American Bar Association

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

May 6, 2008

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 6, 2008. 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, through April 30, 2008, it has received over 35,500 complaints since April 2003. The volume of complaints has gone up every year. The resolution rate has gone up over the last year from 79% to 83%. From April 2003 through April 30, 2008, approximately 1,060 complaints have involved group health plans (including MEWAs). Many of the issues involved in complaints against health plans generally have involved the following 3 categories (1) misdirected communication (e.g. IT error) (2) inadequate separation between the plan and the employer, and (3) employees looking at plan information and using it for nonplan purposes.*

OCR stated that it has not yet imposed a civil money penalty because it has successfully obtained satisfactory corrective actions or agreements with covered entities in all investigations where there were indications of noncompliance. In a case of noncompliance where the covered entity does not agree to corrective action or other agreement that is satisfactory to OCR, penalties will be imposed.

Also through April 30, 2008, OCR has referred more than 431 cases to the Justice Department for review under the criminal penalty provisions of HIPAA. They also referred 231 cases involving HIPAA security to OESS in the Centers for Medicare and Medicaid Services. Some of these are joint investigations, OCR doing the HIPAA privacy investigation and OESS doing the HIPAA security investigation.

OCR pointed to other enforcement statistics available on their website at http://www.hhs.gov/ocr/privacy/enforcement/. These are updated monthly.

Question 2: Are there any plans to issue more formal or informal guidance on the HIPAA privacy rule, or to issue compliance assistance to help plans audit themselves?

Answer 2: *OCR mentioned guidance that they are working on with the U.S. Department of Education concerning the intersection of the HIPAA Privacy Rule and FERPA (The Family Educational Rights and Privacy Act)). Issues and questions concerning the interaction of FERPA and HIPAA privacy and how these two laws apply came up after the shootings at Virginia Tech. This guidance is to address these issues, as well as related questions the respective Departments have received over the years.*

No guidance is currently in the works regarding plan sponsors, but the following issues were discussed as areas where additional guidance would be helpful: wellness program issues; use of enrollment information; subpoena issues; personal representatives (e.g., step parents asking for PHI of children); best practices for business associates with infrequent access to PHI in securing PHI; complying with the minimum necessary rule; the "required by law" rules and whether Covered Entities violate the HIPAA Privacy Rule by choosing not to disclose information.

Deleted: ¶
¶

Question 3: Company Z has instituted a new voluntary wellness program for employees. Employees who wish to participate fill out an extensive health risk assessment (HRA) that asks questions about their current health, whether they smoke, how much they exercise, family health history, etc. Employees who fill out the HRA receive a report that discusses their possible health risks, provides written recommendations on how to reduce their health risk, and recommends following up with their personal healthcare provider for medical advice and treatment where necessary. Employees who fill out the assessment are given a $50 gift card that can be used at a local electronics store. This wellness program operates outside of the group health plan. No incentives are provided within the group health plan to participate in the program. Individual employees who are not enrolled in the group health plan can participate in the wellness program. The employer uses information from the HRA to develop wellness strategies that can be used to develop programs inside and outside of the group health plan.

The program is administered as follows: The employer itself distributes and collects the HRA and provides the completed HRA to an outside entity that prepares the employee report and sends it to the individual employee at their home address. The employer

receives a report with de-identified information that summarizes the health status of the group of employees that completed the HRA. Assume for the purpose of this question that the wellness program is not an "employee welfare benefit plan" as that term is defined under ERISA. Is the program covered by the HIPAA privacy rules such that the employer (plan sponsor) has obligations to protect the HRA information consistent with the HIPAA privacy rules?

Proposed Answer 3:

No. The voluntary wellness program is not a "health plan" as defined in section 160.103 of the Privacy Rule because it is not an individual or group plan that provides or pays for the cost of medical care. In addition, the program operates separately from the group health plan as an employer policy. Also, the program itself is not a "health care provider" since it does not provide medical care. It simply provides educational materials to individuals concerning their medical risks.

Answer 3: *OCR agreed that, assuming the wellness program is not an "employee welfare benefit plan" as defined by ERISA, and the program is offered by the employer and not as part of the health plan, the program is not subject to the HIPAA Privacy Rule. [OCR noted, however, that a separate evaluation would need to be done with respect to the outside entity hired to prepare the employee report to determine whether such entity is a covered health care provider.]*

Question 4: Company H has a fully-insured group health plan for its employees and their dependents. The company outsources its health plan enrollment function to an outside vendor. Employees enroll in their benefit coverage through this vendor. Company H has several hundred employees in Massachusetts. Massachusetts has a health reform law that requires certain employers to distribute and collect from certain employees an "Employee Health Insurance Disclosure Form." Employees who decline health coverage sponsored by Company H must fill out this disclosure form and return it to Company H. The form includes the following information:

- Name
- Social Security number
- Whether the individual is enrolled in the Company's group health plan
- If the person is not enrolled in the Company's plan, whether they have other health insurance

Company H has collected these forms from its Massachusetts employees, and is required under Massachusetts law to retain the forms for three years. Company H has designated an individual in the HR department in the Company's Massachusetts office to collect and keep these forms.

Are these completed disclosure forms considered PHI such that they are subject to HIPAA privacy protections?

Proposed Answer 4: No. The MA law places this requirement on employers not group health plans. As a result, the collection of the forms is an employer function not subject to HIPAA privacy. Furthermore, the information itself is collected from individuals who are not enrolled in the group health plan and could not be PHI.

Answer 4: *OCR agreed that the completed disclosure forms are not PHI subject to the requirements of the HIPAA Privacy Rule because the information is being collected and maintained by the employer and not the health plan.*

Question 5: The X Corporation has a retiree group health plan that consists solely of fully-insured medical benefits. Retirees choose among several insured plan options and inform specific individuals in X Corporation's Human Resources (HR) Department of their selection. The retiree provides the HR Department with the demographic information needed for enrollment purposes, including demographic information relating to dependents in cases where the retiree is enrolling in family coverage. The HR Department sends this enrollment information to the various insurance companies/HMOs either on paper forms or through secure electronic channels. If a retiree adds new dependents or drops coverage, the HR Department provides enrollment/disenrollment updates to the appropriate insurer/HMO. On a monthly basis, each insurer/HMO sends X Corporation an invoice for premiums due, along with a list of each retiree enrolled and the type of coverage (individual/family). X Corporation does not receive any claims information from the various insurers/HMOs. X Corporation covers the cost of the lowest cost plan option. If a retiree chooses a plan option with a premium higher than this set amount, X Corporation's Finance Department deducts the additional amount from the retiree's monthly pension check. Is the enrollment information that X uses to enroll/disenroll retirees in these insured plans PHI? Is the information described above that is sent by the insurers/HMOs to X Corporation each month PHI? Does X Corporation's receipt of this enrollment/premium information from the insurers/HMOS trigger any HIPAA privacy obligations on X Corporation's part?

Proposed Answer 5: The enrollment/disenrollment information sent by X Corporation to the insurers/HMOs is not PHI. X Corporation is performing these enrollment functions on behalf of its retirees and not on behalf of the group health plan. Enrollment information held by insurers/HMOs, as covered entities, is PHI, but the insurers/HMOs are permitted to disclose the type of enrollment and premium information described above to X Corporation for payment purposes. X Corporation may use this enrollment and premium information to deduct the retiree's premium share from pension checks, and in doing so, X Corporation is not performing any functions subject to HIPAA privacy requirements.

Answer 5: *OCR agreed that the enrollment information collected and sent by X Corporation to the insurers is not PHI. The information becomes PHI once the insurer has it, but the enrollment information can be disclosed by the insurer to the employer under 45 CFR 164.504(f)(1)(iii) (permitting the disclosure of enrollment information by a health plan to the plan sponsor) for the employer to use for any purpose, including*

payroll functions. The employer's use of this enrollment information is outside the scope of the HIPAA Privacy Rule.

Question 6: Same scenario as question 5, except X Corporation also has a program that will reimburse retirees for their Medicare Part B premiums. Individuals provide the Corporation with proof that they paid their Part B premium, and the Corporation then reimburses them by adding the premium amount to their pension check. Is the information that X Corporation collects to reimburse these premiums PHI? If so, is the X Corporation required to comply with HIPAA's administrative requirements, or can it take advantage of the special exception in section 164.530(k) of the privacy regulation?

Proposed Answer 6: X Corporation must comply with HIPAA's administrative requirements. It receives PHI as part of its administration of the benefit that reimburses Medicare Part B premiums. This information is neither enrollment information of the type described in Question 5, nor summary health information as defined in section 164.504(a)(it contains the names (and possibly other demographic information) of the retirees). As a result, the Corporation does not qualify for the special exception from HIPAA's administrative requirements.

Answer 6: *OCR stated that, based on the description, the information collected by the Corporation with respect to the Part B reimbursement did not appear to be PHI. If the reimbursement program is simply a payroll benefit provided by the employer and is not a benefit of the health plan, then the program and the information involved would not be subject to the requirements of the HIPAA Privacy Rule. If, however, reimbursement of Medicare Part B premiums is provided as part of the overall health plan benefits or activities, e.g., with respect to coordination of benefits for the plan, then such activity and the information involved is subject to the HIPAA Privacy Rule.*

Question 7: Company X has a self-insured group health plan that is administered by an insurance company. Company X does no internal plan administration other than forwarding a list of health plan enrollees to the insurance company. Company X wishes to improve the health of its employees by offering an incentive for employees to quit smoking. Employees who do not smoke will receive a premium holiday for the last 2 months of the year. Specifically, those who do not smoke will not have to pay their share of the cost of health coverage in November and December. The plan sponsor will pay the full cost for the coverage during these two months.

Company X administers this program by requiring employees to fill out a form during open season stating whether they smoke. If employees do not fill out the form, they cannot enroll in the health plan. This form is filled out by employees and given to human resource staff. Human resource staff then compiles a list of employees and their smoking status. The list is used to determine who will receive the premium holiday. HR staff works with payroll to make sure no employee contributions are deducted from the November and December paychecks of employees who qualify for the premium holiday.

The insurance company that administers the group health benefit is not involved in administering this smoker wellness program. This is done by the employer only. Is the list with the information concerning smoker status considered protected health information under HIPAA's privacy rules?

Proposed Answer 7: Yes. The Company collects this information in order to administer the premium holiday. Since the information is used for a plan administration purpose, it is protected health information. In addition, status as a smoker is health information. Since individual names are included, it is individually-identifiable.

Answer 7: *OCR disagreed with the proposed answer, in part. OCR indicated that the purposes for which the information is collected and how the information is used will determine whether the plan sponsor is functioning as an employer or as a plan administrator. To the extent the program is administered as a condition of health plan enrollment or eligibility for benefits, as it appears in the description above, it would appear the employer is performing a function on behalf of the plan, in which case, the information would be PHI. Similarly, if the premium holiday is administered as a health plan benefit, versus, e.g., a reimbursement program by the employer as in Question 5 above, then the employer is administering the program on behalf of the plan and the information would be PHI. If, however, the smoker wellness program is administered completely outside of the health plan benefit, and the information is not used for plan purposes, then the list is not PHI.*

Question 8: Company C (a company that produces widgets) wants to set up an onsite medical clinic in order to better control health care costs, increase worker productivity, and encourage employees to focus more on their health. The onsite clinic would provide more than treatment for minor injuries or first aid in case of accidents occurring during working hours. The clinic would provide primary health care including vaccinations, treatment of various health problems such as infections and injuries, diagnosis and treatment of conditions such as diabetes and hypertension, and mental health counseling services and referral. The clinic would be open to employees, their spouses and children who are enrolled in the Company's group health plan. The clinic would be integrated with the company's self-insured group health plan so that employees enrolled in the plan would have their clinic benefits covered (they would pay a co-pay for clinic visits).

The onsite clinic would be provided by a third party contractor of the employer. This third party is in the business of contracting with employers to provide onsite health care services. This third party would staff, manage, and operate the facility. It would administer payment of claims by working with the plan's third party administrator. The clinic would conduct standard transactions electronically.

Would Company C have any compliance obligations under HIPAA privacy with respect to this onsite clinic? If the Company owned and ran the clinic would the HIPAA obligations change?

Proposed Answer 8: If Company C outsourced the onsite medical clinic as described above, neither the Company nor the group health plan that it sponsors has any HIPAA privacy obligations. Onsite health clinics are not "health plans" under HIPAA because they are considered excepted benefits that are specifically excluded under the definition of health plan. See definition of "health plan" at 45 C.F.R. 160.103. In this case, even though the clinic may be an employee welfare benefit plan under ERISA, it is specifically excluded as a health plan under the HIPAA privacy rule. The third party contractor would not be a business associate of the group health plan because it is not providing services for a health plan. The third party contractor is itself a covered health care provider under HIPAA, and will have its own HIPAA obligations.

If the Company owned and ran the clinic it would be a health care provider subject to HIPAA privacy. Protected health information created and retained by the clinic must be used and disclosed only as allowed by the HIPAA privacy regulations. Firewalls would have to be established between PHI used and disclosed by the clinic and other information. If the Company does not designate itself as a "hybrid entity," the entire company (not just the clinic) would have to comply with HIPAA privacy. See section 164.103 (definition of hybrid entity), section 164.105, and 67 Fed. Reg. 53203-4 (8/14/02).

Answer 8: *OCR agreed that if the operation of the onsite medical clinic is contracted to an outside covered health care provider, the clinic would be a covered entity in its own right and the Company would not by virtue of such contracting become a HIPAA covered entity. Nor would the clinic be a business associate of the health plan as the mere activity by a health care provider of billing a health plan for health care services does not make the health care provider a business associate of the plan. Thus, neither the Company nor the health plan would have any Privacy Rule obligations with respect to the clinic. (Of course, the health plan, as a covered entity, would still have its own Privacy Rule obligations.)*

They also added, however, that in the situation where the Company owns and runs the clinic, it would be a HIPAA covered entity subject to the requirements of the Privacy Rule. In such case, as the main function of the company described above is non-health care related, it may be beneficial for the company to then become a hybrid entity so that the Privacy Rule would apply only to its health care clinic and not the entire Company.

Question 9: A group health plan agrees to participate in a research study designed to track the success of various types of smoking cessation programs. The data to be used is claims data, which includes PHI. Several other group health plans will also participate in the study. The study, which meets the criteria for research under the Privacy Rule, will be conducted by a university-based research center, the research protocols will be submitted to the University's IRB for approval, in accordance with the Privacy Rule, and the researchers intend to release their findings using summary data. As part of the approval process, a waiver of individual authorizations will be requested. See 45 C.F.R. § 164.512(i) (uses and disclosures for research).

In addition, the university-based research center, using the same PHI described above will provide each participating group health plan with various types of data analysis regarding its own participants that the plan will use for quality assessment and improvement purposes. Under the Privacy Rule, individual authorizations are not necessary for the plan to disclose the claims data to the university research center for this purpose since such disclosure is to carry out health care operations. See 45 C.F.R. §501 (health care operations).

The university research group has told each of the participating group health plans that its lawyers have concluded that a business associate agreement is not required between the university and the plans for either of these uses and disclosures. However, legal counsel for one of the plans disagrees and has asked for a business associate agreement to be executed between the parties covering both types of disclosures. Is a business associate agreement necessary?

Proposed Answer 9: As long as the group health plan's disclosure of PHI to the university researchers meets the definition of research under the Privacy Rule and the IRB approves the research plan, no business associate agreement is necessary to conduct the research. However, to the extent that the PHI disclosed initially for research is then used for another purpose (e.g., quality assessment and improvement of the group health plan), a business associate agreement is necessary since the group health plan is contracting with the university research center to carry out these functions on its behalf. See 45 C.F.R. §160.103 (definition of business associate).

Answer 9: *OCR stated that if the secondary uses of the data are planned for as part of the research, then these secondary uses should be considered by the IRB and covered by the IRB waiver for the research study. Otherwise, use of the data for the secondary purpose would not be consistent with the IRB waiver and the entity would be restricted from using the data for these other purposes unless it had a separate permission under the Privacy Rule. Thus, in these cases where the secondary use is not covered by the IRB waiver, a business associate agreement would be needed between the group health plan and the university research center for the center to carry out the quality activities on behalf of the group health plan.*

OCR also mentioned that an alternative to the IRB waiver and the business associate agreement is for the group health plan to disclose only a limited data set of PHI (that is, PHI with direct identifiers stripped) and enter into a data use agreement with the center for both the research and quality activities (to the extent fully identifiable information is not needed). See 45 CFR 164.514(e). Disclosure of a limited data set pursuant to a data use agreement for research and/or health care operations (e.g., quality studies) requires neither an IRB waiver of authorization nor a business associate agreement.

Question 10: A group health plan received an administrative subpoena from a government drug enforcement agency asking for all medical records on one of the plan

participants. The agency is conducting a criminal investigation, but it does not involve the plan participant. The group health plan is told that the criminal investigation does not involve the participant, but knows nothing else about the investigation. The agency refuses to provide the plan with any other information concerning the investigation. Is the plan required to provide the agency the information under HIPAA? Assume for the purpose of the question that the specific disclosure is not required by law.

Proposed Answer 10: No. All disclosures with respect to law enforcement are permissive disclosures; HIPAA does not require that the disclosure be made. In this instance the plan has no way to assess whether the disclosure is relevant and material, specific and limited in scope, or whether de-identified information can be used pursuant to the three part test in section 164.512(f)(1)(C) of the privacy rule. As a result, the plan may properly refuse to disclose the entire medical record. See also 65 Fed. Reg. 82681 to 82684.

Answer 10: *OCR agreed with the proposed answer, stating that disclosures by a covered entity for law enforcement purposes are permissive, not required, under the Privacy Rule. In addition, OCR further explained that absent the individual's authorization, court order, subpoena issued by a judicial officer or grand jury, or a statutory or regulatory disclosure requirement on the covered entity, the Privacy Rule would require that the covered entity obtain from the law enforcement agency, prior to disclosure, a written administrative request that states that the information requested meets the three-part test described above (relevant and material, specific and limited in scope, and de-identified information cannot be used). See 45 CFR 164.512(f)(1)(ii)(C).*