors.

2. Workstation Use

Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstations that can access ePHI. For example, logging off before leaving a workstation unattended.

3. Workstation Security

Implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users. A risk assessment will need to be performed to gauge the appropriate solutions to workstation security issues.

4. Device and Media Controls

Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility and the movement of these items within the facility.

The purpose of these standards is to protect a covered entity's/business associate's computer systems and related building and equipment from fire and other natural hazards, as well as unauthorized intrusion.

C. Technical Safeguards

The technical safeguard standards address the technology and the policies and procedures for its use that protect ePHI and control access to it. The following are included in the technical safeguards:

1. Access Control

Implement technical policies and procedures for electronic information systems (computers) that maintain ePHI to allow access only to those persons or software programs that have been granted access as specified by the Security safeguards. This standard requires the assignment of a unique name and/or

number for identifying and tracking user identity, and establishing procedures for obtaining necessary ePHI during an emergency. Some facilities may wish to use encryption as a method of denying access to information in a file.

2. Audit Controls

Implement hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI. These are to be put in place to record and examine system activity. Entities have flexibility in implementing the standard in a manner appropriate to their own needs.

3. Integrity

Implement policies and procedures to protect ePHI from improper alteration or destruction. Error-correcting memory and magnetic disc storage are examples of the built-in data authentication mechanism that are commonplace in hardware and operating systems today.

4. Person or Entity Authentication

Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed. For example, digital signatures and soft tokens may be used to implement this standard.

5. Transmission Security

Implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network. Integrity controls and encryption are recommended to achieve this standard.

D. Documentation And Policy And Procedure Requirements

The Security Rule requires covered entities/business associates to implement and maintain written policies and procedures to comply with the Security Rule if they have access to ePHI. The same is true for any actions, activities or assessments required to be documented, such as the risk assessment analysis. Covered entities/business associates must

maintain this documentation for six years from the latter of the date of its creation or the date when it last was in effect.

E. Hybrid And Affiliated Entity Requirements

The provisions relating to affiliated and hybrid entities under the Privacy Rule also apply under the Security Rule. This means that the responsibilities of affiliated covered entities and hybrid entities for the maintenance of ePHI under the Security Rules can be implemented in the same manner as their responsibilities with respect to use and disclosure of PHI under the Privacy Rule.

Breach Notification

As part of ARRA, the Health Information Technology for Economic and Clinical Health (HITECH) Act added a new requirement (effective September 23, 2009) that covered entities (including group health plans and health care providers) notify individuals, and business associates notify covered entities, when an individual's "unsecure" PHI is breached. But, it also created an exception to the breach notification requirement for breaches of "secure PHI."

Secure PHI is PHI/ePHI maintained in accordance with the most current HHS guidance specifying the safe harbor technologies and methodologies that render PHI/ePHI unusable, unreadable or indecipherable by unauthorized persons. In April 2009, HHS issued its first guidance as to what an organization must do to secure PHI/ePHI: a specific level of encryption and specific types of destruction. HHS expects to update this guidance annually. Covered entities and business associates which satisfy the current HHS safe harbor technologies and methodologies do not have to send notices to individuals upon a breach of PHI/ ePHI.

If required, the notification of breach must be provided to individuals within 60 days after discovery of the breach (or the day the entity should have discovered the breach if it had been prudent in its HIPAA compliance efforts). If the breach involves 500 or more individuals' PHI/ePHI, HHS and the media must also be notified within 60 days. If less than 500 individuals are

affected, the breach must be logged and submitted annually to HHS.

Business associates must notify covered entities of their breaches so that covered entities can timely meet the notice requirements. However, a business associate and a covered entity can agree, as part of the business associate agreement, that the business associate will notify affected individuals directly in case of a breach by the business associate.

Enforcement

HIPAA enforcement is left to the HHS Office of Civil Rights, which is empowered to hear complaints from individuals and to conduct compliance audits. Individual complaints must be filed within 180 days after the individual knows of the violation, though the Office of Civil Rights can waive this requirement for good cause. The law also includes provisions prohibiting employers from retaliating against employees for filing complaints.

Violation of HIPAA requirements can result in a civil penalty ranging from $100 to $50,000 per violation, and $25,000 to $1,500,000 for similar violations in the same year. “Knowing” misuse of PHI/ePHI is a criminal matter with a fine not to exceed $50,000 and possible imprisonment of up to one year. If the offense is committed under false pretenses, the fine is capped at $100,000 and imprisonment at five years. If the offense involves commercial advantage, malice, or personal gain, the maximum fine increases to $250,000 and potential imprisonment expands to ten years.

Preparing for Compliance with Privacy & Security Rules

To ensure compliance, you should designate a HIPAA implementation team and a privacy official (and if ePHI is involved, a security official), whether or not the regulations specifically require this. Initially, the team should determine which parts of the organization may be a covered entity, business associate and/or a plan sponsor. An entity whose

operations include both covered and non-covered functions under HIPAA may designate itself as a hybrid entity, subjecting only that portion of the organization involved in covered functions to HIPAA's requirements. In a hybrid entity, the covered portion of the organization must be cautious not to disclose PHI/ePHI to the non-covered portion. (An employer/plan sponsor is not a hybrid entity simply because it sponsors a group health plan.)

After identifying all covered entities and business associates, identify who, when and how your employees come into contact with PHI/ePHI or other individually identifiable health information. With respect to group health plan(s), you should also identify business associates of each plan.

With respect to each individual plan's compliance, the employer/plan sponsor should carefully evaluate whether the plan is insured or self-insured, whether it receives summary health information or PHI/ePHI from the plan, and how it uses the information it receives. If it receives information which it does not need, the employer and business associate should act to eliminate this information where possible in order to limit potential liability.

If applicable, there are more steps that should be taken to ensure that you will comply with the Security Rule. Covered entities and business associates should undertake the following action plan.

1. Identify all ePHI maintained or transmitted by the covered entity/business associate.

The Security Rule applies to all ePHI, but not to written or oral forms of PHI. Therefore, covered entities/business associates should undertake a PHI mapping process to assess their use and transmission of ePHI in order to determine the information and data media that will fall under the Security requirements.

2. Establish information access controls.

Covered entities and business associates should draft written policies and procedures for ePHI access and controls. Among the procedures to be considered are implementation of unique

log-in names, password protection of electronic files, and means of tracking security incidents. In addition, covered entities/business associates should draft sanctions procedures for employees who violate the entity's security policies, as well as personnel termination procedures to eliminate access to ePHI by former employees.

For example, a checklist could be developed for employee termination that includes items such as changing locks, removing the employee's passwords or other access to such information, removing user accounts, and turning in keys or cards that allow access.

3. **Develop mechanisms to protect ePHI from improper use or destruction.**

Covered entities and business associates should begin implementing security mechanisms to verify that ePHI has not been altered or destroyed while being transmitted to or from the covered entity/business associate and implementing technical security measures to guard against unauthorized access to ePHI transmitted by the covered entity/ business associate over an electronic communications network such as the Internet.

4. **Conduct risk analysis and implement risk management measures.**

The HIPAA Security team should conduct a risk assessment identifying the potential risks of improper disclosure and vulnerability of ePHI maintained or transmitted in the covered entity's/business associate's database. This risk assessment should identify potential risks to the confidentiality of ePHI stored and transmitted by the business associate or covered entity such as unauthorized access by former employees, hackers and the potentially devastating effects of computer viruses and worms. Business associates and covered entities must document their findings.

After the Security team conducts the assessment, it should develop and put in place a risk management program designed with sufficient measures to reduce the Security risks and

vulnerabilities identified in the risk assessment. It also should begin developing a contingency plan for responding to emergencies. This plan should list processes to create file backups, include a criticality analysis of what information is necessary to administer the covered entity/business associate, include a disaster recovery plan, and an emergency mode of operations plan, as well as testing and revision procedures.

5. Conduct security awareness training.

Similar to the Privacy Rule, the Security Rule requires each covered entity and business associate to train its workforce. Specifically, all employees with access to ePHI, including management or supervisory employees, need to be trained on Security provisions and the protection of ePHI. The training should involve awareness training, periodic Security reminders, user education concerning virus protection of malicious software such as viruses and worms, emphasis on the importance of monitoring login success and failure and user education regarding passwords.

The preamble to the Security Rule states that this training could be provided as part of the new employee orientation with supplemental training as necessary, such as when new technologies are introduced or when changes are made to the Security policy.

6. Refer to NIST for risk assessment.

On several occasions, HHS makes reference to guides published by the National Institute of Standards and Technology (NIST), as an aid in risk assessment and in the security management process. The NIST "800 Series" publications are important as practical guides that expand upon explanations by HHS of steps to follow and criteria to use, in assessing risk and managing security implementation. The guides also will be important references in enforcement of the Security Rules and in other litigation over security issues; therefore, a covered entity/business associate should consider consulting these guides as it works to address and implement the Security Rule.

7. **Ensure that business associate agreements include the Security Rule provisions.**

The Security Rule necessitates that business associate agreements include language protecting ePHI. Each business associate and covered entity should evaluate its business associate agreements to ensure that the language is broad enough to comply with the Privacy and Security Rule provisions.

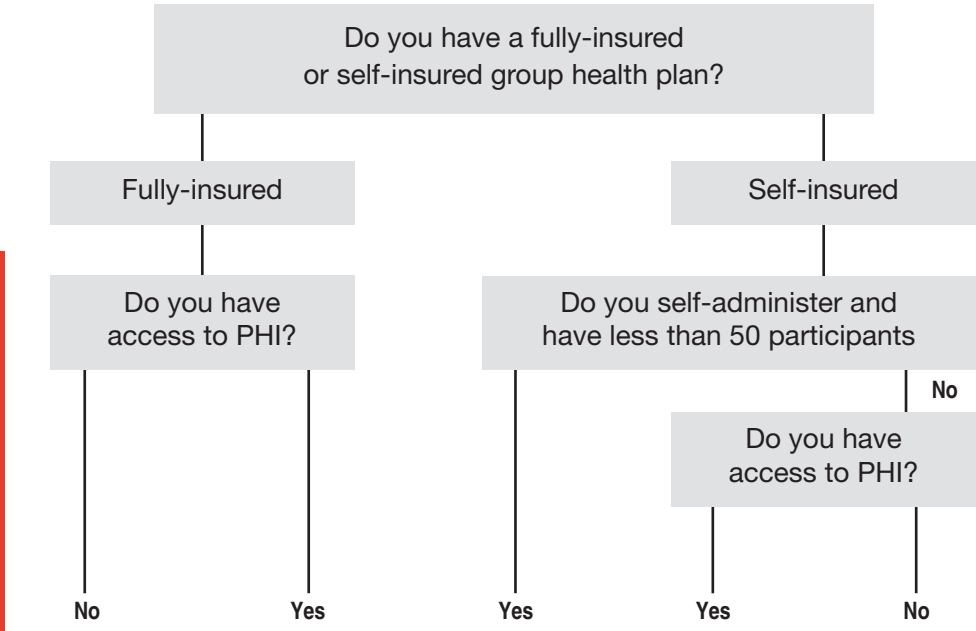
Conclusion

Although the goals of HIPAA's privacy and security regulations are relatively straightforward, its intricate requirements are not. HIPAA's coverage is broad enough to encompass almost every employer that sponsors a group health plan, including plans such as FSAs that might not be immediately apparent. Unfortunately, there is no one-size-fits-all solution because of the variables involved and because the employer/plan sponsor will have to abide by whatever HIPAA solutions it adopts. Moreover, because the law is so new, it is not yet apparent how it will be interpreted, revised and enforced over the coming months. HIPAA is truly a work in progress.

Whether identifying covered plans, analyzing specific compliance obligations or developing notices, forms, policies or procedures, the process of complying with HIPAA's privacy and security regulations is complex and time-consuming. We hope this booklet helps provide a starting point.

For further information about this topic, contact any office of Fisher Phillips or visit our website at www.fisherphillips.com.

Appendix A
HIPAA PRIVACY COMPLIANCE DECISION TREE



- No Compliance *requirements for employer as plan sponsor except as noted in the caveat below.*

You Need:

1. *Business Associate Agreement,*
2. *HIPAA Privacy Policies and Procedures Manual,*
3. *Authorizations as necessary,*
4. *Written HIPAA training materials,*
5. *Job description of HIPAA Privacy Official,*
6. *Plan amendment, and*
7. *Plan certificate of compliance.*

- No Compliance *requirements, except as noted in the caveat below.*
- *Full Access to PHI is permitted.*

You Need:

1. *Notice of Privacy Practices,*
2. *Business Associate Agreement,*
3. *HIPAA Privacy Policies and Procedures Manual,*
4. *Authorizations as necessary,*
5. *Written HIPAA training materials,*
6. *Job description of HIPAA Privacy Official,*
7. *Plan amendment, and*
8. *Plan certificate of compliance.*

You Need:

1. *Notice of Privacy Practices,*
2. *Business Associate Agreement,*
3. *HIPAA Privacy Policies and Procedures Manual,*
4. *Written HIPAA training materials, and*
5. *Job description of HIPAA Privacy Official*

CAVEAT: Regardless of HIPAA Compliance obligations described above, a group health plan may not require individuals to waive HIPAA privacy rights, and may not intimidate or retaliate against individuals for exercising HIPAA privacy rights.

Appendix B
HIPAA SECURITY STANDARDS MATRIX

STANDARDS	SECTIONS	IMPLEMENTATION SPECIFICATIONS (R)=REQUIRED, (A)=ADDRESSABLE
Administrative Safeguards (see § 164.308)		
Security Management Process	164.308(a)(1)	Risk Analysis (R) Risk Management (R) Sanction Policy (R) Information System Activity Review (R)
Assigned Security Responsibility Workforce Security	164.308(a)(2) 164.308(a)(3)	(R) Authorization and/or Supervision (A) Workforce Clearance Procedures (A) Termination Procedures (A)
Information Access Management	164.308(s)(4)	Isolating Health Care Clearinghouse Function (R) Access Authorization (A) Access Establishment and Modification (A)
Security Awareness and Training	164.308(a)(4)	Security Reminders (A) Protection from Malicious Software (A) Log-in Monitoring (A) Password Management (A)
Security Incident Procedures Contingency Plan	164.308(a)(6)	Response and Reporting (R) Data Backup Plan (R) Disaster Recovery Plan (R) Emergency Mode Operation Plan ® Testing and Revisions Procedure (A) Applications and Data Criticality Analysis (A)
Evaluation Business Associates Contracts and Other Arrangements	164.308(a)(8) 164.308(b)(1)	(R) Written Contract or Other Arrangement (R)
Physical Safeguards (see § 164.310)		
Facility Access Control Workstation Use Workstation Security Device and Media Controls	164.310(a)(1) 164.310(b) 164.310(c) 164.310(d)(1)	Contingency Operations (A) Facility Security Plan (A) Access Control and Validation Procedures (A) Maintenance Records (A) (R) (R) Disposal (R) Media Re-use (R) Accountability (A) Data Backup and Storage (A)
Technical Safeguards (see § 164.312)		
Access Control Audit Controls Integrity Person or Entity Authentication Transmission Security	164.312(a)(1) 164.312(b) 164.312(c)(1) 164.312(d) 164.312(e)(1)	Unique User Identification (R) Emergency Access Procedure (R) Automatic Logoff (A) Encryption and Decryption (A) (R) Mechanism to Authenticate Electronic Protected Health Information (A) (R) Integrity Controls (A) Encryption (A)

OTHER BOOKLETS IN THIS SERIES:

Age Discrimination in Employment Act

Americans With Disabilities Act
(Public Accommodations)

Americans With Disabilities Act
(The Employment Aspects)

Business Immigration

COBRA

Employment Discrimination

FLSA
(Exemptions & Recordkeeping)

FLSA
(Wage & Hour Provisions)

FMLA

National Labor Relations Act
(Unfair Labor Practices)

National Labor Relations Act
(Union Organizing)

OSHA

Sexual Harassment

USERRA

WARN Act

ON THE FRONT LINES
OF WORKPLACE LAW™