SUMMARY OF HIPAA PRIVACY RULES

I. Introduction

The privacy rules regulate the use and disclosure of protected health information (PHI) by defining who is authorized to access PHI created or maintained by covered entities and for what purposes. There are three types of covered entities under the privacy rules: health plans **(which include Health FSAs and HRAs)**, health care clearinghouses and health care providers who transmit certain standard transactions electronically. Employers that are not in the health care services field normally will not be covered entities. Nevertheless employers, as health plan sponsors must agree to comply with certain privacy requirements if they want to receive PHI from their health plans.

Health plan sponsors should understand and recognize the following basic concepts under the Privacy Rules: (1) what is PHI, (2) which plans are considered health plans under the privacy rules, and (3) who are business associates.

What is PHI?

PHI is individually *identifiable health information* that is maintained, created or transmitted by a covered entity. Individually identifiable health information is health information that relates to an individual's past, present or future physical or mental health or condition or to the provision of health care to that person, or to the past, present or future payment for that person's health care. Examples of PHI held, created, or maintained by health plans include claims information and claims payment history. Enrollment and disenrollment information is also PHI in the hands of the covered entity or its vendors; however, such information appears to be subject to less restrictive use and disclosure rules (see "Implications of the HIPAA Privacy Rules on Plan Sponsor" below for more information on how the HIPAA privacy rules treat enrollment and disenrollment information)

What is a Covered Entity?

There are three types of covered entities under HIPAA's Privacy Rules: health plans (including Health FSAs), health care clearinghouses and health care providers who transmit certain standard transactions electronically. Employers that are not in the health care services field normally will not be covered entities. Nevertheless, plan sponsors must agree to comply with certain privacy requirements if they want to receive PHI from their health plans. (See "Implications of Privacy Rules on Health Plan Sponsors" for more information on how the Privacy Rules affects plan sponsors.

What is a Health Plan?

The privacy rules define a health plan as an individual or group plan that provides (or pays the cost of) medical care. This definition includes virtually all arrangements that pay the cost of medical care, including, but not limited to:

- Group health plans,
- Health insurance issuers,
- HMOs,

- ERISA plans,
- Medicare and Medicare+Choice,
- Medicaid,
- Medicare supplement policies,
- Issuers of long-term care policies, and
- Welfare benefits plans or other arrangements that provide health benefits for two or more employees.

Health plans that are both self-administered and self-funded and that have fewer than 50 participants are excluded from the definition of a health plan under HIPAA. This exception will not apply to a plan that uses a third-party administrator. Further, there is a regulatory exception for accident-only plans, disability plans, liability insurance plans, workers' compensation programs and on-site medical clinics.

What is a "Business Associate"?

Because health plans have no employees, it is often necessary for plan sponsors to engage the services of third parties to perform various plan related functions. When services are provided on behalf of the health plan (e.g., claims processing), the service provider is known as a "business associate." TPAs, consultants, insurance agents and brokers, claim auditors, and utilization review companies are all examples of business associates to the extent that they perform services on behalf of the health plan. Although business associates are not covered entities subject directly to HIPAA's Privacy Rules, health plans must ensure that business associates protect the PHI that they receive from and on behalf of the health plan. To achieve that end, the Privacy Rules provide that health plans (through their plan sponsors) must enter into business associate agreements with the business associates that will legally obligate the business associates to agree to restrictions on the use and disclosure of PHI. Health plans must execute business associate agreements with all of their service providers before the effective date of the privacy rules. Note that employees of the plan sponsor and the plan sponsor itself are *not* business associates of the health plan.

II. The Privacy Obligations of the Plan

As indicated above, the Privacy Rules regulate the use and disclosure of PHI by covered entities. There are three fundamental components to the Privacy Rules: (a) permissible uses and disclosures, (b) individual rights, and (c) administrative safeguards.

What are the Permissible Uses and Disclosures?

A covered entity cannot use or disclose PHI without a "HIPAA authorization" from the covered individual unless the use or disclosure is for treatment, claims payment, or health care operations (i.e., operations related to claims payment and treatment) or the use or disclosure falls within one of the listed public policy exceptions.

Health plans are most likely to use PHI in connection with activities related to payment and health care operations. "Payment" means an activity undertaken by a health plan to obtain contributions, to determine or fulfill its responsibility for provision of benefits under the health plan, or to obtain or provide reimbursement for health care. Payment includes eligibility and

coverage determinations, billing, claims management, collection activities and related health care data processing. "Health care operations" refers to activities compatible with and directly related to treatment or payment, such as internal quality oversight review, credentialing and health provider evaluation, underwriting, insurance rating, and other activities relating to creation, renewal, or replacement of a contract of health insurance or health benefits (including stop-loss insurance and excess insurance), medical review, legal services, and auditing functions (including fraud and abuse detection), business planning, management and general administration and fundraising.

In addition, to the uses and disclosures for treatment, payment and health care operations, plans may also use and disclose PHI for certain mandated disclosures for public policy and safety reasons without an individual's authorization. These uses and disclosures include:

- Uses and disclosures required by law;
- Uses and disclosures for public health activities;
- Disclosures about victims of abuse, neglect, or domestic violence;
- Uses and disclosures for health care oversight activities;
- Disclosures for judicial and administrative proceedings;
- Disclosures for law enforcement purposes;
- Uses and disclosures about decedents;
- Uses and disclosures for cadaver organ, eye, or tissue donation purposes;
- Uses and disclosures for certain limited research activities;
- Uses and disclosures to avert a serious threat to health or safety;
- Uses and disclosures for specialized government functions; and
- Disclosures for workers' compensation.

Please note that a use or disclosure of PHI pursuant to another federal or state law must be a "required" use or disclosure to be disclosed by the other law and not just a permitted use or disclosure or the exception does not apply. In addition, disclosures must be made to the Department of Health and Human Services in connection with its enforcement and compliance review actions.

If a health Plan desires to use or disclose PHI for any reason other than those set forth above, it must obtain permission, in the form of a "HIPAA authorization" from the person who is the subject of the PHI.

A valid HIPAA authorization must contain the following:

- Description of the information to be disclosed;
- Identification of person(s) authorized to use or disclose PHI and to whom PHI may be disclosed;
- Purpose of the requested disclosure;

- Expiration date or event that would terminate the authorization;
- Signatures by individual whose information will be disclosed; and
- Statements regarding right to revoke authorization, inability to condition treatment, payment, enrollment or eligibility for benefits on authorization and potential for redisclosure.

The Privacy Rules require that the authorization be written in "plain language" and the individual must receive a signed copy of the authorization if such authorization was sought by the covered entity.

Reasons for seeking an authorization will vary. For example, individuals may request to have their PHI disclosed by a health plan for applications for life or disability insurance or for purposes of a lawsuit. A plan sponsor may request an authorization from an individual to allow the plan to disclose medical claims records for FMLA leave or a request for reasonable accommodation under the ADA.

Further a health plan may not condition treatment or payment on an authorization, except in very limited circumstances.

What are an individual's rights under HIPAA?

The Privacy Rules grant individuals certain rights with respect to their health information. Health plans must provide rights to access and amend PHI, provide an accounting of disclosures of PHI, and provide a privacy notice.

An individual has the right to inspect and copy his or her own PHI that is maintained in a "Designated Record Set." For health plans, a "Designated Record Set" is the plan's enrollment, payment, claims adjudication, and case or medical management records or those records used by the plan to make decisions about individuals. A plan is only required to provide an individual with the right to inspect and copy his or her PHI that is maintained in a Designated Record Set.

The plan may require individuals to make requests for access to PHI in writing, so long as individuals are notified in the privacy notice that their requests must be in writing. The plan must respond to an access request within 30 days for PHI that the plan maintains on site or within 60 days if the information is not on site.

The plan is not always required to agree to provide access to an individual's PHI. Access may be denied in certain specified circumstances (e.g., psychotherapy notes). If the plan denies the request it must provide the individual with a written denial that includes the reason for the denial, a statement about the individual's right to review the denial (if applicable); and a description of the plan's complaint procedures, including the name, title and telephone number of the covered entity's contact person or office.

An individual has the right to request an amendment or correction to his or her PHI maintained in a Designated Record Set that is inaccurate or incomplete. The plan may require individuals to make request for corrections in writing and provide support for the requested change, so long as these requirements are communicated to individuals in the privacy notice. If the plan denies the request, it must provide a written notice of the denial that includes:

- The basis for the denial;

- The individual's right to submit a written statement disagreeing with the denial and how to file such statement;

- That the individual may (if he or she does not submit a written statement of disagreement) request that the request for amendment and denial be included in future disclosures of the information; and

- A description of the covered entity's complaint procedures, including the name, title, and telephone number of the covered entity's contact person or office.

The plan must implement a process to track and timely respond to individual requests for amendments, the denials of the amendment by the covered entity, the individual's statement of disagreement, and the covered entity's rebuttal, as applicable. The covered entity must respond to an amendment request within 60 days, and it may extend this period by 30 days, if it gives the participant notice within the original 60-day period.

An individual also has the right to obtain an accounting of certain limited disclosures of his or her own PHI. This right to an accounting extends to disclosures made by covered entities at any time in the last six years (but not including any time prior to the applicable effective date of HIPAA's Privacy Rules, as the case may be). This right does not include disclosures for treatment, payment health care operations, disclosures to individuals about their own PHI, disclosures of health information authorized by the individual and for certain other limited purposes. The accounting must include the date of the disclosure, the name of the receiving party, a brief description of the information disclosed, and a brief statement of the purpose of the disclosure. The covered entity must respond to an accounting request within 60 days.

The health plan is also required to provide a notice of privacy practices for PHI to all individuals enrolled in the health plan. This notice must describe the uses and disclosures of PHI that may be made by the covered entity, the individual's rights, and the covered entity's legal duties with respect to the PHI. The Privacy notices must be provided to individuals (a) no later than the applicable effective date for the privacy regulations; (b) on an ongoing basis after the compliance date, at the time of an individual's enrollment in the plan; and (c) within 60 days after a material change to the notice. In addition, plans must provide a notice of availability of the privacy notice at least once every three years.

If you sponsor more than one health plan, you can likely send out one Privacy Notice for all the plans you sponsor if the information that is required to be in the Privacy Notice for each plan is addressed therein.

<u>What are the Administrative Safeguards</u>

A plan must implement the following administrative safeguard requirements to protect the confidentiality of PHI:

- Designate a privacy official responsible for the development and implementation of policies and procedures.

- Designate a contact person or office for receiving complaints and providing additional information concerning the privacy notice. This may be but is not required to be the same person as the privacy officer.

- Train all employees who will have access to PHI on privacy policies and procedures.

- Establish appropriate administrative safeguards (both technical and physical) to protect PHI from accidentally being used or disclosed in violation of HIPAA's requirements. For example, all PHI should be kept in locked file cabinets and computer systems should have adequate firewalls to protect electronically stored PHI.

- Create a process for individuals to lodge complaints and a system for handling such complaints and recording their resolution.

- Design a system of written disciplinary policies and sanctions for workforce members who violate the privacy rules.

- Mitigate, to the extent possible, any harmful effect that is known to the covered entity resulting from an improper use or disclosure of PHI.

- Refrain from taking retaliatory action against any individuals who exercise their rights under HIPAA.

- Do not require an individual to waive their rights under HIPAA.

- Implement polices and procedures designed to comply with HIPAA and have a written manual of such policies and procedures.

III. Implications of HIPAA's Privacy Rules on Health Plan Sponsors (including sponsors of Health FSAs and HRAs)

Although plan sponsors are not covered entities under the Privacy Rules, plan sponsors will generally be responsible for ensuring that the health plan satisfies its obligations under HIPAA (as described above). In addition, the Plan sponsor must certify that it has implemented certain safeguards to protect PHI in order for it to have access to most PHP. However, the extent of the Plan sponsor's obligations depends on the extent to which the plan sponsor has access to PHI from the health plan. Many plan sponsors may be able to take a "hands off" approach and avoid many of the obligations required by the Privacy Rules. We discuss below the obligations of a "Hands Off" plan sponsor and a "Hands On" plan sponsor.

What is "Hands Off" Plan Sponsor?

What does it mean to be a plan sponsor who is "hands-off" PHI? First, you have to be the sponsor of a fully insured health plan. It does not appear that a self-insured plan sponsor will be able to take a "hands off" approach. NOTE: Your Health FSA and/or HRA is NOT fully insured.

Second, if you take the "hands off" approach, the insurer cannot disclose any PHI to you except

PHI used for enrollment and disenrollment functions. In addition, you may receive summary health information for ERISA "plan settlor functions" such as amending or terminating the plan, or obtaining bids for a new contract (these activities are discussed in more detail below). Summary health information is information that summarizes the claims history, experience and types of claims for participants in the health plan and has had all 18 specific identifiers removed such as names, dates, addresses and social security numbers.

Although "hands-off" PHI plan sponsors are not allowed to access PHI, they may engage in the following plan sponsor activities without becoming subject to the HIPAA compliance requirements:

a. *Provide employees with assistance in claim disputes or in understanding their plan.* Plan sponsors may assist group health plan participants in benefit disputes or appeals or provide employees with assistance in understanding their health plan. When advocating on behalf of an individual, the plan sponsor must obtain the individual's authorization in order to have access to that individual's PHI. Obtaining authorizations and assisting with benefits in this manner does not turn a plan sponsor into a covered entity.

b. *Receive summary health information.* A plan sponsor may receive summary health information from an insurer for the limited purposes of obtaining premium bids or modifying, amending, or terminating the plan without exposing itself to the rest of HIPAA's privacy requirements. The plan's notice of privacy practices (which should be provided by the insurer) should inform participants that the plan may disclose this type of information to the plan sponsor.

c. *Perform enrollment and disenrollment activities and payroll deductions.* Plan sponsors may receive PHI for the purposes of performing enrollment and disenrollment functions without having to comply with the plan document and firewall requirements otherwise required when a group health plan shares PHI with a plan sponsor (as discussed below). A group health plan that is fully insured, and "hands-off" PHI, may directly obtain information about enrollment and disenrollment without subjecting itself to the more onerous administrative requirements. Note: This seems to imply that enrollment and disenrollment information is subject to a lesser standard due to the fact that the plan can release such information to the plan sponsor without the protection of any safeguard implemented by the plan sponsor.

The advantage of being an employer who is taking a "hands-off" PHI approach is that you avoid the following compliance obligations:

- Providing individuals with access to PHI, the right to amend PHI, and receive an accounting of PHI (as described in Section III below).
- Preparing and providing a privacy notice.
- Complying with the administrative safeguards applicable to the Health Plan.

These requirements will be imposed upon the insurer who has issued the insurance contract providing benefits under the health plan. Such plans must, however, refrain from retaliating against health plan participants who exercise their privacy rights and from requiring individuals to waive their rights.

As an important reminder, plan sponsors that wish to avoid the privacy rules must be careful that they do not become so involved in plan administration that they obtain PHI in violation of the privacy rule.

What is a "Hands-On" Plan Sponsor?

A "hands-on" plan sponsor is a plan sponsor of either a fully insured or self-insured health plan that has access to PHI in addition to enrollment/disenrollment information and summary health information. You will be a "hands-on" PHI plan sponsor if you want PHI (beyond summary health information) in order to obtain quotes from insurance carriers or perform plan administrative functions such as quality assurance, claims processing, auditing, and monitoring. However, additional requirements apply to both the plan and you as plan sponsor. Remember that not even "hands-on" PHI plan sponsors may use PHI for employment-related functions or functions in connection with other benefits. Disclosure for those types of uses still requires an individual authorization.

As a "Hands-On Plan Sponsor" you will need to make sure the plan does the following:

- Provide individuals with rights to review, amend, and receive an accounting of their PHI (See "Implications for Self-Insured Plan Sponsors" above for more information).

- Prepare a privacy notice, except that some fully insured plans would only need to provide the notice to participants upon request.

- Comply with the administrative safeguards described above.

In addition, the plan sponsor must amend the health plan (and thereby agree to implement certain administrative safeguards) as follows:

- Describe the employees (or class of employees) or other persons under control of the plan sponsor who may be given access to PHI (access to PHI by plan sponsor personnel should be limited to only those employees who must have it to perform plan administrative functions (i.e., must erect a firewall around employees performing plan administrative functions).

- Restrict access to and use by such individuals to plan administration functions that the plan sponsor performs for the health plans.

- Provide a procedure for resolving any issues of non-compliance by such individuals.

- Describe the permitted and required uses and disclosures of PHI by the plan sponsor.

- Specify that disclosure is permitted only upon written certification that the plan documents have been amended to include specific restrictions and that the plan sponsor agrees to those restrictions.

- Do not use PHI for employment related purposes or non-health plan purposes.

Recap of Plan Sponsor Obligations

The following chart summarizes the obligations of health plans and their sponsors in various scenarios.

Level of Plan Sponsor Involvement with PHI	**Privacy Requirements that Apply to Fully Insured Plan Sponsor and Plan**	**PHI that May Be Disclosed by Plan (or Insurer) to Plan Sponsor**
Hands-Off PHI	No requirements apply to the plan or the plan sponsor, except prohibition on retaliating against employees for exercising their privacy rights and requiring employees to waive their privacy rights.	None; Plan sponsor may have access to de-identified health information and to health information through its own enrollment activities.
Hands-off PHI, plus limited access to summary health information for obtaining bids and amending or terminating the plan.	No requirements apply to the plan or the plan sponsor, except prohibition on retaliating against employees for exercising their privacy rights and requiring employees to waive their privacy rights.	Summary health information only; plus plan sponsor may have access to de-identified health information and to health information through its own enrollment activities.
PHI shared with plan sponsor for "plan administrative functions."	Administrative requirements (including individual rights and administrative safeguards) apply to the plan; limited requirement to maintain and furnish privacy notice applies to the plan. Plan document and firewall requirements apply to plan sponsor.	As described in the plan document; limited to the minimum information necessary to perform the functions described in the plan document.

Breach Notice Requirements

HIPAA defines a "breach" under the Privacy Rule as i) the acquisition, access, use or disclosure ii) of protected health information iii) that is not permitted under the HIPAA Privacy Rule and iv) compromises the security or privacy of the protected health information. There are several steps that covered entities must follow to determine if there has been a breach. If a breach has occurred, various notice requirements are triggered. Keep in mind that there are specific requirements about the content of the notice and the method of notification that must take place. In addition, the clock begins to run as soon as a breach is known (or, by exercising reasonable diligence, would have been known) to any member of the workforce or any agent.

Covered entities must notify affected individuals within 60 days of a breach; if the contact information for the individuals is out of date, the entity must provide substitute individual notice

(either by posting on its web site or in major media). For breaches of unsecured PHI involving 500 or more individuals, entities must also notify the Secretary of HHS. For breaches of unsecured PHI involving fewer than 500 individuals, a covered entity must maintain documentation and notify HHS by 60 days after the end of the calendar year. In addition, if more than 500 individuals in one state or jurisdiction are affected by a breach, the covered entity must provide notice to prominent media outlets in the area within 60 days. Finally, if a breach occurs at or by a business associate, the business associate must notify the covered entity within 60 days.

IV. Enforcement and Penalties

Civil Penalties

HIPAA, as amended by the HITECH Act, establishes a civil money penalty (CMP) structure in which potential CMPs increase with the severity of the violation. HHS has further defined that CMP structure through amendments to the HIPAA Enforcement Rule. These regulations provide a tiered civil penalties structure based on the level of knowledge possessed by the covered entity or business associate, as follows:

- Did not know. Violations for which it is established that the covered entity/business associate did not know and, by exercising "reasonable diligence" ("the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances," 45 CFR § 160.401), would not have known that it violated an administrative simplification provision: $100 - $50,000 per violation, capped at $1.5 million for all such violations of an identical provision in a calendar year.

- Reasonable cause. Violation for which it is established that the violation was due to "reasonable cause" ("circumstances that would make it unreasonable for the covered entity, despite the exercise of ordinary business care and prudence, to comply with the administrative simplification provision violated," 45 CFR § 160.401) and not "willful neglect" ("conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated," 45 CFR § 160.401): $1,000 - $50,000 per violation, capped at $1.5 million for all such violations of an identical provision in a calendar year.

- Willful neglect – corrected. Violation for which it is established that the violation was due to willful neglect and was corrected within the 30-day period beginning on the first date the covered entity knew, or, by exercising reasonable diligence, would have known, that the violation occurred: $10,000 - $50,000 per violation, capped at $1.5 million for all such violations of an identical provision in a calendar year.

- Willful neglect – not corrected. Violation for which it is established that the violation was due to willful neglect and was not corrected within the 30-day period beginning on the first date the covered entity knew, or, by exercising reasonable diligence, would have known that the violation occurred: $50,000 per violation, capped at $1.5 million for all such violations of an identical provision in a calendar year.

In addition, the HITECH Act authorized State attorneys general to file suit on behalf of residents of that State, with damages of up to $100 per violation/$25,000 cap for identical violation, and can also recover costs and attorney's fees.

Under the HITECH Act, HHS is required to provide for periodic audits to ensure that covered entities and business associates comply with the HIPAA Privacy Rule, the HIPAA Security Rule, and the HITECH Act. HITECH Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, Pub. L. No 111-5 (Feb. 17, 2009), at § 13411. In June 2011, HHS awarded two contracts in connection with this requirement. One, issued to Booz Allen Hamilton on June 9, 2011, is entitled "OCR HIPAA Audit Candidate Identification" and is presumably to identify potential covered entities and business associates which should be the subject of such audits. The second, issued to KPMG on June 10, 2011, is entitled "OCR HIPAA Audit Protocol and Program Performance." Under the contract, under OCR's supervision, KPMG is required to develop a protocol for such audits and then carry out approximately 150 audits by the end of the contract period (December 31, 2012). The audit would involve a site visit (with interviews of the entity's leadership; examination of physical features and operations; consistency of process to policy; and observation of compliance with regulatory requirements) and an audit report (including, among other things, best practices observed and specific recommendations for actions the audited entity can take to address identified compliance problems through a corrective action plan).

Criminal Penalties

As amended by the HITECH Act, Social Security Act § 1177, 42 U.S.C. § 1320d-6, provides criminal penalties for the wrongful acquisition or disclosure of individually identifiable health information.

Under the provisions, a person who knowingly and in violation of the HIPAA Administration Simplification provisions

- uses or causes to be used a unique health identifier;
- obtains individually identifiable health information relating to an individual; or
- discloses individually identifiable health information to another person

is subject to the following potential criminal penalties:

- a fine of not more than $50,00, imprisonment for not more than one year, or both;
- a fine of not more than $100,000, imprisonment for not more than five years, or both, if the offense is committed under false pretenses; or
- a fine of not more than $250,000, imprisonment for not more than ten years, or both, if the offense is committed with the intent to sell, transfer, or use individually identifiable health information for commercial advantage.

The HITECH Act added the clarification that, for purposes of the provision, a person (including an employee or other individual) is considered to have obtained or disclosed individually identifiable health information in violation of the HIPAA Administrative Simplification provisions if the information is maintained by a covered entity and the individual obtained or disclosed the information without authorization.

Summary of HIPAA Security Rules

I. Introduction

HIPAA's security rule requires "covered entities" (e.g. health plans and health care providers) that maintain or transmit electronic protected health information ("PHI") to maintain reasonable and appropriate safeguards to ensure the integrity and confidentiality of health information, to protect against threats to security or unauthorized uses or disclosures of information, and to otherwise ensure their officers' and employees' compliance with the security standards.

The Security Rules were designed to be technology neutral and scalable to take into account both large and small plans. The HIPAA Security Rules provide guidelines or "standards" for all types of covered entities while affording flexibility regarding the manner in which each standard is implemented.

To what do the Security Rules apply?

The HIPAA security requirements only apply to PHI in electronic form, which is a subset of health information. HHS clarified that electronic PHI includes individually identifiable health information that is transmitted by electronic media, maintained in electronic media or maintained in any other form or medium. Importantly, electronic media is now defined by the Final Security Regulations 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; and (2) transmission media used to exchange information already in electronic storage media, for example extranet, leased lines, dial-up lines, private networks; and the physical movement of removable/transportable electronic storage media. HHS also clarified 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, not subject to the HIPAA Security safeguards. *Note that this exception for paper faxes applies even if the receiver of the transmission receives the fax via computer.*

What is the role of employer/plan sponsors and service providers?

Employers are not normally "covered entities" under HIPAA; therefore, the HIPAA Security Rules do not apply directly to employers. Nevertheless, plan sponsors must satisfy certain security requirements in order to receive electronic PHI from their health plans. Also, most plans are "legal fictions" that have no employees of their own. Consequently, it is up to the plan sponsor to ensure that all of the plan's requirements have been satisfied.

Likewise, third party administrators ("TPA") and other service providers who perform services on behalf of the plan are not "covered entities" under HIPAA; therefore, much like employer/plan sponsors, the HIPAA Security Rules do not apply directly to TPAs. TPAs and other service providers that assist covered entities in connection with their covered health care functions (known as "business associates") will be required by contract to comply with a number of the same HIPAA Security Rules that apply to the covered entity. That contract is typically called a "Business Associate Agreement". As noted above, you are required to enter into a Business Associate Agreement with your TPAs and other service providers as part of the HIPAA Privacy requirements.

A threshold inquiry that should be addressed is whether the plan sponsor or its business associates have any access to electronic PHI. If the only access to electronic PHI consists of enrollment/disenrollment and summary health information (SHI) disclosed by an insurer, the security requirements do not apply to the plan sponsor (and likewise, would not apply to the TPA or other service provider who assists the employer with enrollment/disenrollment functions).

What are the penalties/consequences of failing to comply?

The Centers for Medicare and Medicaid Services (CMS) is responsible for enforcement of HIPAA's Security Rules and CMS indicates that enforcement will be primarily complaint driven (although it may conduct compliance reviews). The fines for failure to comply with the Security Rules can be up to $100 per violation and the total fine for violating an identical requirement can be up to $25,000. Criminal fines and imprisonment may apply if an individual knowingly obtains or discloses PHI in violation of the Security Rules.

II. What are the Security Requirements?

The HIPAA Security Rules establish a number of "standards" relating to security of electronic PHI. Covered entities are required to comply with all of the standards set forth in the Security Rules (described in more detail below) but the standards are designed to be flexible.

Implementation specifications have been established for each standard. The HIPAA Security Rules contain both "required" and "addressable" implementation specifications and specify whether a standard is required ("R") or addressable ("A") in a Security Standards Matrix (attached as an appendix to the Final Regulations). CMS has also provided a chart of the implementation specifications identifies each specification as "required" or "addressable". You may find a copy of this chart at http://www.cms.hhs.gov/hipaa/hipaa2/education/Physical%20Safeguards%20final.pdf. Of course, required implementation specifications must be adopted by the covered entity. However, covered entities may decide whether an addressable implementation specification is a reasonable and appropriate security measure. The covered entity must undertake a risk analysis to evaluate if the measure needs to be incorporated or whether existing security measures are adequate. In connection with its risk analysis, the covered entity may choose to implement: (1) the addressable implementation specification, (2) one or more alternative security measures, (3) a combination of both, or (4) not implement either an addressable or alternative security measure. Importantly, the covered entity must document *in writing* its final decision, the rationale behind its decision and how the standard is being met. Cost can be a factor in this decision, but HHS stressed that notwithstanding cost considerations adequate security measures must be implemented. In order to comply with these documentation requirements, covered entities should take detailed minutes at any meeting where implementation is discussed and maintain these minutes as part of its documented security procedures.

While every plan sponsor must review its own operations, the following "practical pointers" should provide a point of departure. The HIPAA Security Rules divide the standards into four broad categories:

i) Administrative Safeguards (e.g., what risk assessment, personnel, and training safeguards should be implemented),
ii) Physical Safeguards (e.g., what level of facility protection is reasonable and appropriate),
iii) Technical Safeguards (e.g., what protection(s) are appropriate for electronic data), and
iv) Organizational Requirements (e.g. amend plan documents, review business associate agreements for compliance with the security regulations).

We address each of these requirements in turn and assess how they apply to covered entities and plan sponsors.

III. Administrative Safeguards

Security Management

As part of the privacy process, plan sponsors should have conducted an overall PHI flow analysis to determine what PHI exists, who has access, and what uses and disclosures occur. For security purposes the covered entity must do four things. First it must perform a risk analysis and identify and assess the potential risks and vulnerabilities to electronic protected health information held by the covered entity. Second, it must conduct and implement a risk management analysis to determine appropriate security mechanisms to lessen the risk of improper uses and disclosures and of uses and access by unauthorized users. Third, the covered entity must create a written sanction policy to discipline employees who violate the security standards. Finally, the covered entity must implement a system where it can regularly review its information systems and track user activity through audit logs, access reports and incident tracking reports.

As part of the overall security management process, the HIPAA security team should conduct a risk assessment identifying the potential risks of improper disclosure and vulnerability of electronic PHI maintained or transmitted in the plan's database. This risk assessment should identify potential risks to the confidentiality of electronic PHI stored and transmitted to the plan or its business associates such as unauthorized access by former employees, hackers, and the potential devastating effects of computer viruses and worms. Plan sponsors

are required to document their findings. After the security team conducts the assessment, it must 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 should also 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 health plan, a disaster recovery plan, an emergency mode of operations plan, as well as testing and revision procedures.

As part of their overall risk analysis process, plan sponsors should conduct an assessment of all electronic PHI that they retain and determine whether the data is highly sensitive, less sensitive or not very sensitive. For example, an individual's enrollment data would probably fall in the "not very sensitive" category, while an individual's claims or appeal file might fall in the "highly sensitive" category. Note that this may include PHI above and beyond that required to be maintained as part of the designated record set for Privacy purposes. Examples of common types of electronic PHI are claim appeal and denial letters stored in a computer hard drive or on disk, e-mails from TPAs, pharmacy benefit managers, and between employees in the HIPAA umbrella who perform plan administration functions. Plan sponsors may also maintain electronic PHI through a shared access databases through an Intranet site or a log with an insurer or TPA. Any employees with access to electronic PHI should be identified as well as whether the employees need access to electronic PHI to perform their job functions. (This is also required under the minimum necessary requirements contained in the Privacy Regulations.) Conducting this evaluation will enable plan sponsors to determine which information deserves the greatest attention and dedication of resources. Plan sponsors should evaluate their abilities to review records of information system activity, such as audit logs and access reports.

Assigned Security Responsibility

Plan sponsors should appoint a security official who is responsible for the development and implementation of security polices and procedures. A specific person must be named but this may be the same person as the privacy official required by the HIPAA Privacy Rules. The preamble to the final regulations suggests that the Security Official should be an individual in the workforce who can ensure accountability with the rules. Plan sponsors should begin drafting written policies and procedures for electronic information access controls. These should include implementing appropriate "firewalls" such as assigning unique login names or numbers to each employee with access to electronic PHI, password protection of files containing electronic PHI, automatic computer logoff, procedures to modify employee's access to electronic PHI through network controls, and ways to internally track system activities such as logins, file access and security incidents. In addition, plan sponsors should begin to draft and implement sanction procedures for employees who violate the plan's security policies as well as termination procedures to eliminate access to electronic PHI by former employees and employees who change job functions.

Workforce Security

Plan sponsors should evaluate their operations to determine those employees who should be given authorization to access electronic and/or non-electronic PHI and those that should not have access. For example, do marketing personnel need access to specific claims files? Do all claims personnel need access to all client files? This analysis should be updated on a regular basis to reflect changing roles and responsibilities so that an authorization of access can be revoked or granted as needed. Plan sponsors should consider implementing a checklist that is followed when an employee terminates employment and/or changes roles. This checklist could include (as appropriate) requiring employees to surrender their building access cards, deleting an employee's login and pass code to various systems that house PHI, and requiring employees to delete any PHI from personal computers that are kept at home. NOTE: The HIPAA Security Rules apply to members of the workforce who from outside locations, such as the employee's home.

Information Access Management

For electronic PHI, entities should identify all systems in which such data is maintained and implement appropriate policies and procedures for granting access to PHI such as requiring passwords and user IDs. If documents containing PHI are maintained on a shared drive to which all employees within an organization have access, consider limiting access to such documents to those employees who are permitted to have such access. For PHI in non-electronic forms, entities should give serious consideration to locking the mechanisms in which highly sensitive PHI is stored so that access can be limited to employees who are authorized to have such access.

Security Awareness and Training

Plan sponsors are required to train all employees with access to PHI, including management or supervisory employees, regarding security provisions for the protection of electronic PHI. This should involve awareness training, periodic security reminders, user education concerning virus protection or malicious software such as worms, importance of monitoring login success and failure, and user education regarding passwords. The preamble to the Final Security Regulations provides 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. Plan sponsors should evaluate the strengths of their computer virus protection devices and consider updating their systems with devices that permit monitoring of log-in attempts and reminders to employees to regularly change their passwords. If on-line access is granted to participants, steps should be taken to ensure adequate firewalls are in place.

Security Incident Procedures and Contingency Plan

Plan sponsors must implement procedures to address security incidents and have policies and procedures to respond to an emergency or other occurrence, such as fire, vandalism or system failure. This would include data back up (see below) and recovery, and having an emergency mode operation plan. Further, plan sponsors should evaluate the contingency plans of their TPAs and subcontractors to make sure they are taking appropriate steps to protect data they maintain or store on their behalf.

Evaluation

Plan sponsors should periodically evaluate the status of their safeguards in response to environmental or operational changes affecting the security of their PHI.

Amend Business Associate Contracts

The HIPAA Security Rules require security protections to be added to business associate agreements. Specifically, the agreement must provide that the business associate will: (1) implement safeguards to protect electronic PHI it creates, receives, maintains or transmits on behalf of the health plan; (2) ensure that any agent or subcontractor to whom it provides the health plan's electronic PHI agrees to implement safeguards to protect the PHI; (3) report to the covered entity any security incidents of which it becomes aware; and (4) authorize termination of the agreement by the health plan, if the health plan determines that the business associate has violated material terms of the agreement. As with the Privacy Rule, a plan will generally not be responsible for security breaches by business associates unless it had knowledge of the breach and failed to take corrective action.

IV. Physical Safeguards

Facility Access Controls

Plan sponsors should implement procedures to ensure that access to their facilities (i.e. physical premises where electronic PHI is located) is limited to employees and authorized contractors. Further, areas within the facility in which PHI is stored (e.g. where the benefits department resides) might have additional physical access controls.

Workstation Use and Workstation Security

Plan sponsors should evaluate the placement of workstations (including laptops) on which PHI will be processed and how such workstations may be accessed. Employees should be required to log off or lock their workstations before leaving them unattended. Automatic log-off procedures should be considered as well.

Device and Media Controls

Plan sponsors must implement procedures to destroy electronic PHI after the appropriate retention period has passed (generally 6 years after last use or, if longer, the ERISA retention period). Further, plan sponsors should ensure that electronic PHI is removed from computers and/or electronic media before they are available for reuse, and ensure that the appropriate levels of backups of electronic PHI is maintained.

V. Technical Safeguards

Access Controls

To ensure that only employees who are authorized to access electronic PHI have such access, plan sponsors must implement unique user logins and passwords. Plan sponsors should also consider installing automatic logoff devices on their systems so that the workstation will lock after 10-15 minutes of inactivity. Moreover, the access controls should extend to employees who work at home or at an offsite location.

Audit Controls

Plan sponsors should implement hardware or software that can record and examine activity in their information systems that contain electronic PHI. By implementing a card check-out system, plan sponsors can record those that access non-electronic PHI as well.

Integrity

Plan sponsors should implement electronic mechanisms to corroborate that electronic PHI has not been altered in an unauthorized manner. Examples provided by HHS include error-correcting memory and magnetic disk storage.

Person or Entity Authentication

Prior to releasing electronic PHI to a person or entity seeking access to it (such as over an enrollment website), the plan sponsor must be sure that the person seeking it is the one claimed. Plan sponsors should implement procedures such as checking identification and credentials or requiring passwords. Consideration should be given to what (if any) information will be given to an employee/plan participant about a spouse (e.g., to facilitate payment) and whether to release information to a spouse.

Transmission Security

Plan Sponsors should begin implementing security mechanisms to verify that electronic PHI has not been altered or destroyed while being transmitted to or from the health plan, implement technical security measures to guard against unauthorized access to electronic PHI that is being transmitted by the plan sponsor or health plan over an electronic communications network such as the Internet. Plan sponsors should assess their ability to encrypt electronic PHI when it is sent via email or over the internet. Although encryption has been made an "addressable" specification as opposed to a "required" specification, it is likely a good business practice to routinely encrypt internal and external emails. Commercially available software (e.g., PGP and/or Lotus Notes) may help facilitate internal (e.g., Lotus Notes) and external (e.g., PGP) encryption.

With respect to non-electronic PHI, plan sponsors might require that the sender of a facsimile containing PHI contact the recipient prior to sending the facsimile to ensure that the material is instantly retrieved by its intended recipient.

VI. Organizational Requirements

Assemble Security Team and Learn the Security Rules

The plan sponsor should assemble an internal HIPAA Security Team and create a compliance agenda. Members of the Security Team should include delegates from information technology department, human resources, benefits, accounting, and legal departments. Team members should also be educated on the HIPAA security, privacy and EDI requirements, a security budget should be established and an internal timeline and meeting schedule should be set.

Amend Health Plan Document

If plan sponsors have access to electronic PHI (above and beyond summary health information and enrollment data) they must amend the plan documents to provide that they will safeguard electronic PHI in accordance with the security rules.

VII. Enforcement and Penalties?

See IV. Enforcement and Penalties under the HIPAA Privacy Rules overview above.