American Bar Association

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

May 2, 2006

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 2, 2006. 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: 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:
As of the end of March 2006, OCR had received approximately 18,900 complaints. OCR has resolved 72% of these complaints. Complaints have been resolved through voluntary compliance, or cases have been closed because they do not implicate the HIPAA privacy rule for various reasons (e.g., it does not involve a covered entity). Between one-third and one-half of all complaints have been closed because the complaint is defective or does not state an issue under the jurisdiction of the HIPAA privacy rule.

Most complaints involve (in order of frequency) improper use of PHI, lack of adequate safeguards, access to records, excessive fees for obtaining access to records, disclosing more than is minimally necessary, and failure to receive authorization. This list is based on complaints against all types of covered entities. OCR has not seen a unique pattern in terms of the types of complaints lodged against group health plans. They are consistent with the above list of types of complaints received from other covered entities. A misdirected Explanation of Benefits (EOB) is an example of a type of complaint received OCR has received concerning a group health plan. OCR stated that they received most

complaints against private doctor's offices, followed by hospitals, outpatient facilities, group health plans and pharmacies.

OCR elaborated on the excessive fee complaints that they receive. OCR stated that the law allows a reasonable cost-based fee such as copying costs, but there has been some push back regarding entities also charging based on the charges for staff time used to retrieve the PHI. OCR has not set a specific threshold, but will defer to state statutes that set fee structures, as long as the state laws do not involve a flat fee or retrieval costs.

OCR has referred more than 300 cases to Department of Justice for assessment of criminal violations. DOJ has chosen not to investigate most of these cases. OCR mentioned the two criminal prosecutions brought by DOJ, the *Gibson* case, and a more recent case in Texas. The Texas case, *Ramirez*, involved the selling of PHI by an employee of a physician's office to an FBI informant. OCR noted that, from the information that they had, the prosecution involved a charge of aiding and abetting a covered entity.

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

Answer 2:
Although OCR did not provide any specifics, they will continue to provide technical assistance materials on various issues. There was positive feedback on the use of Frequently Asked Questions as a means to get out information. OCR stated that these are not regulations, but they are official departmental interpretations of the regulations, and OCR believes it is bound by them (although courts may not necessarily give deference to the FAQ). In response to a question concerning changes to the content of the FAQ answers or later withdrawal of FAQs from the website, OCR stated that the FAQs are subject to change, but these will generally be announced on the listserve or on the "What's New" section of the website.

OCR did mention that they were working on internal projects and technical assistance around the issue of electronic medical records and emergency preparedness (i.e. how to connect people with their medical information during an emergency).

Question 3: In a recently released OCR Frequently Asked Question, OCR discussed several ways in which a covered entity can comply with the requirement for covered entities to send out, at least every three years, a reminder that the HIPAA Notice of Privacy Practices is available and how to obtain it. See 45 C.F.R. 164.520(c)(1)(ii). May a covered entity required to send this reminder send it out electronically instead of in hard copy?

Proposed Answer 3:
An electronic notice of the reminder may be sent if it meets the same standards required to send the Notice of Privacy Practices itself electronically under 45 C.F.R. 164.520(c)(3). Under this requirement, the notice may be sent out by email only if the

individual recipient agrees to receive notices electronically, and such agreement has not been withdrawn. The individual retains the right to obtain a paper copy of the notice from a covered entity upon request.

Answer 3:
OCR agreed with the proposed answer. They said the reminder should be distributed in a manner that is consistent with the distribution of the original. They noted that there are several options to sending the notice in hard copy, including making the reminder part of another publication, like a plan's electronic newsletter. It is not necessary for the reminder to be the exclusive contents of a distribution. OCR commented that this question is addressed in its FAQs, which also discuss another, related question concerning how a small health plan (at the time of the original privacy notice) that had now become a large group health plan determined the date it needed to send the reminder. OCR indicated that the date the original notice was sent determined the date that a reminder was required, not the size of the group health plan giving the notice. Finally, OCR mentioned that a group health plan was not required to wait three years to provide a reminder; more frequent reminders were encouraged.

In response to a follow-up question concerning how a participant can elect to receive reminders electronically, OCR noted that the individual must specifically elect to receive it electronically. To protect itself, the covered entity must have some kind of evidence or proof on file that a person has in fact waived the right to receive this notice in hard copy and has agreed to receive it electronically. This proof can itself be electronic.

Question 4: A self-insured plan sponsored by an employer contracts with a third party administrator (TPA) to administer claims. The plan sponsor and the plan do not receive protected health information (PHI). The plan has in place with a TPA a business associate agreement. There is an improper disclosure of PHI when the TPA sends out over 200 Explanation of Benefit (EOB) notices to the wrong participants. Participants received the EOBs of other participants that contained PHI including names, social security numbers and the names of specific medical procedures that were received. The TPA is aware of the improper disclosure but does not notify the plan, nor does it take any action in response to the mistake. A complaint is filed with OCR alleging that the plan has violated HIPAA's privacy rule. Assuming that the improper disclosure of PHI is a violation of the HIPAA privacy requirements, under the final enforcement regulation for HIPAA administrative simplification, can OCR assess a penalty against the plan? If the plan was aware of the breach, could OCR assess a penalty against the plan?

Proposed Answer 4:
Under 45 C.F.R. 160.402(c) of the HIPAA Administrative Simplification Enforcement Rule a violation of HIPAA's privacy requirements by a business associate cannot be attributed to a covered entity if (1) the covered entity has complied with the business associate provisions of the HIPAA privacy rule, and (2) did not know of a pattern of activity of the business associate resulting in the breach. Where the plan was not aware of the breach and they had a proper business associate agreement in place with the TPA, a penalty cannot be assessed. A penalty could be assessed against the plan if the plan was

aware of the breach, except where the plan took reasonable steps to cure the breach or end the violation, and if such steps were not successful, terminated the contract with the business associate. If termination was not feasible, the plan must report the problem to the Secretary. See also 45 C.F.R. 164.314(a)(1).

Answer 4:
OCR does not agree with the proposed answer. They stated that, if feasible, termination of the contract with the TPA would be required if the TPA refuses to take any action to mitigate the problem. OCR indicates that there is a very high threshold as to the feasibility of termination. OCR stated that to the extent the problem was cause by a computer error, the business associate should do a manual work around to correct the problem.

Question 5: A self-insured plan contracts with a pharmacy benefit manager (PBM) to administer its drug benefits. The plan has a business associate agreement with the PBM. The plan has applied to receive the Medicare Part D Retiree Drug Subsidy. The PBM will be submitting to CMS, on the plan's behalf, specific claims information as part of the reconciliation process required in order to obtain the retiree drug subsidy. See 42 C.F.R. 423.888(b)(4). The plan has hired a claims auditor to review the claims information that the PBM has provided to CMS for accuracy and completeness. The plan has a business associate agreement with the claims auditor. Assuming the claims information is PHI, can the PBM provide this information directly to the claims auditor for review without individual authorization under HIPAA's privacy rule?

Proposed Answer 5:
Yes. PHI can be exchanged between business associates of a covered entity as long as it is at the direction of the covered entity, and is for treatment, payment, or health care operations. In this instance, the disclosure of claims information to the claims auditor is a "health care operation" as defined under the privacy rules to include, "conducting or arranging for …auditing functions, including fraud and abuse detection and compliance programs." See 45 C.F.R. 164. 501. In addition, 45 C.F.R. 164.502(e)(1)(i) states that a covered entity may "allow a business associate to … receive protected health information on its behalf…" provided that a business associate agreement is in place.

Answer 5:
OCR generally agreed with the proposed answer, but added that the exchange of PHI can occur between business associates as long as the business associate agreement provides the business associate with the authority to provide the PHI to other business associates. They also noted that HIPAA cannot be used to prevent the flow of PHI for the "health care operations" of the plan, including audits of business associates and insurance carriers. An example was raised where an insured group health plan was attempting to do a claims audit of its insurance carrier and the insurance carrier had refused to provide information necessary for the audit citing HIPAA. OCR stated that HIPAA allows the disclosure of PHI for a "health plan operation" such as an audit, assuming the plan otherwise meets HIPAA's requirements such as amending plan documents.

OCR also added a reminder that the Notice of Privacy Practices must disclose information and examples about how PHI is disclosed for health plan operations such as audits.

Question 6: An employer has a self-insured plan through an administrative services agreement with an insurance carrier (ASO). The ASO/carrier provides and administers the benefit. The plan sponsor has amended plan documents, has human resource professionals dedicated to benefit activities, and the plan sponsor receives PHI for various plan administration activities. The plan has a business associate agreement with the ASO. Part of the benefit administered by the ASO is a voluntary wellness program designed to help improve the health outcomes of pregnant participants and their newborns. Under the wellness program, case managers contact pregnant women, who have signed up for the program, during each trimester of the pregnancy to ask a series of questions and answer any questions that the expectant mother has. The case managers work with those identified as having high-risk pregnancies to coordinate needed care. Assuming the wellness program is itself a group health plan covered by the HIPAA privacy rules, could the ASO, on behalf of the plan, use claims information it receives to administer the plan's group health coverage to target individuals who may benefit from the wellness program, and send them literature about the program? Alternatively, could the ASO provide the information to the plan sponsor, and the plan sponsor send out material to the selected participants about the wellness program?

Proposed Answer 6:
Under HIPAA's privacy rules, a covered entity may use and disclose PHI for the "health care operations" of the plan without individual authorization. 45 C.F.R. 164.502(a)(1)(ii). "Health care operations" include, "population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment." See 45 C.F.R. 164.501. The wellness program in this case is a care management program, and therefore, covered entities may use PHI to identify individuals that may benefit from the program and send them literature about the program. A business associate may do this on behalf of a covered entity, or it may send PHI to a plan sponsor (assuming that the plan sponsor has amended its plan documents pursuant to 45 C.F.R 164.504(f)), so that the plan sponsor may identify individuals and send them a communication.

In addition, HIPAA's privacy rules exclude from the definition of "marketing" communications sent for "case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual." See 45 C.F.R. 164. 501. As a result, covered entities do not need to obtain individual authorization to use or disclose (or have their business associate's use or disclose) the PHI for this purpose.

Answer 6:
OCR agreed with the proposed answer, but noted that any PHI that went to the plan sponsor could not be used for employment purposes. If the PHI obtained stayed with the

business associate (ASO in this case) then OCR has less concern about this arrangement. To the extent PHI was going to the plan sponsor as the conduit of this information, adequate firewalls would need to be maintained. The information could be provided to a designated benefit representative of the plan sponsor as long as plan documents have been amended.

Question 7: The Company, which is a state-licensed insurance carrier, provides supplemental insurance policies which provide so-called "cancer-only," "heart-only," "personal injury-only" and "hospitalization-only" coverages. Under these policies, benefits are contingent upon a diagnosis of cancer, diagnosis of heart disease, personal injury or hospitalization, respectively. Thereafter, the policies provide cash payments, the amounts of which are pre-determined under the policy terms, directly to the insured individuals and without regard to the existence of other insurance upon the occurrence of events such as hospitalization, utilization of ambulances, specific treatments (*e.g.*, chemotherapy), traveling for treatment, *etc.*

The Company markets the policies as providing financial protection against unexpected loss. In other words, the policies are intended to provide income replacement in the event of personal catastrophe. The policy proceeds are generally far less than the cost of the medical procedures or expenses incurred in connection with the events which give rise to the payments. Policyholders are free to use the policy proceeds in any way they see fit. They are not required to use policy proceeds to pay expenses related to the events which gave rise to the payments.

Is the Company a "covered entity" subject to the Health Insurance Portability and Accountability Act's Administrative Simplification ("HIPAA") provisions?

Proposed Answer 7: No. For purposes of HIPAA, "covered entities" are health plans, health care clearinghouses, certain health care providers and prescription drug card sponsors under Part D of Medicare. The Company is clearly not a health care clearinghouse, health care provider or prescription drug card sponsor.

The Company meets the requirements for being a "health insurance issuer" (within the meaning of 45 CFR § 160.103) because it is licensed to engage in the business of insurance in a State. However, it is not a "health plan" (within the meaning of 45 CFR § 160.103) because it does not "provide[], or pay[] the cost of, medical care (as defined in Section 2791(a)(2) of the PHS Act, 42 USC 300gg-91(a)(2))."

Under Section 2791(a)(2) of the PHS Act, the term "medical care" means "amounts paid for --

(A) the diagnosis, cure, mitigation, treatment, or prevention of disease, or amounts paid for the purpose of affecting any structure or function of the body,

(B) amounts paid for [*sic*] transportation primarily for and essential to medical care referred to in subparagraph (A), and

(C) amounts paid for [*sic*] insurance covering medical care referred to in subparagraphs (A) and (B)."

The Department of Health and Human Services has recognized that the term "medical care" is "critical in making a determination as to whether a health plan is a 'health plan' for purposes of administrative simplification." See Preamble to the Final Regulations for the Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82461, 82578 (December 28, 2000).

Though certain payments under the policies may be made as a result of medical care, the Company and the policies do not "pay[] the cost of, medical care" within the meaning of the statute because the proceeds are not reimbursements for medical expenses and policyholders need not, and in fact typically do not, use them to pay medical expenses. Moreover, there is no direct relationship between the amount of the policy proceeds and the amount of medical expenses.

Answer 7:

OCR declined to answer the question at this time. They stated that it is difficult to give a simply yes or no answer as to coverage of this type of product, and generally they will not provide advisory opinion unless it is in the context of a specific complaint. All insurance products are different, and they are in the process of evaluating different types of income replacement policies. OCR requested information from the group on these types of products, and other similar products that may be commonly marketed to small employers.

Question 8: Life insurance is generally not "health plan" coverage subject to HIPAA's Administrative Simplification (AS) provisions. See 45 C.F.R. § 160.103 incorporating exclusions in 2791(c)(1). However, long term care (LTC) insurance coverage generally is considered to be a "health plan" for HIPAA AS purposes. See SSA §1171(1)(5)(G); 45 CFR § 160.103. The question presented is whether an accelerated death benefit (ADB) rider to a life insurance policy would be subject to HIPAA's AS provisions. The ADB benefit is offered by many plan sponsors and insurers and it provides per diem benefits for a covered individual who is chronically ill or terminally ill. Enacted as part of HIPAA, the ADB clarification under Section 101(g) of the Tax Code, makes it clear that a life insurance policy may offer an accelerated death benefit that is excludable from the recipient's gross income (e.g., as an advance on life insurance proceeds). This accelerated death benefit can be structured in one of two ways: (i) as a benefit for a "terminally ill" individual; or (ii) as a benefit that provides payment for long term care costs incurred by a "chronically ill" individual. A terminally ill individual is an individual diagnosed with a condition which can reasonably be expected to result in death in 24 months. A "chronically ill" individual is an individual is defined for ADB purposes as it is for LTC purposes, as an individual who cannot perform at least two activities of daily living. See Section 7702(B)(c)(2) of the Tax Code. Section 818(g) of the Tax Code (also enacted as part of HIPAA) specifically provides that for insurance taxation purposes ADB coverage is life insurance not LTC.

Proposed Answer 8:
An ADB rider to a life insurance policy is only a minor, additional benefit. The primary benefit in this situation is life insurance coverage. Based upon the fact that an ADB rider is only a supplemental, minor benefit under the life insurance policy and the fact that the Tax Code provides that ADB coverage is life insurance, a life insurance policy with an ADB rider is considered life insurance and is exempt from HIPAA's AS provisions.

Answer 8:

OCR agreed with the proposed answer. Unlike the types of products discussed in Question 7, the HIPAA privacy regulations specifically address life insurance and exclude life insurance from coverage under the HIPAA privacy regulations. OCR stated that the condition that triggers a payment under a life insurance policy does not change the character of the policy as a life insurance benefit, and therefore it is excluded from coverage under the HIPAA privacy regulations.

Question 9: 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 9: 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. 508(c)(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 9:
This question was not discussed at the May 2, 2006 meeting.

Question 10: This question is a follow up to a response to a question from 2005 (Question 6 from 2005). 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. Question 6 from 2005 asked whether the plan sponsor or business associate could use information obtained during a claims audit to terminate the coverage of an employee and/or dependent. OCR agreed with the proposed response that the information could be used to terminate coverage under the plan. As a follow up question, assume that the employer audits the plan and determines that an

employee has engaged in fraud, such as by obtaining controlled substances through fraudulent prescriptions. May the employer:

1. Terminate the employee's coverage under the group health plan until the employee enrolls in and successfully completes the employer's drug and alcohol rehabilitation program (assuming that the employer's drug and alcohol rehabilitation program is itself a group health plan subject to HIPAA)?

2. Advise the employee that the employer will terminate the employee's coverage unless the employee enrolls in and successfully completes the employer's drug and alcohol rehabilitation program? (The difference from situation 1, above, is that in this case coverage would not be terminated so long as the employee successfully completed the rehab program).

Answer 10:
Yes to both questions. Consistent with OCR's response to the question from 2005, if the plan can use PHI it has concerning fraud to terminate an individual's coverage, it can use the same information for other plan purposes, such as a requirement to participate in a rehabilitation program to continue coverage. OCR stated that this assumes that these are plan activities as distinct from employment activities. A plan investigation can result in plan actions (such as requiring participation in a rehab program of the plan), but not an employment action, such as termination of employment. PHI may flow from the employer to the plan, but not from the plan to the employer. Employers may have other means to assess and investigate employees, such as drug testing, that are separate from the group health plan. OCR did indicate that the plan could tell the employer that a particular person no longer has plan coverage.

Question 11: Are there any issues regarding HIPAA privacy concerning group health plans that HHS is currently discussing or evaluating where input from members of the ABA's Joint Committee on Employee Benefits would be of assistance? One area that has been raised for discussion is the movement toward electronic medical records. Recently some group health plans that have contracted with carriers to provide health benefits have noticed that some of these carriers are offering a service for participants that allow participants to request that their in-network lab results such as cholesterol and blood sugar test results be automatically stored and sent to a data management service so that participants may start to keep an electronic health record. This is a voluntary program. The data storage is free to the participant, and is available through arrangements made between the carrier and the data storage company. Group health plans are not involved in the arrangement to store the information, nor do they have access to any of the data stored. Does this raise any HIPAA privacy concerns for group health plans?

Answer 11:
OCR stated that if the data management were a service provided by the group health plan, then the carrier would be a business associate of the plan, and the PHI could be used by the carrier for this purpose. However, since this scenario does not involve data

management as a service of the plan, the carrier would need to get individual authorization to be able to disclose the information to a data management service.