HIPAA PRIVACY FOR EMPLOYERS
A Comprehensive Introduction

HIPAA Privacy Regulations-General

The final HIPAA Privacy regulation was released on December 20, 2000 and was effective for compliance on April 14, 2001. The final rule offers the first comprehensive federal protection for the privacy of health information. The Office of Civil Rights will enforce the regulation. The federal privacy regulations are considered a "floor" of privacy standards and may be superceded by more stringent state privacy regulations. The Privacy rule regulates the use and disclosure of protected health information. Employers who offer or conduct certain benefits or services may be required to comply.

This summary document and the attachments has been written to provide employers and plan sponsors with a detailed overview of the Privacy Regulations under HIPAA and assist them in identifying potential areas of review and action. The full text of the Privacy Regulations can be found at **http://aspe.os.dhhs.gov/admnsimp.**

This document and the attached exemplar material should be considered as informational only and is not meant to convey legal advice or counsel. Employers and group health plan sponsors should involve their legal counsel to advise and assist them in determining what they must do to meet their specific obligations under the HIPAA Privacy Rule.

SECTION ONE: KEY COMPONENTS OF THE PRIVACY RULE

CONSUMER CONTROL OVER PROTECTED HEALTH INFORMATION

The HIPAA Privacy Rule gives patients and members significant rights in both understanding and controlling how their health information is used. All individually identifiable health information that is maintained or communicated in any form (electronic, paper or oral) by a Covered Entity is considered to be PHI.

More specifically:

- Covered entities must provide Notices of Privacy Practices to patients/members that provide clear, written explanations of how the covered entity can use, maintain, and disclose their health information
- Patients/members must be allowed access to their medical records upon request and must be allowed to request and obtain copies of their records.
- Patients/members may request amendments to the information in their medical records if they think it is incorrect.
- Patients/members may request a documented accounting of certain disclosures of their protected health information by the covered entity.
- Providers are not required to obtain Consent from their patients before disclosing medical information to third parties but they can if they choose to do so. They are required to make their patients aware of how they protect their patients' health information by giving their patients a copy of their Notice of Privacy Practices and making a god faith effort to obtain a written acknowledgement from the patient that it was received.
- Specific patient/member authorization must be obtained prior to the release of protected health information for purposes other than treatment, payment or health care operations or for certain other purposes permitted by the Privacy Rule (oversight of the health care system, public health, law enforcement, judicial and legal proceedings, etc.).
- Patients/members have the right to request restrictions on the uses and disclosures of their PHI and to request confidential communication of their protected health information.

LIMITATIONS ON THE USE AND RELEASE OF PROTECTED HEALTH INFORMATION

With few exceptions, an individual’s protected health information can be used for health care related purposes only (treatment, payment, and healthcare operations). More specifically:

- Protected health information cannot be used by employers to make employment or personnel decisions
- Uses and disclosures of protected health information must be limited to the minimum amount of information necessary to accomplish the purpose of the use or disclosure.

- Authorizations for disclosure other than for treatment, payment and health care operations must provide for informed and voluntary authorizations in clear and understandable language.

IMPLEMENTATION REQUIREMENTS

The Privacy regulations leave the format and content of the detailed policies and procedures for meeting the standards to the discretion of each covered entity thus allowing for flexibility and scalability. In general, covered entities must:

- Adopt written privacy policies and procedures that define access to protected health information, the use of protected health information by the covered entity and the process for disclosure of protected health information.
- Take steps to ensure that their business associates adequately provide for the confidentiality and privacy of protected health information.
- Train their employees on the basic provisions of the Privacy regulations and the organization's Privacy Policies and Procedures.
- Establish sanctions for employees that violate the Privacy policies and procedures.
- Designate a Privacy Official to be responsible for ensuring the organization's Privacy procedures are followed.
- Establish procedures that provide a means for patients/members to make inquiries or register complaints regarding the privacy of their records.
- Establish procedures that provide a means for patients/members to access, make copies of and request amendments to their records.
- Provide a Notice of Privacy Practices to their patients/members.

ACCOUNTABILITY AND ENFORCEMENT

Covered Entities that violate the Privacy regulations are subject to penalties under HIPAA as indicated below. Enforcement will be through the DHHS Office of Civil Rights.

- Civil penalties are $100 per incident, up to $25,000 per violation per year per standard.
- Federal criminal penalties exist for covered entities that knowingly and improperly disclose information or obtain information under false pretenses. Criminal penalties include fines up to $50,000 and one year in prison for improperly obtaining or disclosing protected health information; up to $100,000 and up to five years in prison for obtaining protected health information under "false pretenses"; and up to $250,000 and up to 10 years in prison for obtaining or disclosing protected health information with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm.
- There is no statutory authority for a private right of action for individuals to enforce their privacy rights.

OTHER PERMITTED DISCLOSURES

The Privacy Regulations permit certain disclosures of health information without individual authorization for the certain national priority activities and for activities that allow the health care system to operate more smoothly. These activities include:

- Oversight of the health care system, including quality assurance activities
- Public Health, reporting of disease and vital statistics
- Research, generally limited to when a waiver of authorization is independently approved by a Privacy Board or Institutional Review Board
- Judicial and administrative proceedings
- Limited law enforcement activities
- Emergency circumstances
- Identification of a deceased person or to determine the cause of death
- Inclusion in facility patient directories
- Activities related to national defense and security

SECTION TWO: EMPLOYERS AND GROUP HEALTH PLANS

The final Privacy Regulation is applicable to covered entities, which are defined as health plans, health care clearinghouses and those health care providers who conduct certain financial and administrative transactions electronically. Employers or Plan Sponsors who provide health plans are NOT covered entities but the Group Health Plans they establish for their employees are Covered Entities. Group Health Plans are "Covered Entities" under HIPAA and are defined as "*an individual or group plan that provides, or pays the cost of, medical care*". In addition to the traditional insurance plans, this definition includes the following:

- Group Health Plan - an employee welfare benefit plan including insured and self-funded plans established by the Plan Sponsor that provides for medical care benefits and that either has 50 or more participants or is administered by another business entity. The benefits can be fully insured by a health insurance carrier or administered by an external nonaffiliated third party (such as a third party administrator).
- Employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers
- Any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care
- An insurer, but only when actually providing group health insurance and not simply acting as a third party administrator
- An HMO

WHAT DOES HIPAA PRIVACY MEAN TO GROUP HEALTH PLANS?

The HIPAA Privacy Regulations will significantly affect Group Health Plans. The degree of this impact will greatly depend on whether the Group Health Plan is fully-insured or self-funded for their health care benefits. Another variable affecting the impact of HIPAA compliance on groups is the amount of PHI that the Group Health Plan elects to receive.

What Does Non-Compliance Mean?

Group Health Plans should be aware that non-compliance with the Regulation could mean both civil and criminal penalties (please refer to the previous section on accountability for details on the potential penalties for non-compliance). With these types of consequences at stake, Group Health Plans must familiarize themselves with the Privacy Regulation and how they can become compliant.

Are Groups Subject to the HIPAA Privacy Regulation?

Most Group Health Plans health plans (with the exception of self-administered Group Health Plans with less than 50 participants and certain government-funded plans) are Covered Entities as defined by the Privacy Regulation. There is no distinction in the definition of Group Health Plan between insured groups and self-funded groups. Therefore, Group Health Plans are subject to the Privacy Regulation. However, there are exceptions in the Regulations that allow groups, under certain circumstances, to both limit their exposure to the penalties for non-compliance mentioned above and reduce the level of effort needed to comply.

Strategy for Compliance

The first step is for the Group Health Plan to determine its insurance status as either fully-insured or self-funded. While there is no distinction in the definition of Group Health Plan between insured and self-funded groups, there is a difference in what a group must do to comply based on its insured status.

The next step is to determine how important it is for the Group Health Plan to receive protected health information (PHI). The following information will assist each Group Health Plan in analyzing what they need to do to comply with the Privacy Regulations.

FULLY-INSURED GROUPS

Fully-insured groups that have access to PHI (other than enrollment/disenrollment and eligibility data and Summary Health Information) must fully comply with all the following provisions of the Privacy Regulations:

- Develop and implement Privacy Policies & Procedures
- Furnish a Notice of Privacy Practices to their members (Sample Notices are included in Attachment 1. These sample Notices are provided as examples only and should not be used without consulting with legal counsel.)
- Appoint a Privacy Official and establish a contact office
- Train employees on their privacy policies and procedures and establish sanctions for violations.
- Implement data privacy and security safeguards
- Develop a mitigation plan in the event of Privacy breaches

- Establish a complaint process for members
- Allow for access, copying and requests for amendment of health information
- Provide members for an accounting of disclosures upon request
- Retain compliance documentation for six years

Important Exception: If a fully-insured Group Health Plan elects to only receive summary health information, it will fall under the insurer's HIPAA Privacy umbrella. Summary Health Information is PHI that summarizes claims history, claims expenses or type of claims experience by enrollees for whom the Plan Sponsor has provided benefits under the Group Health Plan and is stripped of all individual identifiers but is not necessarily fully de-identified as defined by the Privacy Regulation. The level of effort required to comply with the Privacy Regulations is significantly reduced as indicated below:

- No HIPAA specific Privacy Policies and Procedures required
- No Notice of Privacy Practices to distribute or maintain
- No requirement to appoint a Privacy Official and establish a contact office
- No employee Privacy training or sanctions required
- No HIPAA specific data privacy and security safeguards required
- No HIPAA specific complaint process required
- No requirement to allow members to access, copy or request to amend their health information
- No requirement to provide enrollees with an accounting of disclosures
- Must only retain any plan document amendments for six years.

If fully-insured Group Health Plans elect not to receive PHI, and elect instead to receive only Summary Health Information, they should formally document this decision and modify any of their existing practices that involve greater use of PHI.

SELF-INSURED GROUP HEALTH PLANS

Fully and partially self-Insured Group health Plans are not granted the same exceptions for compliance with the HIPAA Privacy Regulations as those available to fully-insured Group Health Plans. This means that the self-funded Group Health Plan must fully comply with all provisions of the Privacy Regulations that were outlined above for fully-insured groups that elect to receive PHI. However, even though they must comply with all provisions of the Regulations as outlined above, self-funded Group Health Plans may be able to reduce the actual amount of administrative work they must do by limiting the amount of PHI that their employees use or disclose.

A self-funded Group Health Plan can do this by hiring a third party administrator to administer their health plan and electing to only receive enrollment or eligibility data and Summary Health Information. Because many of the administrative requirements of the Regulations can be included in a Business Associate contract between the Group Health Plan and the third party administrator (provide access & amendment, account for disclosures, safeguard the PHI, provide access to books & records, etc.), the

administrative burden for such a group to comply with the regulations are less than if the group receives PHI on individual members and the treatment they receive.

GROUP HEALTH PLANS AND THEIR BUSINESS ASSOCIATES

When Group Health Plans have taken the necessary steps to become HIPAA compliant based on their fully-insured or self-funded status as well as the amount of PHI they elect to receive or create, they must then ensure that their Business Associates are HIPAA compliant as well. A Business Associates is an external nonaffiliated third party that the Covered Entity contracts with to perform a covered function(s) on its behalf involving the use or disclosure of PHI. For example, an insurer that provides third party administration for a self-funded plan is the Business Associate of the self-funded plan.

Group Health Plans that share PHI with their Business Associates must obtain "satisfactory assurance" that their Business Associates will safeguard their enrollees' PHI. This is accomplished by executing a written contract or contract amendment with its Business Associates which contractually obligates the Business Associates to protect the PHI they create, use or disclose. Therefore, the Business Associate contracts must specify that the Business Associate:

- Must use and disclose PHI only as permitted by the contract with the Group Health Plan and consistent with the Privacy Regulations
- Must implement data privacy and security safeguards
- Must ensure any agents or subcontractors they employ to assist in fulfilling their contract obligations to the Group Health Plan adhere to the same restrictions
- Must provide enrollees with access, amendment and disclosure accounting upon request
- Must report improper use or disclosure of PHI to the Group Health Plan
- Must make their books and records available to DHHS upon request
- Must return or destroy PHI at the end of the contract if feasible to do so. If not feasible, the Business Associate must ensure that no improper use or disclosure of PHI occurs.

A sample of a HIPAA compliant Business Associate contract amendment to an ASO contract between a self-funded Group Health Plan and its third party administrator is included as Attachment 2 This document is similar to the Business Associate Amendment that our Company is using to contract with its business associates and contains the applicable provisions of the Privacy Regulations. As with the other sample material furnished throughout this document, this sample contract is not intended to provide legal advice. The Group Health Plan's legal counsel needs to review it should the group health plan decide to use it.

IMPACT OF HIPAA ON DISCLOSURES TO PLAN SPONSORS

The Privacy Regulation has a significant impact on the information that can be made available to a Plan Sponsor. The Plan Sponsor is usually the employer. The Plan Sponsor is the legal entity that establishes and maintains the Group Health Plan. The Plan Sponsor can be an employer, a union, a joint board of trustees or other similar group. Plan Sponsors are not Covered Entities under HIPAA.

More specifically, the Group Health Plan (and the insurer that services it) may not disclose their enrollees' PHI to the employer or plan sponsor. However, the plan sponsor may receive Summary Health Information from the Group Health Plan or the insurer for obtaining bids on the plan's health insurance coverage or for the purpose of modifying, amending or terminating the health plan. As described earlier, Summary Health Information is PHI that summarizes claims history, claims expenses or types of claims experience by enrollees for whom the Plan Sponsor has provided benefits under the Group Health Plan and is stripped of all individual identifiers but is not necessarily fully de-identified as defined by the Privacy Regulation. A sample form for use by Plan Sponsors to request summary health information from the Group Health Plan or insurer is included as Attachment 3. This sample is being provided as information only and does not constitute legal advice. The group's legal counsel should review this document to ensure it is acceptable for use by the Plan Sponsor.

There is an exception to the prohibition of making PHI available to the Plan Sponsor and that is when the Plan Sponsor performs "plan administrative functions" for the Group Health Plan (such as case management, utilization review, claims processing, reimbursement, benefits administration, etc.). If this is the case, the Group Health Plan or insurer may disclose PHI to the Plan Sponsor for such plan administration purposes only if the plan documents are amended to include the following provisions:

- The PHI must be safeguarded per the requirements of the Privacy Regulation.
- The employees of the Plan Sponsor who are given access to the PHI must be described.
- Employee access to and use of PHI must be restricted to the specific plan administrative functions involved.
- No use or disclosure is allowed for the purpose of making employment decisions or in conjunction with the Plan Sponsor's other employee benefit plans.
- All agents and subcontractors must adhere to the same restrictions on use and disclosure of PHI as the Plan Sponsor.
- Enrollees must be provided the right to access, copy, amend and receive an accounting of disclosures upon request.
- The Plan Sponsor's books and records must be made available to DHHS upon request.
- PHI must be returned to the Group Health Plan or insurer when no longer needed or else the Plan Sponsor must ensure that there is no improper use or disclosure of the PHI.
- Procedures must be defined for resolving issues of non-compliance.

Only the minimum amount of PHI necessary to accomplish the plan administrative function(s) to be performed by the Plan Sponsor must be disclosed by the Group Health Plan or insurer. The Group Health Plan or insurer can rely on the Plan Sponsor's certification that the plan documents have been properly amended and they are not required to review the actual documents themselves.

In order to assist Plan Sponsors and employers in fully researching the requirement to amend their Plan Documents, we have included the text of Section 164.504 (f) of the

Privacy Regulation as Attachment 4 to include a sample compliance checklist. This material provides more specific information on the requirement to amend the Plan Documents so Plan Sponsors can receive PHI if they need or elect to do so. Also included is an sample draft of a HIPAA compliant amendment to a plan document (Attachment 5) and an sample draft of a Plan Sponsor certification of amendment (Attachment 6). Again, this material is provided for informational purposes only and is not to be considered as legal advice. Legal counsel should review this material prior to its use to make sure that it adequately addresses the requirements for amending the Plan Documents to ensure compliance under the Privacy Regulations.

SECTION THREE: EMPLOYERS AS PROVIDERS

Many employers provide medical or other health services via on site health clinics as well as wellness programs, disease management programs, employee assistance programs and occupational health and medicine services. All such services or programs meet the definition of health care.

If an employer provides or otherwise furnishes such services, they may also fall under the HIPAA Privacy Regulations as a Provider and should consult with their legal counsel to determine their HIPAA compliance requirements in this capacity.

SECTION FOUR: COMPLIANCE

Employers must become aware of and informed about the HIPAA privacy Regulations and their impact on their organizations and their operational policies and procedures.

SUGGESTED PLAN OF ACTION FOR COMPLIANCE (THE GROUP'S LEGAL COUNSEL SHOULD BE THOROUGHLY INVOLVED IN THIS PROCESS)

- Define the group's status as a Covered Entity.
- Ensure the distinction between the Group Health Plan and the Plan Sponsor is clear.
- Perform a gap analysis (current operation versus what is required by the Privacy Regulation).
- Identify the organization's risk areas (the "gaps").
- Develop a strategy to eliminate the gaps (the compliance plan).
- Implement the strategy - execute the plan.
- Document all compliance efforts. (If it is not documented, it did not happen.)

SECTION 5: HELPFUL REFERENCES

There is a wealth of information being published to keep the health care community informed of what is happening on the HIPAA front. The following helpful HIPAA Web sites are available for assistance with HIPAA implementation:

Public Resources:

-Text Of Administrative Simplification Law And Regulations: http://aspe.os.dhhs.gov/admnsimp
-HIPAA Strategy and Project Plan: http://www.hipaainfo.net
-WEDI Strategic National Implementation Process: http://snip.wedi.org

For More Information:

-Boundary Information Group: http://www.hipaainfo.net
-HIPAA Alert: http://www.hipaadvisory.com

Tools For Organizations:

-WEDI SNIP White Papers: http://snip.wedi.org
-Early View-Tool for HIPAA Self Assessments: http://nchica.org

ATTACHMENTS

1. Sample Group Health Plan Notices of Privacy Practices
2. Sample Template for a Business Associate Agreement
3. Sample Plan Sponsor's Summary Health Information Request
4. Extract of Section 164.504 (f) of the Privacy Regulation to Include a Sample Compliance Checklist
5. Sample Plan Sponsor's Amendment to Plan Documents Required for Access to PHI
6. Sample Plan Sponsor Certification of Amendment to Plan Documents