Critical Care for Compliance: Focus on HIPAA Security

Last year, the Office of Civil Rights ("OCR"), part of the Department of Health and Human Services, announced that it would begin the second phase of its audit program in 2015. During the second phase, selected covered entities will be audited for compliance issues under the Privacy Rule, the Security Rule, or the Breach Notification Rules, but not all three. Of the three areas of focus, compliance with the Security Rule is often the most overlooked, and thus the requirement that is most likely to trigger compliance issues and penalties. However, even though this article will focus on potential issues with respect to the Security Rule that covered entities, such employer-sponsored health plans, may want to consider, they must comply with all three requirements. Will your organization be able to provide a healthy dose of security protection for your health plan’s protected health information and avoid penalties?

1. **Appoint a Security Officer for your plan.** Under the HIPAA Security Rule administrative safeguards requirements, employer-sponsored health plans must identify a security official (often called a “Security Officer”) who is responsible for the development and implementation of the plan’s HIPAA Security policies and procedures. Unlike the requirement to designate a Privacy Officer, the requirement to designate a Security Officer applies to all employer-sponsored health plans subject to HIPAA, including employer-sponsored group health plans that provide benefits only through health insurance issuers or HMOs and that do not create or receive protected health information (“PHI”) other than summary health information or enrollment/disenrollment information. Has your organization appointed a Security Officer for your health plan?

2. **Provide long-term care for Risk Analysis.** A significant percentage of the recent Resolution Agreements entered into by the OCR have identified one key missing instrument in the offending employer’s medicine bag – a well-documented Risk Analysis. Employer-sponsored health plans must conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic Protected Health Information (“ePHI”) held by the plan. However, many plans skip this crucial step or fail to update their existing Risk Analysis when either a change in operating environment or in requirements occurs. The Risk Analysis is the cornerstone to HIPAA Security compliance. Failure to either conduct or update a Risk Analysis not only leaves an organization vulnerable to undetermined risks (such as theft of ePHI), but it also leaves an organization open to penalties of up to $1.5 million per year for each year that it failed to conduct or update a Risk Analysis. Does your health plan have a current and well-documented Risk Analysis?
Employers should carefully evaluate their health and welfare plans to determine if they are in compliance with both federal and state law. If you have any questions about one or more of the Critical Care concerns for 2015 listed above or would like additional information on how Gallagher constantly monitors laws and regulations impacting employee benefits and supports employers in their compliance efforts, please contact your GBS representative or click here.

The intent of this analysis is to provide you with general information. It does not necessarily fully address all your organization’s specific issues. It should not be construed as, nor is it intended to provide, legal advice. Questions regarding specific issues should be addressed by your organization’s general counsel or an attorney who specializes in this practice area.