

HIPAA Security For Small Group Health Plans

The final security rules released in 2003 under the Health Insurance Portability and Accountability Act (“HIPAA”) require small group health plans to protect electronic patient information. Self-administered plans with fewer than 50 participants are exempt from the security rules. Non-exempt small group health plans must comply by April 20, 2006. (Large group health plans were required to comply by April 20, 2005.) A “small” group health plan is a plan with annual premiums (insured plans) or claims paid (self-insured plans) under \$5 million. Plans covered by the security rules include health FSAs, HRAs, medical reimbursement plans, and insured plans. If your group health plan had to comply with the HIPAA privacy rules, it is most likely required to comply with the security rules as well. While the security rules apply to group health plans, the employer sponsoring the plan is generally responsible for ensuring the plan’s compliance with the rules, and may have HIPAA obligations of its own through plan amendments required by HIPAA.

Example: Suppose an employer maintains a fully insured group health plan and a health FSA administered by a TPA. What are the plan’s and employer’s obligations under the security rules?

1. Fully insured plan: If the plan and employer do not create or receive “protected health information” (“PHI”) other than summary health information and enrollment information, then the plan and employer may have no obligations under the HIPAA security rules, and have only very limited HIPAA privacy obligations. “Summary health information” consists of employer-wide information about claims history, plan expenses and similar information useful for making plan design decisions.

2. Health FSA: Because the health FSA is not self-administered, it must comply with the security rules. Accordingly, the TPA will need to execute a business associate agreement, and the plan will need to be amended to require the employer to comply with certain security obligations. The exact nature of the plan’s other security obligations depends on the particular circumstances. However, as a practical matter the plan’s and employer’s security obligations will be reduced to the extent the TPA handles the day-to-day operations of the plan and the plan and employer receive little if any PHI.

The security rules require plans to maintain administrative, physical, and technical safeguards to ensure the integrity, confidentiality, and accessibility of electronic protected health information (“ePHI”). ePHI consists of health information that is created, maintained, received, or transmitted in electronic form and which identifies or reasonably could be used to identify an individual. “Electronic form” includes diskette, CD, and computer hard drive. It does not include FAX or voicemail, but does include faxback and voice response systems. Even if the plan does not itself create, maintain, receive, or transmit ePHI, the security rules apply if a business associate, such as a third party administrator, does so for the plan.

Plans should act now to ensure compliance by the 2006 deadline. Penalties for violating the security rules include fines of up to \$100,000 and up to five years in jail for improper use,

acquisition, or disclosure of ePHI, and fines of up to \$250,000 and up to 10 years in jail for use, acquisition, or disclosure with intent to sell or use ePHI improperly.

Compliance steps could include the following:

1. Amend Plan documents. Plan documents must be amended to include language specific to ePHI and the security rules.
2. Update business associate agreements. Contracts with business associates must contain provisions assuring that the business associate will safeguard ePHI. Business associate agreements drafted for the privacy rules likely do not contain the required security language, and thus should be reviewed and amended if necessary.
3. Designate a security official. If desired, the same person may serve as both the HIPAA privacy and security official.
4. Organize a committee. Complying with the security rules will likely require that the security official, management, staff, and technology staff or consultants work together to develop and implement a compliance plan.
5. Learn the security rules.
6. Complete a risk analysis. Plans must complete a risk analysis of the potential vulnerabilities to ePHI held by the plans. Most employers already provide some level of security for their electronic information. The security rules require employers to compare and contrast their existing security measures with the requirements of the security rules, and to plug any gaps.
7. Develop compliance and contingency plans and adopt policies and procedures. Plans must protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI and unauthorized use or disclosure of the information. This includes preparation for national and natural disasters.
8. Train employees. Plans must ensure compliance with the security rules by employees. Plans must implement a security awareness and training program for all employees.
9. Secure ePHI and implement policies and procedures. Plans must develop measures to secure ePHI in their custody and when it is in transit. Plans must protect against any reasonably anticipated uses or disclosures of ePHI that are not permitted by the security rules.
10. Review and document compliance. Documentation of compliance with the security rules must be kept for at least six years.
11. Conduct periodic reviews of technology, policies and procedures, implementation, and staff compliance. Train new staff. Periodically re-train staff.

As with the privacy rules, complying with the security rules will require a significant effort by organizations that sponsor group health plans. Each organization should consult its own legal

counsel or take other steps to determine whether and how HIPAA applies to them. Companies should act promptly to ensure compliance by the April 20 deadline.

This article is for general information purposes only. Nothing in this article is intended to be or should be construed to be legal advice. If you would like assistance with HIPAA security rules, please contact Jeff Kirtner.