BURR ARTICLE

So, Are You REALLY Compliant With HIPAA?

By Debra Lee Mackey

Reprinted with Permission from the *Birmingham Medical News*

As covered entities under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), healthcare providers are intimately familiar with the strict privacy and security requirements imposed on them by HIPAA and the importance of full compliance. Measures taken over the years to ensure compliance have become ingrained in daily practice, routine to employees, so HIPAA no longer keeps providers up at night. Check. Done. Right?

Hopefully. Maybe. What else is there?

If you are an employer, you may sponsor a group health plan to benefit your employees and their dependents. Group health plans are also covered entities under HIPAA. This article provides an overview of how the HIPAA privacy and security rules apply to group health plans. The breach notification and transaction standards apply to group health plans as well, but are beyond the scope of this article.

Privacy and security protections similar to those that apply to your patients' protected health information ("PHI") apply to the PHI of participants in group health plans offered to your employees. The degree to which a group health plan must provide these protections depends on how the plan is funded and whether you or your employees have access to participant PHI that is maintained by the plan.

If your group health plan is fully insured, you may be able to avoid HIPAA compliance, shifting the burden to the insurance carrier instead. If your plan is self-insured, you can't avoid responsibility for HIPAA compliance altogether. Again, the degree of your compliance burden depends on the information to which you have access. Note that the source of the PHI is key. HIPAA compliance is triggered when the access to PHI is from the plan. If the PHI is received directly from the employee or under an authorization from the employee, the HIPAA protections do not apply.

You must implement measures to ensure the privacy and security of your employees' and dependents' PHI in the group health plan similar to those in place to ensure the privacy and security of your patients' PHI. Even though your group health plan is the covered entity, it is highly unlikely that the plan has any employees, thus the plan is unable to act on its own. As sponsor of the plan, you or your employees must act on the plan's behalf and perform the functions of the plan (or hire a third party to perform them). If you or your employees perform any administrative functions for the plan, you likely receive PHI.

The first step to ensuring compliance with these HIPAA obligations is to identify your group health plans. Note that a group health plan for HIPAA privacy and security is defined more broadly than for HIPAA portability (i.e., the creditable coverage rules). The following types of plans are subject to

HIPAA privacy and security: major medical (e.g., your ACA compliant plan); dental and vision plans (including limited scope plans that are exempt from the portability rules); health flexible spending account; HRA; high-deductible health plan; retiree medical; and discount for medical services provided by you to employees and their dependents. Fixed indemnity and specified disease insurance and EAP/wellness programs may or may not be a group health plan, depending on the particular benefits provided. Small, self-administered plans are exempt — plans for which fewer than 50 employees (or former employees) are eligible to participate that are fully self-administered by the sponsoring employer. Self-administered refers to the actual performance of administrative functions, not necessarily the entity named as the plan administrator. An insured plan does not qualify for this exemption.

The second step is to identify how the group health plans are funded. Are they fully insured, fully self-insured, or partially insured and partially self-insured? As noted above, the HIPAA obligations are greater for self-insured plans, and generally minimal for fully insured plans.

The third step is to determine the type of information to which you or your employees have access. If you do not receive any PHI from the plan, you have no obligations. Even if you do not ordinarily receive PHI, the compliance obligation is triggered by the right to access. Employers frequently receive basic information that does not trigger these obligations. Receipt of enrollment/disenrollment information is not PHI. Receipt of summary health information solely for purposes of obtaining premium bids or for amending or terminating the plan is not PHI. Receipt of de-identified information is not PHI. However, when you receive or have access to PHI for plan administrative functions (treatment, payment, and healthcare operations), that triggers compliance. Note that a plan is not allowed to share PHI with the employer for any purpose other than the performance of these administrative functions.

Once you determine that you have access to PHI, what are your primary privacy compliance obligations? You must comply with the use and disclosure restrictions, inform participants of their privacy rights, and implement administrative requirements. These obligations are accomplished by:

- Naming a Privacy Officer;
- Preparing and distributing a Notice of Privacy Practices;
- Amending group health plans and implementing amendments;
- Establishing policies and procedures designed to ensure compliance;
- Entering into business associate agreements with third parties who receive PHI; and
- Training your workforce.

Most of these are very similar to your obligations as a provider, but two are unique to plans or implemented differently. These are summarized below.

Notice of Privacy Practices. For a fully-insured plan, the primary notice obligation is on the insurance carrier. If the employer's access is limited to summary health information, enrollment/disenrollment information and de-identified information, a separate notice for the plan is not needed. If the employer has access to any PHI, a separate notice is required, but it need not be distributed except upon request. A self-insured plan must always issue its own notice. The notice must be provided upon enrollment to individuals covered by the plan and every three years they must be told how to request a copy of the notice. The notice must also be provided upon request to anyone who requests it.

Plan Amendment. PHI may be shared with you and your employees only if the group health plan sets forth the permitted uses and disclosures of PHI, which must be limited to the administrative functions performed by the employer for the plan. If the plan does not contain this information, a plan amendment is required. As sponsor of the plan, you must provide a written certification to the plan that the plan has been so amended (or complies) and further state that as sponsor of the plan you agree to the terms of the amendment. Finally, the amendment must require that a firewall be established between those employees who have access to PHI and those who do not have access.

If you store, receive or transmit any PHI received from the plan electronically, security compliance is required as well. The security obligations are primarily related to information technology and the proper use of that technology. These obligations are accomplished by:

- Naming a Security Officer;
- Amending group health plans and implementing amendments. The amendment must require the employer to undertake four security related obligations: implement administrative, physical and technical safeguards; establish a security firewall: require compliance by agents and subcontractors; and establish a mechanism to report security incidents;
- Establishing policies and procedures designed to ensure compliance;
- Amending the business associate agreement with any business associate that stores, receives or transmits PHI electronically; and
- Training your workforce.

This article has presented a general overview of HIPAA privacy and security for group health plans. The key takeaway: educate healthcare providers that their HIPAA obligations may extend beyond their medical practice to group health plans offered by the provider to employees, encouraging them to undertake a self-audit to determine if any sponsored group health plans are subject to these HIPAA rules, and if so, whether the HIPAA obligations are being met.

Debra Lee Mackey
Counsel Birmingham Office
Phone (205) 458-5484
E-Mail dmackey@burr.com

Debra Mackey serves as counsel in the Health Care Industry Group at Burr & Forman LLP and has extensive experience advising clients on health benefit program issues.