

APPLICABILITY OF HIPAA TO PARTIALLY SELF-FUNDED HEALTH PLANS

Susan J. Freed

It is common practice for employers who sponsor fully-insured health plans with high deductibles or out-of-pocket maximums to subsidize a portion of the deductible or out-of-pocket maximum. For example, the employer purchases a fully-insured policy with a \$1,500.00 deductible. The employer then funds \$1,000.00 of the \$1,500.00 deductible so the employee has, in effect, a \$500.00 deductible. This practice is considered a self-insured benefit plan. Although this precise situation has not yet been addressed by HHS, it appears this type of plan would be considered a "health plan" subject to the HIPAA privacy regulations.

Generally, self-insured health plans are subject to the HIPAA privacy regulations. However, there is an exception for self-insured health plans with fewer than 50 participants that are self-administered. Therefore, if an employer has fewer than 50 participants in its group health plan and the employer self-administers the subsidized deductible/out-of-pocket maximum, the HIPAA privacy regulations would not apply. If, however, the employer does not self-administer the plan or has 50 or more participants, the plan will need to comply with the following requirements:

- Provide participants with the right to access, amendment and accounting;
- Prepare a privacy notice and provide the notice to participants;
- Designate a privacy officer and contact person;
- Implement policies and procedures to comply with HIPAA;
- Train its workforce dealing with plan administration on its policies/procedures;
- Establish reasonable safeguards to secure protected health information;
- Implement a complaint procedure for individuals who wish to file complaints;
- Design disciplinary procedures and sanctions for employees who violate HIPAA policies;
- Mitigate any damage that might occur from the improper use/disclosure of protected health information;
- Refrain from intimidating or retaliating against individuals exercising their HIPAA rights;
- Refrain from asking individuals to waive their HIPAA rights;
- Enter into Business Associate Agreements with all business associates;
- If the plan sponsor will have access to protected health information, amend the plan document to incorporate amendments required by HIPAA and obtain plan sponsor's certification.

The employer, as plan sponsor, is responsible for ensuring that the plan complies with the HIPAA regulations. The employer will be considered a "hybrid entity" so that only those employees whose duties require protected health information will need to comply with the regulations and be trained on the employer's confidentiality policies/procedures.

The employer may also contract with a third party administrator ("TPA") to handle many of the HIPAA requirements; however, the plan will ultimately be liable under the regulations for any failure of the TPA to comply with the regulations. If an employer chooses to contract with a TPA to perform plan administration and its HIPAA requirements, a detailed Services Agreement should be in place with a corresponding Business Associate Agreement.

The compliance date for health plans is April 14, 2003; however, small health plans have an additional year to comply. Small health plans are health plans with less than five million dollars in receipts. For partially self-insured plans, "receipts" will equal the amount of premiums paid under the fully-insured portion of the plan in the last full fiscal year plus the amount of claims paid under the self-insured portion of the plan in the last full fiscal year. If that number is less than five million, the plan has an extra year to comply.