**American Bar Association**

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

**May 5, 2009**

**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 5, 2009. 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 regarding group health plans. What kinds of complaints are you receiving with respect to group health plans?

**Answer 1**:

*OCR went through their enforcement activities to date, which include approximately 43,000 complaints received since the April 2003 compliance date through March 31, 2009, of which eighty six percent have been resolved. Twelve hundred plus complaints have been received that concern group health plans, including multiple employer welfare plans (MEWAs). The type of complaints against group health plans/health plans has been consistent. They include misdirected communications (including mass mailing errors), failure to update systems, failure to abide by a request for confidential communications, inadequate separation between the plan and the employer, sharing information with persons not identified in the plan documents, and the loss of unencrypted electronic media. Information on enforcement is available on the OCR website at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/index.html*

*OCR also mentioned recent resolution agreements entered into with CVS Pharmacy and Providence Health & Services, which required corrective action plans and payment of monetary amounts to resolve indications of noncompliance.*

**Question 2**: What are your current plans to issue formal or informal guidance on the HIPAA privacy 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)?

**Answer 2**:

*OCR stated that a Notice of Proposed Rulemaking (NPRM) for public comment will be issued soon on section 105 of GINA, with the preamble to the rule explaining the proposal and requesting comments.*

*Concerning HITECH, OCR mentioned that guidance on "unsecured protected health information" and a request for information (RFI) concerning breach notification standards were issued April 17, 2009. OCR issued this guidance and RFI jointly with the Office of the National Coordinator for Health Information Technology (ONC) and the Centers for Medicare & Medicaid Services (CMS). OCR will be issuing a number of regulations in the future under HITECH, including for breach notification, business associates, and updated enforcement. In addition, HITECH requires HHS to issue additional guidance in a number of areas, including for de-identification and minimum necessary.*

*OCR stated that there are staggered effective dates for various pieces of HITECH, but will try to do as much consolidation as they can to better ensure that all pieces fit together and to allow for more efficient compliance. Some of the regulations will require coordination with ONC and the Federal Trade Commission (FTC).*

**Question 3**: A corporation has a voluntary wellness program that consists of two parts: (1) a health risk assessment questionnaire (HRA), and (2) certain biometric tests. The wellness program is part of the corporation's self-insured group health plan. The program requests (but does not require) that an individual fill out the HRA. If they fill out the questionnaire, they will receive a fifty-dollar discount each month off their monthly premium contribution to the corporation's group health plan. The HRA consists of several questions concerning current health status as well as questions about the individual's family medical history.

The wellness program also requests (but does not require) that individuals undergo one or more of three biometrics tests (body mass index testing, blood pressure screening, and cholesterol screening). Individuals will receive a monthly twenty-dollar discount from their monthly premium contribution for each of the three tests that they take.

Information from the HRA and the results of the biometric tests are evaluated by a vendor of the health plan. The vendor provides a report to each individual who

participated in the wellness program discussing their possible health risks, providing written recommendations on how to reduce their health risk, and recommending follow up with their personal healthcare provider for medical advice and treatment where necessary. The vendor also provides a report to the employer providing information about the health status of the population in the group health plan that participated in the wellness program. The employer uses this to develop and target other wellness initiatives. The report contains de-identified information as defined under the HIPAA privacy regulations.

After the effective date of the Genetic Nondiscrimination Act of 2008, can the wellness program continue to ask questions in their HRA about current health status and family history? Can the program continue to request the three biometric tests? Is the plan required to update its privacy notice to include any requirements in GINA?

**Proposed Answer 3**: The plan is prohibited under GINA from requesting that participants provide information about family history in the HRA, since family history information is considered genetic information. Such information cannot be used under GINA for either an underwriting purpose or prior to enrollment in the plan. Since the family history information would be used to compute the contribution amounts under the plan, it is genetic information used for an underwriting purpose. Information about current health status is not genetic information if it is limited to information about current manifested medical conditions. Plans are not prohibited from including these types of questions in their HRAs.

Nothing in GINA prevents the plan from requesting the three biometric tests since none of these tests are genetic tests as defined under GINA.

Unless the current Privacy Notice includes a specific reference to the HIPAA privacy rule allowing plans to use protected health information for underwriting, there is no need to change the Privacy Notice.

**Answer 3**:

*OCR stated that the issue of what requests health plans are permitted to make to individuals under GINA is under the purview of the Departments of Labor, Treasury, HHS (CMS) and not OCR because the Privacy Rule and GINA Section 105 address only the permitted uses and disclosures of genetic information. OCR did agree, however, as a general matter based on the statutory language, that since family history is genetic information, health plans would be prohibited from requesting such information through an HRA for underwriting purposes or prior to enrollment.*

*OCR also agreed that the three biometric tests indicated are not genetic tests.*

*OCR stated that they will be putting out a proposed rule on the GINA changes to the HIPAA Privacy Rule, which will address related issues with the HIPAA notice. OCR*

*stated that the GINA changes are a change to the permitted uses and disclosures for health plans under the HIPAA Privacy Rule, and the Privacy Rule does require that plans provide notice to individuals covered by the plan within 60 days of a material change. OCR stated that they were interested in comments on the best way to inform individuals of the change in a way that may minimize the burden of reissuing the Privacy Notice.*

**Question 4:** The group health plan of employer Z contracts with a disease management (DM) company to implement a DM program for its group. Part of the program involves targeting people with a family history of diabetes for additional benefits such as diabetes-related counseling and education services. This is done by requesting the information through a questionnaire and/or asking individuals over the telephone about family history who have been identified through review of claims data. Those enrolled in the DM program do not receive any premium or cost-sharing adjustments for participating. Can the plan continue to target individuals in this way after the effective date of GINA?

**Proposed Answer 4**: Yes, although the plan is requesting information about family history, it is not using this information for an underwriting purpose or prior to enrollment in the group health plan. The information is not being used to calculate premiums, and it is not being used to determine eligibility for group health plan (although it is used to determine eligibility for the DM program).

**Answer 4:**

*As above, OCR stated that the issue of what requests health plans are permitted to make to individuals under GINA is under the purview of the Departments of Labor, Treasury, HHS (CMS) and plans should look to these agency regulations for clarification on this issue. The HIPAA Privacy Rule regulates the use and disclosure of genetic information. OCR noted, however, that the definition of underwriting in GINA is broad and includes determinations of eligibility for or determination of benefits under the plan, coverage, or policy.*

**Question 5**: An employer has a fully insured group health plan. The plan has a 12-month preexisting condition exclusion and otherwise complies with the HIPAA portability requirements concerning preexisting condition exclusions. To implement the preexisting condition exclusion the plan requests that individuals enrolling in the plan fill out a questionnaire containing questions about current health status and family medical history of cancer or heart disease. Does GINA prohibit the plan from requesting this information?

**Proposed Answer 5**: The plan is prohibited under GINA from requesting that participants provide information about family history in the questionnaire, since family history information is considered genetic information. Such information cannot be used under GINA for either an underwriting purpose or prior to enrollment in the plan. Since

the family history information would be used to apply a preexisting condition exclusion under the plan, it is genetic information used for an underwriting purpose. Information about current health status is not genetic information if it is limited to information about current manifested medical conditions. Plans are not prohibited from including these types of questions in the questionnaire.

**Answer 5**:
*Subject to the caveat that the issue of what requests health plans are permitted to make to individuals under GINA is under the purview of the other agencies, OCR agreed with the proposed answer with respect to the use and disclosure of genetic information, such as family history, for an underwriting purpose.*

**Question 6**: The additional civil monetary penalties (CMP) added under the HITECH Act provide for a tiered increase in the amount of CMPs under the following three categories, (1) violations by those that did not know and exercising reasonable diligence could not have known of the violation, (2) violations due to reasonable cause and not willful neglect, and (3) violations due to willful neglect. Is the maximum CMP amount available at tier levels (1) and (2) $50,000 for each violation with the total amount imposed on a person for violations of an identical requirement during a calendar year not to exceed $1,500,000?

**Answer 6**:

*OCR stated that it appears that the statute provides for a maximum penalty at the first two tiers of $50,000 for each violation, not to exceed $1,500,000 for all violations of an identical requirement per calendar year. OCR is in the process of conforming the enforcement regulations to these new statutory provisions and will provide its interpretation in those rules.*

**Question 7**: The HITECH Act appears to require that business associates comply directly with the provisions in section 164.504(e) of the HIPAA privacy regulation, and that business associate agreements be revised accordingly. Are plans required to amend all business associate agreements prior to the effective date? Are business associates required to have written privacy policies and procedures, a privacy official and all of the other administrative requirements provided in the HIPAA privacy regulations?

**Answer 7**:

*OCR offered no specific guidance on the business associate issues from the HITECH Act other than to state that regulations would be issued concerning these business associate requirements, with an opportunity for public comment, prior to the effective date.*