AMERICAN BAR ASSOCIATION

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

May 17, 2005

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 Tuesday, May 17, 2005. 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. This document has not been reviewed or cleared by the government officials involved in the meeting.

Question 1: Can you please provide a brief summary of any audit or enforcement activities that HHS/OCR has undertaken in the last year with respect to the HIPAA Privacy Rule – particularly any such activities with respect to health plans?

Answer: HHS has received 13,000 complaints on HIPAA privacy since the start of their compliance efforts. HHS has steadily increased the closure rate to 65%, and now has 5,200 open complaints.

There are not as many complaints regarding health plans as there are for providers. The order for most complaints regarding violation of the privacy rule is: (1) private practices; (2) hospitals; (3) pharmacies; (4) outpatient facilities; and (5) health plans. There are more complaints regarding group health plans than government plans or other types of plans. (This categorization is not precise, since investigators may label something on initial intake as a group health plan that is not exactly a group health plan).

There are investigators in HHS's 10 regional offices. Approximately 200 investigators in those offices handle complaints regarding both civil rights and HIPAA privacy. The regions organize themselves in different ways, and there is not always a dedicated privacy person in each region.

The primary issue being raised on complaints is impermissible disclosure of protected health information (PHI). There are also many complaints about misdirected billing activity. On the provider side there are a large number of complaints about employees misusing PHI.

HHS has not levied any civil money penalties. HHS recently issued procedures for imposing civil money penalties.

HHS has provided technical assistance to let providers know what is a permissible disclosure. HHS recognizes that personal representatives are still having trouble getting information from providers. HHS is working with providers to let them know what is proper disclosure.

Question 2: HHS has continued to update the frequently asked questions on HIPAA privacy, which has been very helpful. (ABA members should be aware that the frequently asked questions and answers are available at http://www.hhs.gov/ocr/hipaa/assist.html, then clicking on the link titled "View and Search Health Information Privacy Frequently Asked Questions (FAQs)".) Are there any plans, however, to issue any more formal guidance on the HIPAA privacy rules?

Answer: HHS does not have any immediate plans to issue any more formal guidance than the FAQs. HHS has gotten good feedback on using FAQs. HHS has a project to repackage the existing guidance by groups – such as by providers or by group health plans – and add additional examples and explanations to address more common situations to the particular group.

Question 3: If an employee or former employee files a charge with the Equal Employment Opportunity Commission (EEOC) against an employer the defense of which involves the use of protected health information (PHI), to what extent may the group health plan sponsored by the employer disclose such PHI to the employer to assist in its defense of the charge?

For example, assume a claim is filed against an employer for discriminating against an employee because of the employee's pregnancy. To defend against the charge, the employer needs to present statistics on its treatment of other pregnant employees. Can the employer request information from the health plan on which employees have been pregnant?

Proposed Answer 3: To the extent an EEOC charge is premised on a violation involving benefits under a group health plan, the group health plan may disclose PHI to the employer to the extent necessary to allow the employer to defend against the charge without the consent or authorization of the charging party or any other individual whose PHI is disclosed, provided that the PHI would be available during discovery in litigation or the employer reasonably believes that the plan would be the proper defendant in litigation. The above approach is necessary because the requirements for disclosure of PHI under 45 CFR § 164.512(e) do not provide adequate means for an employer to obtain the information needed to defend an EEOC charge involving benefits-related claims.

Alternatively, the employer's request for PHI to defend the EEOC charge is made pursuant to an "other lawful process" not accompanied by an order from a court or administrative tribunal (*see 45 CFR § 164.512(E)(1)(ii)),* and the plan's disclosure of the PHI is governed by 45 CFR § 164.512(e)(1)(iii).

Answer: HHS **disagreed** with the proposed answer. HHS stated that if the EEOC claim is not related to the group health plan's activities, the information cannot be provided by the group health plan on a voluntary basis. The information could, however, be subpoenaed from the group health plan.

Question 4: If a group health plan provides benefits entirely through insurance policies and is generally hands-off with respect to PHI, would the plan's administration of COBRA continuation coverage (e.g., enrollment and payment history) cause it to be subject to the HIPAA privacy rules?

Proposed Answer 4: Yes. Because enrollment information and payment history held by the group health plan is PHI, the plan would be subject to the HIPAA privacy rules.

Answer: HHS **disagreed** with the proposed answer. HHS noted that if a plan is fully insured and the employer only has enrollment and disenrollment information and summary health information, then the obligations with respect to the privacy fall upon insurer. HHS opined that the plan's administration of COBRA does not change the result.

Question 5: Is a Health Savings Account (HSA) subject to the HIPAA privacy rules? If the answer is yes, who has the responsibility for ensuring that the HIPAA privacy requirements are met, the individual account owner, the custodian or trustee of the HSA, or an employer who maintains the related High Deductible Health Plan?

Proposed Answer 5: The privacy rules apply to "covered entities," which include health plans, health care clearinghouses, and health care providers. The definition of health plan includes individual and group plans that provide or pay for the cost of medical care.

Although the definition of health plan is broad enough to include HSAs established by an individual with no involvement on the part of the individual's employer, the privacy rules were not intended to apply in this context. The privacy rules serve, in part, to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well being. As the Department of Labor noted in Field Assistance Bulletin 2004-1, "HSAs are personal health care savings vehicles rather than a form of group health insurance." Furthermore, funds held in an HSA need not be used exclusively for the payment of medical care (although they may lose certain tax benefits if they are used for other purposes). HSAs were introduced as a means of promoting savings and assisting individuals with the high cost of health care. Subjecting HSAs to the burden of HIPAA compliance would discourage rather than promote savings because it would discourage trustees and custodians from offering such accounts and would add to the costs of maintaining them. In balancing the promotion of health care savings with the need to protect individuals' health information, we believe the better approach is not to subject individual HSA accounts, nor the custodians or trustees that sponsor them, to the HIPAA privacy rules where there is no involvement by employers in the establishment or maintenance of the account.

Answer: HHS stated that it is coming to the conclusion that HSAs are not health plans and therefore are exempt from the HIPAA privacy rule. HHS is trying to distinguish between HSAs, which function more like individual savings accounts, and group health plans. HHS may issue further guidance on this issue in fall 2005.

Question 6: This was a question that we asked in 2004. The answer was that the question had provoked considerable discussion within HHS, but HHS did not share any of their thinking on this question. Do you have any further thoughts as to a response?

A health plan document and SPD provide that coverage may be terminated and warn that other disciplinary action, including termination of employment, may be taken if an employee or dependent files false claims or submits other fraudulent or misleading information under the plan. Under HIPAA's privacy rule:

(a) May a business associate or plan sponsor (acting in a plan administrative capacity) audit claims to detect fraud?

(b) If fraud is discovered, may the business associate use or disclose that information to terminate the coverage of the employee and/or dependent?

(c) May that information then be used or disclosed to discharge the employee?

Proposed Answers: Exactly how this situation unfolds depends on the circumstances. At a minimum, the plan sponsor or business associate should be allowed to conduct the audit, use or disclose the information discovered to terminate coverage, and use or disclose certain information to advise a plan sponsor that enrollment has been terminated for fraud and of the magnitude of the problem, even though an employer may (and to a large extent to permit an employer to) terminate an employee's employment or take other employment-related actions. More specific information should not be disclosed without individual's authorization.

(a) Plan sponsors and business associates may audit claims under a plan generally and may specifically audit for fraudulent claims. These audits would be considered part of the plan's health care operations. *See* 45 CFR 164.501 and 164.502(a) (1)(ii). The audit may be conducted by either a business associate pursuant to the terms of the relevant business associate agreement, 45 CFR 164.504(e), or by a plan sponsor pursuant to an appropriate plan amendment, 45 CFR 164.504(f)(2)(C). *See also* 45 CFR 164.502(e). An audit of an individual's claims could be conducted pursuant to the written authorization of that individual, 45 CFR 164.508, but in these circumstances it would typically be impractical to obtain individual authorization.

(b) Both business associates and plan sponsors who discover evidence of false claims in the course of an administrative claims audit should be permitted to use that information for purposes of terminating the individual's coverage under the plan. The termination of an employee for filing false claims constitutes an administrative action taken pursuant to the plan's terms. Even if protected health information is deemed to be used in terminating the individual's coverage, that use (or disclosure for that use) would be warranted as meeting the definition of either "payment" or "health care operations." 45 CFR 164.501. Of course, the authority given to the business associate in the business associate agreement or plan sponsor in the plan document should be broad enough to allow them to use or disclose protected health information for this purpose.

In certain circumstances, the use and disclosure of protected health information may be limited. False claims may have little or nothing to do with an individual's actual medical condition or health care. *See* 45 CFR 160.103 ("protected health information" and "individually identifiable health information"). For example, when an individual fraudulently loans out his or her HMO

identification card or falsely obtains prescription drugs for resale, there may be little in the record that would constitute protected health information for that individual. The medical information at issue may be for another person or completely fabricated. The business associate or plan sponsor (acting as plan administrator) should take reasonable measures to filter actual protected health information out of what it uses or discloses for these purposes to safeguard legitimate privacy interests.

(c) The potential use or disclosure of protected health information for purposes of employment actions raises greater concerns. While a plan sponsor may use and disclose protected health information for various plan administrative purposes, it may not use or disclose that information for employment-related actions. 45 CFR 164.504(f)(2)(ii)(C). Business associates would not ordinarily have a basis for disclosing protected health information to an employer for an employment action. The disclosure could not ordinarily be justified as treatment, payment or health care operations for the plan.

However, the fact that the plan itself has terminated the coverage of an individual cannot be kept from the plan sponsor or employer. Plan sponsors and ultimately employers need to be informed that the plan has disenrolled an individual for various purposes (such as premium payments and payroll deductions or reductions). Plans are expressly permitted to "disclose to the plan sponsor information on whether the individual is participating in the group health plan...." 45 CFR 164.504(f)(1)(iii). The question is how much information may accompany notice of this administrative disenrollment.

If the plan sponsor receives only the barest information, an employer may be placed in the position of making a decision about terminating an employee based solely on the knowledge that the plan administrator has terminated the individual's coverage for reasons under the plan. It would be more sensible for an employer to have more information before making a decision as to whether to terminate the employee's employment. The fact that coverage was terminated for filing false claims and the amount that the plan paid as a result of this fraudulent activity do not reveal anything about the individuals health condition or care or the benefits paid for actual health care. It would allow an employer to consider, for example, whether coverage were terminated because false claims were filed over a period of several years at a substantial cost to the plan. The provision of sufficient information for an employer to assess the extent of a problem that resulted in a termination of coverage would also be appropriate in light of concerns expressed in HIPAA (in provisions that extend beyond the administrative simplification provisions) about fraud in the health care industry. Further information could be obtained to the extent the individual authorizes the employer to have access to the information.

Answer: HHS agrees with the first two proposed responses, with respect to permitting audits and ending the coverage for the employee who engaged in a fraudulent act. That is, the privacy rule permits a plan sponsor, third party administrator or business associate, to (a) conduct audits of the plan to, among other things, detect fraud, and (b) permits information to flow back to the plan in order to effectuate the coverage termination as a result of fraud.

HHS argued that it would be difficult to use the PHI to fire the employee without violating the privacy rules. JCEB representatives suggested that an employer might be able to obtain an authorization that, as a condition of employment, an employee must give an authorization for disclosure of job related health information, since OCR does not regulate employers as

employers, but only regulates employers in their function as health plan sponsors. HHS cautioned that such an authorization could not be worded to require that the employee have health coverage under the plan to remain employed by the employer, since doing so might be treated as a compelled waiver of an individual's privacy rights.

Question 7: Are there any issues regarding HIPAA privacy concerning health plans that HHS is currently discussing or evaluating where the input of the members of the ABA's Joint Committee on Employee Benefits would be of assistance?

Answer: JCEB and HHS representatives spent some time discussing the disclosure of PHI in the merger and acquisition (M&A) context. We discussed that, although the privacy rule specifically addresses the merger of covered entities (such as two hospitals), it does not address corporate transactions involving two employers that are non-covered entities. We noted that the issues are particularly complex in an asset situation.

HHS suggested that it would be helpful for any interested persons to (1) layout what the steps are in the various commonly recurring corporate transactions and where health information comes into play at various steps; (2) identify what clarity can be provided in terms of who actually needs the information and their role (i.e., plan versus employer versus others), and (3) identify where there is a need for clarification, or where there is any misunderstanding, in terms of how the privacy rule would apply at the various points.