



ALTHOUGH THE FOCUS IN WASHINGTON IS ON CAPITOL HILL—WITH CONGRESSIONAL debate on healthcare and, to a lesser extent, financial regulatory reform sucking up all of the oxygen—the work of the bureaucracy continues.

The Departments of Labor and Health and Human Services have issued guidance to clarify and ease compliance with security breach notification requirements under the Health Insurance Portability and Accountability Act (HIPAA).

After publishing guidance on the rule in July 2008, Labor recently issued supplemental guidance on the 2009 Schedule C fee reporting

guidelines. These FAQs cover a number of issues of interest to Council members.

■ The guidance says there is no

specific date for required written disclosures to plan administrators. However, in certain circumstances, information is required to a plan administrator within 120 days after the end of a plan year. In other cases, disclosure should be provided by whatever date has been agreed upon with the administrator. Disclosure must be made well enough in advance of the Form 5500 filing to provide the administrator with enough information for a complete, correct filing.

■ Disclosure must be specific and identify the services for which the broker is receiving indirect compensation. If that is impossible, be specific about compensation for one or more funds.

■ An investment advisor whose disclosure meets the requirements of the securities laws would have to provide additional disclosures to meet the requirements of the alternative reporting option for eligible indirect compensation.

■ Group health plans and other welfare benefit plans required to file a Schedule C, are subject to indirect compensation reporting requirements.

■ A fee on a per claim basis for a health plan would be considered

charged on a transaction basis for Schedule C. Fees charged for benefit eligibility inquiries, claim status request and response, and other similar fees could be treated as transaction-based fees.

■ Fees on a mutual fund prospectus, such as 12b-1 fees and shareholder servicing fees, are viewed as being charged against the mutual fund assets and reflected in the value of the investing plans' shares for Schedule C.

■ Commission payments and other agent and broker compensation in connection with placement or retention of a general account investment contract is reportable compensation to the recipients. Agent and broker insurance fees and commissions in connection with a plan's purchase of or investment in an insurance contract that are reportable on Schedule A do not need to be reported on Schedule C.

■ Non-monetary compensation of "insubstantial value"—such as coffee mugs and calendars—are not reportable. Similarly, meals, entertainment and similar gifts are not reportable if the amount of the gift or the status of the recipient is not dependent on the recipient's position with an ERISA plan.

HIPAA SECURITY BREACH NOTIFICATION REQUIREMENTS

The American Recovery and Reinvestment Act of 2009 made changes to the privacy and security provisions of HIPAA that require covered entities and business associates who handle personally identifiable health information to notify the public when security breaches occur. HHS has issued guidance on "best practices" for securing information. Compliance with these best practices provides a safe harbor from the security breach notification requirements. Most notably,

these best practices include use of encryption to secure electronic personally identified health information that is either stored or being transmitted between parties.

The government does not endorse any specific practice for storing or transmitting paper records. It does, however, recommend that entities ensure that personal data in destroyed records cannot be read or reconstructed. For electronic records, use standards created by the National Institute of Standards and Technology (NIST).

■ Stored records should be encrypted. See NIST Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices*.

■ Records being transmitted should be encrypted in compliance with Federal Information Processing Standards 140-2. See NIST Special Publication 800-52, *Guidelines for the Selection and Use of Transport Layer Security Implementations*; Special Publication 800-77, *Guide to IPsec VPNs*; or Special Publication 800-113, *Guide to SSL VPNs*.

■ Records being disposed of should be cleared, purged or destroyed consistent with Special Publication 800-88, *Guidelines for Media Sanitization*.

If insurance agents and brokers are unable or unwilling to utilize encryption for storing or transmitting electronic information, they will be required to notify affected individuals and the federal government if there is a breach. To minimize this risk, agents and brokers may wish to ensure they avoid handling the information.

Oops!

New rules make disclosure of compensation and client information a very risky business.

SINDER, A PARTNER AT STEPTOE & JOHNSON, IS CIAB GENERAL COUNSEL. ssinder@steptoe.com FIELDING IS OF COUNSEL AT STEPTOE & JOHNSON. jfielding@steptoe.com BOLTON IS OF COUNSEL AT STEPTOE & JOHNSON. rbolton@steptoe.com