American Bar Association

Technical Session Between the Department of Health and Human Services and the Joint Committee on Employee Benefits

May 10, 2007

The following notes are based upon the personal comments of the various individuals from the Office for Civil Rights of the Department of Health and Human Services who attended a meeting with the representatives of the various sections comprising the Joint Committee on Employee Benefits from the American Bar Association on Thursday, May 10, 2007. The comments were made by these individuals in their individual capacities and not as representatives of the Department of Health and Human Services, the Office for Civil Rights, or of any other government agency or office. None of these comments should be considered official guidance or the position of any agency.

This document has been prepared by private sector members of the American Bar Association's Joint Committee on Employee Benefits who were present at the meeting and reflects their description of the answers to the questions that were discussed at the meeting.

Question 1: Please provide a brief summary of any audit or enforcement activities that HHS/OCR has undertaken since April 14, 2003, with respect to the HIPAA privacy rule – particularly any such activities with respect to group health plans. What kinds of complaints are you receiving with respect to group health plans?

Answer 1:

OCR stated that as of April 2007, OCR has received approximately 27,000 complaints, and has resolved about 75 percent of these complaints. About 390 complaints have been referred to the U.S. Department of Justice. Additional statistics were provided that are now available on OCR's new webpage on compliance and enforcement, which also includes case examples of some investigations and the corrective actions taken. The website is http://www.hhs.gov/ocr/privacy/enforcement.

The number of complaints continues to increase each year. Most complaints continue to involve private physician practices, followed by hospitals, outpatient facilities, group health plans and issuers (including MEWAs), and pharmacies. OCR stated that complaints concerning group health plans do not always distinguish between whether the violation is being alleged against the group health plan or a health insurance issuer (carrier).

Question 2: Are their any plans to issue more formal or informal guidance on the HIPAA privacy rule?

Answer 2:

OCR did not state any specific initiatives in the works concerning group health plans, but OCR asked if there were any issues that the group thought OCR should address. One member of the group noted that the case examples on the website were limited to situations where the carrier in an insured arrangement had violated HIPAA privacy. A request was made for some group health plan examples. Another member of the group requested that OCR take a look at some of the informal nonbinding guidance that OCR has issued in recent years at the annual ABA/JCEB question and answer sessions, and consider putting out more formal guidance on some of the issues addressed in these sessions.

Question 3: If an individual executes a valid HIPAA authorization with a specified expiration date and subsequently dies before the expiration date, how does that affect the validity of the authorization? If no expiration date is specified, does that change the result? If the individual no longer has the ability to revoke the authorization (because they are deceased) is the scope of the authorization altered? Has HHS made any efforts to coordinate state laws that may control this issue?

Proposed Answer 3: The Privacy Rule requires that an Authorization contain either an expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. 45 C.F.R. 164.508(c)(1)(v). An Authorization remains valid until its expiration date or event, unless effectively revoked in writing by the individual before that date or event. In the case of a deceased participant, an executor or personal representative could revoke the authorization in writing. The death of the participant does not by itself limit the scope of an authorization. The fact that the expiration date on an Authorization may exceed a time period established by State law does not invalidate the Authorization under the Privacy Rule, but a more restrictive State law would control how long the Authorization is effective.

Answer 3:

OCR agreed with the answer, and stated that the authorization remains valid unless it expires or is revoked. A state law could impact this outcome, but the state law would have to be evaluated along with the specific facts of the case. Except for specific cases (investigations or enforcement actions) or in addressing requests for preemption exception determinations, OCR does not make determinations as to the application of a state law.

Question 4: May a self-insured employer discipline an employee based on enrollment information that shows that an employee has improperly enrolled a dependent in the

employer's health plan (e.g., ineligible ex-spouses, ineligible children above a specific age who are not college students, etc.)?

Proposed Answer 4: In 2005, this group discussed the extent to which a group health plan could audit claims data and, if the plan discovered evidence that an individual had committed a claims fraud under the plan, that data could be used for purposes of terminating the individual's coverage under the plan. At that time, HHS/OCR representatives opined that it would be very difficult for an employer to use any evidence of the fraud to discipline the employee without running afoul of the Privacy Rule, since the claims data is, by its nature, Protected Health Information (PHI). (The discussion regarding audits is reported in Q&A-5, at www.abanet.org/jceb/2005/qa05hhs.pdf.) However, that question only addressed claims data, not enrollment data.

The preamble to the 2002 modifications to the Privacy Rule states that individually identifiable health information received or created by the group health plan for enrollment purposes is PHI under the Privacy Rule. 67 Fed. Reg. 53181, 53208 (Aug. 14, 2002). Therefore, when enrollment information is transferred by an employer to the group health plan, it becomes PHI.

An employer may discipline an employee who improperly enrolls a dependent in the employer's group health plan without violating the Privacy Rule, provided that the employer takes such action without regard to any claims data or other PHI (other than PHI that is enrollment information) that it holds with respect to the employee or dependent.

Answer 4:

The Privacy Rule regulates the conduct of covered entities, not of employers acting in their employment capacity. An employer's disciplining of an employee could, on the other hand, violate the amended plan documents and the plan sponsor's certification pursuant to 45 C.F.R. 164.504(f)(2)(ii). OCR distinguished between information obtained by an employer under the enrollment provisions in 45 C.F.R. 164.504(f)(1)(iii), and information obtained through a plan administration activity. If the employer as a plan sponsor has taken responsibility for enrollment and eligibility, then information that the plan sponsor obtains from the GHP regarding whether an individual is participating in the GHP is not subject to the plan document restriction on the sponsor's use of that information. In order for the plan sponsor to obtain claims information, it must amend its plan documents and agree not to use or disclose it for employment-related activities (including disciplining an employee).

Question 5: In August 2006, the Securities and Exchange Commission adopted new final regulations that substantially changed the disclosure requirements for public companies with respect to executive and director compensation. See, 71 Fed. Reg. 53158 (September 8, 2006). As part of these final regulations, a public company is required to describe the compensation programs of its named executive officers and specifically list

the dollar value of the compensation program. These descriptions and dollar values must be included in the public company's annual filings with the SEC.

Assume a public company sponsors an executive physical program that pays for annual physicals and diagnostic tests for certain executives (the "Physical Plan"). Assume further that the Physical Plan is a "health plan" under the HIPAA privacy rules. Pursuant to the new SEC regulations, the public company is required to disclose the fact that a named executive officer participates in the Physical Plan and the annual dollar value of the Physical Plan. The public company proposes to comply with these regulations by describing in its SEC filings, that each named executive officer received an annual physical and the dollar amount of the total claims paid on each executive's behalf for the year. However, no other PHI will be disclosed, and in particular, no information regarding whether certain diagnostic tests were performed and the results of the physical and any related tests will not be disclosed.

Is this disclosure required by law and therefore exempt under HIPAA Regulation Section 164.512(a), or is the Physical Plan required to obtain an individual authorization from each named executive officer prior to disclosing the above information?

Proposed Answer 5: HIPAA Regulation Section 164.512(a) provides that if a disclosure is required by law, a health plan is not required to obtain an individual authorization prior to releasing PHI that is related to satisfying the legal requirement. The new final SEC regulations require public companies to disclose each compensation program and the dollar value of the program for each named executive officer. The most logical amount to disclose for the dollar value of participation in the Physical Plan is the total dollar amount of claims paid on behalf of each named executive officer. Therefore, disclosing a named executive officer's participation in the Physical Plan and the total dollar amount of claims paid on his/her behalf is required by law, and the Physical Plan is not required to obtain an individual authorization prior to the disclosure.

Answer 5:

OCR stated that Section 164.512(a) only applies to a covered entity. The SEC regulations are directed to the employer (e.g., plan sponsor), not the CE (e.g., the group health plan). Therefore, section 164.512 would not be applicable to disclosures from the GHP to the plan sponsor. If information is needed from the GHP for this purpose, the employer could obtain an authorization from each of its executives permitting the plan to disclose the information sought for the reporting. If the GHP, under properly amended plan documents, is already providing the data to the plan sponsor for plan administration purposes, the plan sponsor would be allowed to redisclose it as required by law.

Question 6: There has been much discussion in the trade press regarding electronic personal health records ("PHR"). Many of these discussions concern health care providers establishing and maintaining the PHR. PHR arrangements also are provided by employer-sponsored plans through fully-insured arrangements with a health insurance carrier. Assume a plan contracts with a health insurance carrier to provide fully-insured

group health benefits. The coverage also includes a free service provided by the carrier to provide employees with electronic personal health records (PHR). Although the carrier and a data storage company provide the service, it is part of the group health benefit provided by the group health plan. For employees that wish to participate, claims and other health information such as lab results will be stored and sent to a data management service so that participants may start to keep a personal electronic health record. The plan has no access to any of the information kept in the PHR. The carrier and the data storage company have access to the information in order to administer the service. Must the plan execute a business associate agreement with the insurance carrier in order for the carrier to access PHI for this purpose? Is the plan required to disclose the arrangement in its Notice of Privacy Practices?

Proposed Answer 6: The group health plan is not required to have a business associate agreement with the carrier where the service is offered through a fully-insured arrangement. See generally, 45 C.F.R. 164.506(c)(5). The carrier itself is a covered entity under HIPAA, is responsible for complying with HIPAA, and is required to have a business associate agreement with the data storage company.

A general description of the arrangement should be included in the Notice of Privacy Practices. However, the health insurance carrier, not the plan, is responsible for providing the Notice. 45 C.F.R. 164.520.

Answer 6:

OCR agreed that no business associate agreement is required between the plan and the carrier. The carrier would be responsible for providing the Notice of Privacy Practices. They noted that the disclosure in question generally falls into the definition of "health care operations." The requirements for the Notice of Privacy Practices do not require an example for every type of disclosure, so a general description of this specific arrangement is not necessarily required, although it may be a prudent thing to do.

Question 7: Recently, health plans, specifically employer-sponsored self insured group health plans, have started to provide PHRs for their employees and dependents who participate in the health plan. These PHRs are typically accessible from a secure website, using a specific user name and password. In addition, one vendor's particular type of PHR automatically integrates with a health plan's third party claims administrators, so that when a participant goes to a physician and that physician files a claim with the third party claims administrator, the claims administrator will transmit a copy of the claim to the PHR vendor, and the PHR vendor will then automatically upload the claim into the participant's PHR. The PHR and the automatic update process are provided for all participants without their request. However, in order to access the PHR, the participant must sign on to the secure website to view the PHR. If a participant did not want an PHR for some reason, the participant would not be required to view the PHR on the secure website, but it would still be resident in the PHR vendor's computer system in case the participant changed his or her mind in the future. The PHR is not removed from the

computer system, because if it was, then the participant's PHR would not automatically update. If the participant changed his or her mind in the future and wanted the PHR, the PHR would then not contain any updates and would need to be started from scratch. Because PHR's are provided without the consent of the participant or spouse, does this violate the HIPAA privacy rules?

Proposed Answer 7: No. Assuming all of the appropriate business associate contracts are in place, a PHR provided by a health plan is part of the health plan's "health care operations" activities, and can be created and updated without the consent of the individual who is the subject of the PHR.

Answer 7:

OCR agreed with the proposed response and stated that the provision of a PHR is part of health care operations, and individual consent or authorization is not needed. Going forward when discussing the development of PHRs in the context of the framework enunciated by the American Health Information Community (AHIC), there is envisioned a heightened degree of consumer control in regard to an individual's PHR. In addition, OCR cautioned that, as the industry moves towards connectivity and interoperability of individuals' health information, it is envisioned that such a system would incorporate some form of consumer choice as to whether and how much to participate.

Question 8: A group health plan contracts with a health insurance carrier to provide fully-insured group health benefits for its employees and dependents. The carrier provides, at no additional charge to the plan, a service designed to assist employers in assessing the health risks of their employee population. Under this service, the carrier administers a health risk assessment program (HRA) where employees can voluntarily fill out an online questionnaire that asks questions concerning height, weight, physical activity, and medical (claims) history. Individuals who complete the HRA receive a personalized health report from the carrier that assesses their health status and provides information on how the individual can improve or maintain their health status. The carrier contracts with a third party to assist in administering the program. The carrier also prepares a report for the plan sponsor that summarizes the results of the HRAs completed and provides aggregate information including the medical history of those who completed the HRA. It does not include names, social security numbers, health plan account numbers, birth dates or specific dates of treatment, but does include the ages of individuals who completed the survey and includes information about past diagnosis or recent treatment received. Other than this aggregate summary report, the plan sponsor does not have access to any other information from the HRAs or access to the completed HRAs.

Must the plan obtain a HIPAA business associate agreement with the carrier under the HIPAA privacy rules? Can the plan sponsor receive the aggregate summary report from the carrier without individual authorization? Does the analysis change if the plan is self-insured and the carrier is simply administering the self-insured benefit and providing the

HRA program? What are the plans obligations to disclose the arrangement in its Notice of Privacy Practices?

Proposed Answer 8: There is no requirement for the fully-insured plan to have a business associate agreement with the carrier. See generally, 164.506(c)(5). The carrier is itself a covered entity under HIPAA, and has its own obligations to comply with HIPAA and execute a business associate agreement with its own third party contractors. HIPAA allows the disclosure of information for health care operations without individual authorization. Health care operations include population- based activities related to improving health or reducing healthcare costs. As a result, the aggregate summary report may be disclosed to the plan sponsor without individual authorization, as long as plan document amendments are made pursuant to 45 C.F.R. 164.504(f).

Where the plan sponsor is self-insuring the benefit, a HIPAA business associate agreement must be executed with the carrier. The plan sponsor may receive the aggregate summary report, if plan documents have been amended pursuant to 45 C.F.R. 504(f).

The Notice of Privacy Practices should provide a general description of the arrangement. For a fully-insured plan, the health insurance carrier is responsible for providing the Notice. The insured group health plan is not required to provide or maintain the Notice under 45 C.F.R. 164. 520(a)(2)(ii) since the information it receives in the aggregate summary report is "summary health information" as defined in 45 C.F.R. 164.504(a). The self-insured plan must provide the Notice.

Answer 8:

OCR agreed that in the insured scenario, the plan is not required to obtain a HIPAA business associate agreement with the carrier. In the self-insured example, a business associate agreement is required.

Concerning the disclosure of the aggregate summary report, OCR stated that the HIPAA regulation allows disclosure of health information to a plan sponsor (1) if plan documents incorporate certain requirements including restricting the plan sponsor's uses and disclosures to those permitted by the Privacy Rule and the plan sponsor needs this information to perform plan administration functions for the group health plan; (2) if the information is limited to "summary health information" (as the term is defined at § 164.504(a)) and is provided pursuant to § 164.504(f)(1)(ii) for purposes of the plan sponsor shopping or modifying the plan; or (3) if the information is de-identified in accordance with § 164.514(a)-(c). Note that even if the identifiers listed at § 164.514(b)(2)(i) are stripped, the information is not de-identified if the covered entity has actual knowledge that the information could be used alone or in combination with other information to identify an individual.

OCR agreed with the proposed answer concerning the responsibility for providing the Notice of Privacy Practices. With respect to the description in the Notice itself, OCR stated that the requirements for the Notice of Privacy Practices do not require an example of every type of disclosure, so a general description of this specific arrangement is not necessarily required, although it may be a prudent thing to do.

Question 9: Some group health plans want to require that their employees complete a health risk assessment (HRA) in order to be eligible for coverage. The plan would use the PHI obtained in the HRA in order to assess what types of wellness programs would work best to improve health outcomes in the plan. Would this practice violate HIPAA privacy?

Proposed Answer 9: No. The HIPAA privacy regulation allows the use of PHI by a covered entity for health care operations, which includes population-based activities related to improving health or reducing healthcare costs. It does not prohibit the disclosure of PHI by a plan participant as a condition of eligibility for health coverage.

Answer 9:

OCR agreed with the answer, adding that HIPAA's Privacy rules do not address the determination of eligibility for a group health plan. They have forwarded inquiries on this topic to the Department of Labor's, Employee Benefits Security Administration, who is working with the EEOC to address these types of questions.