ABA Section of Taxation
Employee Benefits Subcommittee on COBRA, Welfare Plans and Cafeteria Plans
October 2002

Mark L. Stember
Kilpatrick Stockton LLP
607 - 14th Street, NW, Suite 900
Washington, DC 20005-2018
Phone: 202.508.5802
Fax: 202.585.0018
mstember@kilpatrickstockton.com

Final HIPAA Privacy Regulations Issued – Implications for Employers

On August 14, 2002, the Department of Health and Human Services ("HHS") finalized the much-anticipated amendments (the "Final Amendments") to the HIPAA privacy regulations. For the most part, the Final Amendments track the amendments that were proposed by HHS in March 2002 (the "Proposed Amendments"). The Final Amendments together with the original HIPAA privacy regulations issued in December 2000 now comprise the final HIPAA "Privacy Rule." However, in the Preamble to the Final Amendments, HHS indicated that it is studying various issues surrounding the Privacy Rule and will issue future guidance as necessary to further clarify the Privacy Rule provisions. Such guidance would probably take the form of questions and answers similar to the guidance it issued in July 2001.

The Privacy Rule applies to "covered entities," which are health plans, health care providers and health care clearinghouses. Unless specifically authorized by the individual or otherwise allowed by the Privacy Rule, the Privacy Rule prohibits such covered entities from using or disclosing an individual's protected health information ("PHI"). In order to prevent the non-authorized use or disclosure of PHI, the Privacy Rule imposes numerous requirements on Covered Entities. This Article focuses on certain of the requirements applicable to health plans. The specific requirements applicable to health plans will vary depending upon whether the health plan is self-insured or provides health benefits through a health insurer or HMO. Sponsors of self-insured plans will be required to adopt numerous written policies and procedures regarding the privacy of PHI and distribute a privacy notice to its participants, while sponsors of insured plans will be exempt from most of these requirements (unless the sponsor is receiving PHI). Additionally, plan sponsors who receive PHI from their health plans, whether insured or self-insured, will be required to make changes to their plan documents. This Article discusses the key concepts of the Final Amendments and how they affect the implementation of the Privacy Rule by employers and their health plans.

Extension for Business Associate Agreements. Under the Privacy Rule, health plans and their business associates that receive PHI (*i.e.,* third party administrators, attorneys, actuaries, accountants and other service providers) must enter into a business associate agreement, which addresses various Privacy Rule provisions. The business associate agreement is designed to protect PHI that is used or maintained by a business associate. In the Proposed Amendments, HHS proposed an extended transition period for existing business associate

© 2002 Mark L. Stember

contracts that meet certain requirements. Further, HHS also proposed model language that could be used in amending business associate agreements. In the Final Amendments, HHS adopted the extended transition period for certain business associate contracts and clarified other issues regarding the model language.

Based on the Final Amendments, a health plan may now continue to operate under an existing contract with a business associate if (i) prior to October 15, 2002 the health plan has entered into a written contract with the business associate and (ii) the contract is not renewed or modified between October 15, 2002 and April 14, 2003. A contract that meets these two requirements will be deemed to be in compliance with the Privacy Rule (*i.e.,* no Privacy Rule amendments will be required) until April 14, 2004, or the date such contract is renewed or modified after April 14, 2003, if earlier. HHS has clarified that contract renewals under automatic "evergreen" provisions and contract modifications that occur without any action by the parties do not prevent the contract from otherwise qualifying for the extended transition period. Further, as in the Proposed Amendments, the Final Amendments do not apply the transition period to "small health plans," which already have an extra year to comply with the Privacy Rule (*i.e.,* April 14, 2004 is the compliance date for small health plans).

If an employer does not have an existing written contract in place with a business associate, it may execute a new contract prior to October 15, 2002 to obtain the extension. Such new contract (as well as any existing contract) must at a minimum describe in general terms the functions, activities or services that make the entity a business associate. In addition, the Privacy Rule appears to require that the written contract be between the health plan (as the covered entity) and the business associate. Often such contracts are between the business associate and the employer, and not the health plan. Thus, any new contracts should be executed between the health plan and the business associate. For purposes of existing contracts, it would appear useful to clarify that the employer was acting on behalf of the health plan as the plan's representative when it entered into the current contract. Such clarification could be done by formally amending the contract or executing a separate letter agreement, and in either case should be done before October 15, 2002 to qualify for the extension.

Although the extended transition period allows health plans up to an additional year to amend qualifying contracts with business associates, health plans must still comply with the Privacy Rule provisions during the extended transition period. For example, a health plan must still allow an individual to access and request a copy of his or her PHI, including PHI maintained by a business associate. Therefore, as a practical matter, health plans should confirm in writing that their business associates will comply with the applicable Privacy Rule provisions. To ensure such written confirmation is not considered a "modification" to the business associate contract, this should be accomplished prior to October 15, 2002.

In regard to the model business associate contract provisions, HHS adopted these provisions with few modifications in the Final Amendments. However, HHS did change the title of the provisions from "model provisions" to "sample provisions" to clarify that the provisions are merely sample clauses and are not required to be included in a business associate agreement by the Privacy Rule. In addition, HHS clarified that use of the sample provisions would be considered strong evidence of a covered entity's compliance with the business associate

© 2002 Mark L. Stember

agreement provisions, but would not constitute a "safe harbor." The sample provisions provided by HHS generally should not be used without supplementing and adapting the sample language before it is included in a business associate agreement. The sample language is deficient in a number of key areas that should be addressed with business associates, including indemnification, transfers of PHI upon termination, and audits of the business associate's privacy practices.

Outsourcing of HIPAA Compliance to Business Associates. Prior to the issuance of the Final Amendments, it was unclear whether a self-insured health plan was required to provide individuals with the access, amendment and accounting rights to their PHI that is maintained in the individual's designated record set ("DRS") or whether such requirements could be outsourced to a business associate. (For insured health plans, insurance companies and HMOs, as covered entities in their own right, are directly required to comply with these rules.) Because in most cases the business associate maintains the vast majority of records that comprise an individual's DRS (copies of EOBs, payment records, claims by providers, etc.), it would be more efficient for a participant to deal directly with the business associate with respect to these requests. Fortunately, in the Final Amendments, HHS has clarified that health plans and business associates may agree in the business associate agreement that a business associate that maintains all or part of the original DRS shall directly receive and address participant requests relating to the access, amendment and accounting provisions of HIPAA. Thus, this clarification eliminates some of the health plan's HIPAA-compliance burden, if the health plan does not maintain the original DRS. However, health plans that choose to outsource those activities apparently would need to have a business associate agreement (addressing at least the outsourced activities) in place with the business associate prior to April 14, 2003, and therefore would not be able to entirely take advantage of the extended transition period.

Employment Records – Not PHI. In the Final Amendments, HHS adopted its proposed exception that excludes items in employment records from the definition of PHI. However, HHS declined to adopt a formal definition of "employment records," but noted in the Preamble that information needed by an employer to facilitate FMLA requests, sick leave requests, drug screening programs, fitness-for-duty exams, OSHA requirements and other similar programs could be included as an employment record. In addition, HHS clarified that an employer has dual roles – one role as an employer and another role as a health plan (based on its responsibility for the plan as plan sponsor). Health information that is created or received by an employer in its health plan capacity is PHI, while health information that is received by an employer in its employment capacity is not PHI. For example, medical information given to an employer by an employee to document sick leave or other authorized leave and placed in the employee's employment record would not be PHI and would not be subject to the Privacy Rule. However, if the employer sought to obtain the same medical information from its health plan, such information would be PHI and could not be released by the health plan without the individual's written authorization. Thus, the nature of the information does not determine whether certain information is or is not an employment record. Rather, it depends on whether the employer obtained or created the information in its capacity as an employer or in its capacity as a covered health plan.

© 2002 Mark L. Stember

Incidental PHI Disclosures are Exempt from Privacy Rule. The Final Amendments adopted the proposed "incidental disclosure" exception, which exempts incidental and unintentional disclosures that may occur as a result of engaging in normal health plan operations. For example, an incidental disclosure could occur if another employee overhears a conversation containing PHI. However, HHS clarified in the Preamble that such exception is only valid to the extent that the health plan has otherwise applied reasonable safeguards to protect the disclosure of PHI and has otherwise implemented the minimum necessary standard. (The minimum necessary standard requires health plans to limit any use or disclosure of PHI to only the minimum amount of PHI that is necessary to accomplish the purpose of the use or disclosure.)

Disclosure of Enrollment Information. HHS adopted its proposed exemption concerning disclosures of enrollment information to health plan sponsors. Thus, health plans (including health insurers and HMOs) are permitted to disclose enrollment or disenrollment information to a plan sponsor without meeting the plan document amendment and other related Privacy Rule requirements. This exception will serve to simplify compliance with the Privacy Rule (particularly for employer's sponsoring insured health plans). However, HHS noted that enrollment and disenrollment information still remains individually identifiable health information, and therefore would constitute PHI when received by the "health plan."

Clarification of the Minimum Necessary Standard. In the Preamble to the Final Amendments, HHS explained that a number of comments to the Proposed Amendments expressed concerns about the application of the minimum necessary rule to workers' compensation programs. HHS clarified that the minimum necessary standard permits health plans to disclose PHI that is reasonably necessary for workers' compensation purposes. Further, HHS intended the Privacy Rule to operate so as to permit information to be shared for such purposes to the full extent permitted by applicable law.

Clarification of Health Care Operations Disclosures. The Privacy Rule allows health plans and other covered entities to use and disclose PHI for health care operations purposes. The Preamble to the Final Amendments clarifies that if the Privacy Rule permits a covered entity to share PHI with another covered entity, the covered entity is permitted to disclose the PHI directly to a business associate of the other covered entity. In addition, a health insurer or HMO may disclose PHI to a health plan, or a business associate of the health plan (*e.g.,* a third party administrator), because the relationship between the insurer or HMO and the health plan constitutes an organized health care arrangement as defined in the Privacy Rule. Therefore, this clarification would appear to allow disclosures of PHI from an HMO to a health plan for underwriting and premium rating purposes, so that the health plan could determine whether the HMO is cost efficient relative to other benefit options.

"Layered" Privacy Notices Allowed. The Preamble to the Final Amendments discussed several comments received by HHS indicating that individuals would be more apt to read a shorter notice that was in a standard format. The commenters then requested that HHS provide a model privacy notice and to reduce the number of items that are required to be included in the notice (*e.g.,* they proposed to eliminate the requirement that the notice explain any "more stringent" state privacy laws). Despite these comments, HHS declined to change the items required to be included in the notice and declined to issue a model privacy notice. However,

© 2002 Mark L. Stember

HHS did clarify that covered entities may use a "layered" notice. The "layered" notice would consist of a short (presumably one-page) notice that briefly summarizes the individual's rights and other pertinent information, and a longer notice that is layered beneath the short notice that contains all the elements required by the Privacy Rule.

What's Next? The Final Amendments did not change the date for complying with the Privacy Rule, which remains April 14, 2003. ("Small health plans," which are health plans with annual receipts of $5 million or less, have until April 14, 2004 to comply.) In spite of the hopes of some that the Final Amendments would delay the general compliance date, we now have further evidence of HHS' determination not to delay it. At the same time, as noted above, those employers who have an executed written contract in place with a business associate prior to October 15, 2002 are granted up to an extra year to comply with the business associate agreement provisions of the Privacy Rule, and current action can still secure this extension. Clearly the HIPAA clock is ticking, particularly for employers with self-insured health plans for whom HIPAA's burdens are greater. The new guidance will facilitate compliance, but HIPAA compliance remains highly involved and deserves to be a current priority for all employer sponsors with health plans above the $5 million threshold.

© 2002 Mark L. Stember