IMPACT to EMPLOYER / PLAN SPONSOR of HIPAA PRIVACY

As the Plan Sponsor/Employer you must contend with yet another federal requirement on your group health plans: the "Health Insurance Portability and Accountability Act" (HIPAA) privacy rules. The goal of the rules, to ensure that health information about employees and family members is not used for purposes other than health care, is laudable, but the implementing regulations and the flexibility granted to individual States to craft tougher privacy rules will be challenging for you.

One of the first challenges you must confront is a conceptual one. The rules directly regulate group health plans and not you. Given that a group health plan is usually nothing more than a plan document, it is the sponsor of the group health plan, the employer or the trustees, who must comply with the rules along with the companies and individuals who provide services to the group health plan.

Not all the health related information you maintain is subject to the HIPAA privacy rules. The health information you create, receive and maintain when operating in the group health plan capacity is subject to HIPAA privacy. The health information you create, receive and maintain when operating in the employer capacity is not subject to HIPAA privacy, but instead protected under other rules, such as the Americans with Disabilities Act and FMLA.

The regulations refer to health information the employer obtains when operating in the capacity of an employer as employment record information, which is separately maintained from group health plan information. While the regulations do not adopt a definitive definition of employment record, the regulations clarify that medical information needed to carry out an employer's obligations under FMLA, ADA, and similar laws, as well as files or records related to occupational injury, disability insurance eligibility, sick leave requests and justifications, drug screening results, workplace medical surveillance, and fitness-for-duty tests of employees may be considered employment-related and not subject to HIPAA privacy. This would mean that you should not have copies of information relating to the health plan in an employment file.

As your third party administrator, GISC, can help you to achieve the separation of function that HIPAA envisions. The health information GISC creates, receives and maintains is associated with the group health plan and as such is subject to HIPAA privacy. If you request any individually identifiable health information from GISC, HIPAA imposes strict requirements on how that information can be used. If you use the information for anything other than plan administration functions, you must first obtain an authorization from the individual whose information you seek to view. HIPAA imposes detailed requirements on the authorization form that you must use and it requires you to disclose the reason they seek to view the information.

GISC will be frequently reminding you of these requirements and will assist you by acting as a kind of sentinel of the plan information. If GISC questions you about why you want some information, remember that this is to prevent you from violating HIPAA privacy. GISC is acting in your best interest and helping you to avoid heavy monetary penalties. While GISC can be very helpful, the final responsibility always resides with the employer, plan sponsor or plan trustees. Note: In most cases, the purpose for which you request plan information from GISC is for plan administration functions and therefore authorizations will not be required.
Your responsibilities under the HIPAA privacy rule depend on what type of health information is viewed. Is it individually identifiable or is it summary information that is de-identified? If members of your workforce see or hear any individually identifiable information that comes from the plan, you must comply with HIPAA privacy. In most self-funded plans, some members of the workforce receive individually identifiable health information from the plan including but not limited to, check registers, audits, hold lists (funding requests), explanation of benefits, drug reports, 50% reports, etc. GISC has chose to de-identify the majority of this information so that you will not have to be concerned with a violation of HIPAA privacy.

Below is a brief overview of the group health plan requirements. As you will see the requirements are not overly burdensome, but they do require formalizing and documenting policies and procedures, as well as thinking through the flow of medical information in your offices.

**Business Associate Agreement**

When an employer on behalf of a group health plan hires a third party to perform some functions for the plan and those functions require access to employee medical information, the group health plan is required to have a "business associate agreement" with the third party to ensure that the medical information will be protected.

You need to be thinking about the organizations you contract with to provide services to the group health plan. In some cases you will contract directly with utilization review firms, pre-certification companies, brokers, pharmacy benefit management firms and networks. In other cases you will contract with GISC and rely on GISC to subcontract work to these entities. Many of you will have a hybrid approach and directly contract with some vendors, while relying on GISC to subcontract with other vendors.

As the “Covered Entity” you will need to have a "business associate agreement" with GISC as well as any vendor who you contract with directly such as a utilization review firms, pre-certification companies, brokers, pharmacy benefit management firms and networks, etc. If the GISC contracts with these firms on behalf of your group health plan, GISC will have a subcontractor agreement with these firms that flows down the restrictions of the business associate agreements to them. GISC has sent all of you a business associate agreement for you to sign as the “Covered Entity” and for GISC to sign as your business associate. Further, GISC has sent subcontractor agreements to all of the vendors to ensure that they comply with the privacy rules. Note: If you have a direct relationship with a vendor you are responsible to complete a business associate agreement with them this may also apply to your broker and/or consultant.

**Policies and Procedures**

You will need to develop policies and procedures relating to the use, disclosure and access to medical information of employees and family members. The first step in developing policies and procedures is to examine your office operations to determine who has access to this information and how the information is stored. The next step is to create safeguards (administrative, technical and physical) to protect the information from being accessed by individuals who should not be accessing it. The third step is to draft a procedure manual explaining your policies and procedures. The fourth step is to train members of your workforce regarding privacy requirements and document that the training has been provided.
HIPAA requires that you designate a "privacy official" that is responsible for the development and implementation of the privacy policies, as well as designate a contact person who is responsible for receiving complaints about privacy violations.

You will also need to have an avenue for individuals to make complaints concerning the privacy policies and procedures and document all complaints received and how they were handled. You will have to develop appropriate sanctions against members of your workforce who fail to comply with the privacy policies and procedures, as well as document the sanctions that are applied. You will need to take action to mitigate any harmful effect that is known of the improper use or disclosure of medical information.

For most of you the HIPAA privacy requirements will impose some rethinking of your office handling of medical information and will heighten your employees' sensitivity to proper handling of medical information. Once the policies and procedures are in place, HIPAA privacy should become a minimal routine part of standard office operations.

**GISC has placed sample forms for requesting information, etc. on its’ website.**

**Health Plan Document**

The group health plan document must be amended to reflect the new policies and procedures. In addition to explaining how the group health plan will use and disclose individually identifiable health information (referred to below as "protected health information"), the document must include a statement that the plan sponsor agrees to:

A. Not use or further disclose "protected health information" other than as permitted or required by the plan documents or as required by law;
B. Ensure that any agents, including a subcontractor, to whom it provides "protected health information" agree to the same restrictions and conditions that apply to the plan sponsor;
C. Not use or disclose the information for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the plan sponsor;
D. Be vigilant of any use or disclosure of "protected health information" that is inconsistent with the permitted or required uses or disclosures;
E. Make available "protected health information" to individuals;
F. Provide individuals with the opportunity to amend "protected health information;"
G. Provide individuals with an accounting of the disclosure of their "protected health information;"
   H. Make its internal practices, books, and records relating to the use and disclosure of "protected health information" available to the Secretary for compliance purposes;
I. Return or destroy all "protected health information," if feasible;
J. Ensure that adequate separation exists between employees who are authorized to use "protected health information" and those who are not. Describe those employees or classes of employees to be given access to "protected health information." Restrict the access to and use by these employees. Provide an effective mechanism for resolving any issues of noncompliance by persons who have access to "protected health information."

**GISC has prepared this amendment for your plan and it is enclosed for your certification and distribution to covered employees and COBRA participants.**
Privacy Notice

You must distribute a privacy notice to inform individuals about how their medical information is handled and about any rights they may have with respect to their information. In a self-funded group health plan, you as the employer/plan sponsor are required to provide the privacy notice. The privacy regulations set forth very specific elements that must be included in the privacy notice.

A group health plan must provide the privacy notice to individuals covered under the plan no later than the compliance date (April 14, 2003, or April 14, 2004 for small group health plans). Thereafter, the notice must be provided at the time of enrollment to new enrollees, and within 60 days of a material revision to the notice. No less frequently than once every three years, the plan must notify individuals currently covered by the plan of the availability of the notice and how to obtain the notice. GISC has prepared the notice for you and it is enclosed. If you chose to use a different notice, please be sure to forward a copy to GISC for its' files.

Other Important Requirements

You must give individuals the opportunity to agree or object to disclosures to family members. Employee benefit analysts were initially concerned that the rule could be interpreted to require group health plans to obtain an agreement (i.e., signed statements) from non-minor children and spouses before an explanation of benefits statement containing information on a non-minor child or spouse could be sent to the employee. However, discussions with Department of Health and Human Services regulation writers clarified that the intent of the regulations was not to require group health plans to solicit non-minor children and spouses, but rather to require health plans to give these individuals the opportunity to request that the health plan withhold their information from the employee. This means that a covered spouse may request the plan to send explanation of benefits directly to the spouse and not the covered employee. Administratively, this is a substantial difference. Group health plans may be able to satisfy this requirement by simply including some language in their summary plan descriptions.

You must allow individuals to request restrictions on the uses and disclosures of their medical information. You are not required to agree to restrictions. This will give you control over restrictions that you believe are unreasonable and would hinder the routine processing of claims.

You must give individuals the opportunity to inspect or obtain copies of their medical information, with exceptions for psychotherapy notes and information compiled for use in a civil, criminal or administrative action.

You must provide individuals the opportunity to amend their medical information for as long as the employer group health plan maintains it. An employer may deny an individual's request for amendment if it determines that the medical information was not created by the group health plan.

GISC has placed the forms necessary to request the information outlined in this section on its’ website. Please go to www.giscinc.com and click on HIPAA Privacy.

Effective Date

Group health plans must be in compliance no later than April 14, 2003 (small group health plans have until April 14, 2004).
Looking Ahead

The security component of HIPAA is another section of the law that you will have to incorporate into your privacy compliance efforts. The final security regulations have just been released and they provide details on how you are to protect the storage and dissemination of medical information. GISC will keep you informed as to implementation dates, etc.

As mentioned at the outset of this summary, you will need to stay apprised of developing state law with respect to privacy, given that HIPAA does not preempt state privacy laws that are more stringent than the federal requirements.

Conclusion

You will find that the paperwork you currently receive from GISC will change because of the privacy rules. We have de-identified many of the standard reports sent via e-mail, facsimile or US mail so that inappropriate personnel in your office do not see them. You will no longer receive a copy of the prescription drug billing as it contains a multitude of protected health information. GISC realizes that this will change the interaction that you have with us and will work to provide you with what you need in order to perform your health plan functions while protecting the health information of your participants.

Of significance is that when it comes to health care coverage and benefits, you as the sponsor of a self-funded medical benefit plan clearly wears two hats; one as the fiduciary of the plan and one as the employer. The two roles should never be confused. As a fiduciary, you are responsible to discharge your duties solely in the interest of the plan participant. Willful violations of employees right to privacy or confidentiality can result in liability under a civil suit or regulatory action for civil penalties.

As with any governmental compliance requirement which is just being implemented there will be changes to procedures due to both amendments and interpretation of the regulation by its’ authors, GISC will keep you informed.