BUSINESS NOTES

October 2001

C The Effect of New HIPAA Privacy Regulations on Employer Health Plans. The new privacy regulations issues under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) will soon require all employers to make significant changes to health plan documents, contracts, and administration of plan benefits. Employers will also learn that the HIPAA privacy rules will affect both self-insured and fully-insured health benefit plans.

The HIPAA privacy regulations were issued by the U.S. Department of Health and Human Services on December 28, 2000. These regulations apply to the following types of healthcare-related entities: (i) Health Plans; (ii) Health Care Clearinghouses; and (iii) Healthcare Providers. The general rule in the privacy regulations is that entities covered by the regulations may not use or disclose individually identifiable health information unless either the entity has obtained the appropriate form of permission from the patient or the use or disclosure is expressly allowed by the HIPAA privacy regulations. The HIPAA privacy regulations became effective on August 14, 2001, and Health Plans must comply with the privacy regulations by April 14, 2003.

Employers are not by themselves a covered entity under the HIPAA privacy rules; however, most employers have components such as fully-insured or employer-sponsored health plans that are subject to the privacy rules. Such employers are deemed hybrid entities by the privacy regulations. Thus, the HIPAA privacy regulations will affect the use and disclosure of an employee's or dependent's health information by the health plan component of an employer.

The actual affect of the HIPAA privacy regulations on employers will depend on both the type of plan (e.g., self-insured and self-administered, self-insured with a third-party administrator, and fully-insured) and by the volume and type of health information received by the Health Plan or the Health Plan sponsor. For example, employers that self-insure and self-administer their health plans must comply with all of the administrative requirements under the HIPAA privacy regulations for covered entities.

The administrative requirements of the HIPAA privacy regulations require affected employers to: (i) appoint a Privacy Official and complaint contact person; (ii) adopt specific policies to ensure compliance with the privacy regulations; (iii) train employees on the privacy policies adopted by the employer; (iv) adopt certain safeguards to protect the privacy of health information; (v) create a process to receive and address complaints concerning the employer's privacy practices; and (vi) enforce disciplinary sanctions against employers for violation of the employer's privacy policies.

Continued on back

Many employers with fully-insured health plans will surprisingly need to comply with the above listed administrative requirements of HIPAA *unless* they make certain changes to the health information they receive from their health plan or health insurance carrier. The HIPAA privacy regulations provide that a "group health plan" is not subject to the HIPAA administrative requirements only if the plan meets the following criteria:

(1) the plan provides benefits "solely" through an insurance contract with an insurer or HMO; and

(2) the plan does not create or receive health information, except for: (i) "summary health information;" or (ii) information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from an insurer or HMO.

Generally, group health plans receive more than "summary health information" or member enrollment data from their insurers. "Summary health information" is defined broadly in the HIPAA privacy regulations to include: (i) claims history; (ii) claims expenses; or (iii) type of claims experience by individual employees or dependents. The regulations require that summary health information be stripped of all personal identifiers (e.g., name, address, social security number, and phone number) except for the 5-digit zip code. Thus, unless information received by employers from health insurers is stripped of all of these personal identifiers, then the receipt of such information will cause employers to be subject to the administrative requirements in the privacy regulations.

Employers with a fully-insured group health plan should review the information currently received from their health insurers to determine if this information contains the personal identifiers listed in the previous paragraph. If an employer must continue receiving this information, then it might consider asking the health insurer to de-identify the information by deleting all personal identifiers to turn this information into "summary health information" as defined in the HIPAA privacy regulations.

Clay J. Countryman, (225) 389-3729; E-Mail: clay.countryman@keanmiller.com