American Bar Association

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

May 4, 2010

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 4, 2010. 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 and security rules and changes made by the HITECH Act – particularly any such activities regarding group health plans. What compliance problems is OCR seeing with respect to group health plans?

OCR Answer 1:

OCR reviewed their latest statistics on enforcement that are available on their website. For example, since the April 2003 compliance date and through March 31, 2010, OCR has received 50,989 complaints and resolved 45,493 of these complaints. More than 10,515 of these complaints involved an investigation and some form of corrective action by the covered entity. From the compliance date to March 31, 2010, there have been 1,725 complaints involving group health plans including MEWAs. The most common complaints involved improper disclosure and lack of reasonable safeguards.

Concerning breach notice issues that have been reported to OCR, many have involved loss of a laptop or misdirected communications.

Through March 31, 2010, OCR also has opened 44 compliance reviews and closed 31 of them. Over 470 matters have been referred to the Department of Justice.

OCR is gearing up to exercise its new audit authority provided under the HITECH Act. OCR expects that audits will differ from compliance reviews. Compliance reviews are typically event or complaint driven, while the audit program will likely be a more structured program targeted at specific issues or types of covered entities.

State attorneys general have authority to enforce certain HIPAA requirements under the HITECH Act. As of this meeting, only Connecticut has brought a case under this new authority. OCR is working with the National Association of Attorneys General to develop a training program on HIPAA.

Question 2: What are your current plans to issue formal or informal guidance on the HIPAA privacy and security rule, especially concerning HIPAA privacy rule provisions in the Genetic Information Nondiscrimination Act of 2008 (GINA), and the American Recovery and Reinvestment Act of 2009 (HITECH Act)? What new responsibilities will OCR have concerning new Administrative Simplification provisions that are part of the health care reform law (the Patient Protection and Affordable Care Act of 2010, as amended by the Health Care and Education Reconciliation Act of 2010)?

OCR Answer 2:

OCR published a Notice of Proposed Rulemaking (NPRM) on July 14, 2010, to implement the changes to the HIPAA Privacy and Security Rules required by the HITECH Act. These proposed regulations cover business associate liability, the right to request restrictions, E-access provisions, the sale of PHI, marketing and fundraising, among other things. OCR stated that the issue of whether a new Notice of Privacy Practices will need to be provided by the covered entity is addressed in the NPRM.

OCR expects to finalize their proposed rule concerning the privacy provisions of the Genetic Information Nondiscrimination Act (GINA) in the coming months.

CMS is the lead on the new Administrative Simplification provisions that are part of the Patient Protection and Affordable Care Act.

Question 3: Will OCR issue an updated Model Business Associate Agreement this year that will include changes due to the HITECH Act?

OCR Answer 3:

OCR expects to issue updated sample business associate provisions at the time it publishes the final HITECH Rule. The NPRM includes discussion regarding business associate agreements going forward, including a proposed transition period for modifications to business associate agreements. OCR acknowledges that the breach notification rule could implicate the content of the business associate agreement and that

the covered entity and its business associates should be working out between themselves the mechanics of compliance with the breach notification rule.

There was a discussion about whether business associate agreements with attorneys would be different from agreements with other entities that administer benefits. OCR stated that they always contemplated that agreements would be specifically tailored for different types of business associates.

Question 4: The use of "administered" in the definition of the group health plan 50 participant exclusion in 45 CFR Section 160.103 is not defined. If an employer group health plan is insured, will this automatically mean that there is administration by the insurer and that the employer group health plan is not eligible for the 50 participant self-administered exclusion in 45 CFR Section 160.103? The preamble to the 12/28/2000 regulations provides: "The definition of "group health plan" is adopted from the statutory definition at section 1171(5)(A), and excludes from the rule as "health plans" only the few insured or self-insured ERISA plans that have less than 50 participants and are self administered." (65 Fed. Reg. 82461, 82576.) Could you clarify whether an insured plan could be subject to the 50 participant exception.

Proposed Answer 4: If an employer group health plan is insured, this automatically means that the insurer is performing some administration. Thus, an insured group health plan will never be eligible for the 50 participant self-administered exclusion in 45 CFR Section 160.103. Note that the "plan administration functions" definition discussed in the context of plan sponsor access in 45 CFR Section 164.504(a) is not the definition intended for use in evaluating the 50 participant exclusion. The 50 participant exclusion use of the word "administered" is a broader definition.

We note that the preamble of 12/28/2000 regulations provides: "The definition of "group health plan" is adopted from the statutory definition at section 1171(5)(A), and excludes from the rule as "health plans" only the few insured or self-insured ERISA plans that have less than 50 participants and are self administered." Although we recognize that this provision might be ambiguous, this excerpt does not imply that an insured plan might be self-administered for purposes of the 50 participant exclusion. It is only the self-insured plans that might meet the 50 participant exclusion.

OCR Answer 4:

OCR stated that this issue has not come up. Plans that have less than 50 participants and are self-administered are excluded from the definition of group health plan. As a general matter, OCR expects few plans to fall within this category and, with respect to small fully insured plans, OCR would presume that such plans are generally not self-administered. However, OCR would not categorically say that fully insured plans would never fall within the exclusion. It would be a fact-specific inquiry about whether the plan has (1) less than 50 participants, and (2) is itself conducting plan administration.

Question 5: Employer A contracted with Insurer Z to be the third party administrator of Employer A's self-funded group health plan and the insurer of Employer B's dental plan from 1994 to 1999. Employer A subsequently hires other providers. In 2005, Employer B acquires substantially all the assets of Employer A in an asset acquisition. In 2010, Insurer Z contacts more than 700 individuals who were employees of Employer A in 1997 to 1999 to inform them that a laptop has been stolen from Insurer Z and that the laptop contained the individual's name, address, Social Security number, and claim information. Does Employer B have any obligations under HIPAA's privacy and security regulations with respect to the stolen information? If instead of an asset acquisition Employer B acquired Employer A by means of a stock acquisition, would Employer B have any obligations under HIPAA's privacy and security regulations with respect to the stolen information?

Proposed Answer 5: If the acquisition is an asset acquisition and Employer B did not assume Employer A's liabilities, then Employer B has no obligations under HIPAA's privacy and security regulations with respect to the stolen information.

If instead the acquisition was a stock acquisition and Employer B assumed Employer A's liabilities, then it is likely Employer B does have obligations. If a violation of HIPAA's privacy or security rules occurs after the effective date of the relevant portion of HIPAA, then it does not matter when the protected health information was obtained before or after the relevant effective date. In other words, the HIPAA rules that are currently in effect apply to all protected health information no matter when the health information was gathered.

Employer B is not likely to have a business associate agreement with Insurer Z. Nevertheless, Employer B should contact Insurer Z and work to determine the scope of the breach. If Insurer Z has not provided notice to the affected 700 individuals, Employer B may be obligated to do so. Employer B is also obligated to notify HHS and a major media outlet.

OCR Answer 5:

OCR stated that it is not clear from the question what happened to the plan after the acquisition or what relationships remain between Employer A, Employer B, and Insurer Z. OCR stated that the HIPAA obligations fall on the plan and not the employer. Concerning the obligations of a business associate to a plan that no longer exists, OCR stated that under the HIPAA regulation's business associate agreement requirements, the obligations to protect protected health information that is not returned or destroyed continue as long as the protected health information is held by the business associate. If the relationship between Employer A and Insurer Z as a TPA preceded the HIPAA Rules, then the information from this relationship was not protected health information, there is no business associate agreement, and thus no HIPAA contractual obligation to protect the information.

Question 6: The Security Breach Notification rules define a "breach" as the acquisition, access, use or disclosure of protected health information in a manner not permitted under subpart E (the HIPAA privacy rule) which compromises the security or privacy of the protected health information. If a group health plan has otherwise complied with the HIPAA privacy rules (has adequate safeguards etc.) and yet someone steals data in hard copy containing protected health information (for instance, there is a break in to a facility and hard copy data containing protected health information that was locked in a file drawer is stolen by a third party), is this still considered a breach that would require a breach notice? For this question, assume that the breach poses a significant risk of financial, reputational, or other harm to the individual.

Proposed Answer 6: Yes, the definition of "breach" in the interim final breach notice rules does not require that there be a violation of the HIPAA Privacy Rule, but that the facts involve a disclosure of protected health information that is not expressly permitted by the Privacy Rule. Here the theft of PHI by a third party is clearly an improper disclosure under the privacy rule, although it may or may not be a violation of the Privacy Rule by the plan.

OCR Answer 6:

OCR stated that the trigger for the breach notice under the Breach Notification Rule is the impermissible disclosure under the HIPAA Privacy Rule, which is a violation. Even though the disclosure is due to the actions of a third party, the breach notice is still required.