Proceed With Caution

Does HIPAA Apply to Your Business?

BY GABRIELA SANCHEZ AND JEFF C.D. BRECHT

Even if your business is not in the health care industry, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as updated by the Health Information Technology for Economic and Clinical Health Act (HITECH Act), may impact your workplace. Here's why: HIPAA's rules protect individually identifiable health information held by "covered entities" and their "business associates." HIPAA protected health information is commonly called PHI. A "covered entity" under HIPAA includes health care clearinghouses, health plans and most health care providers (but not employers in their capacity as employers). A "business associate" under HIPAA is a person or entity that performs services for covered entities involving access to PHI. If your business sponsors a group health plan that has at least 50 members and is not self-administered, then your plan is likely a "covered entity" under HIPAA, even though your business is not. That means that even though records maintained by your business solely in its role as an employer are exempt from HIPAA, the PHI that your group health plan shares with your business (as a plan sponsor) to perform group health plan functions is still covered by HIPAA.

In fact, if your plan is a HIPAA-covered entity, then your business (as a plan sponsor) should not even receive PHI from your HIPAA-covered plan unless your business first provides the plan with a certification of HIPAA privacy and security compliance. Among other things, the certification must state that your business (plan sponsor) will: 1) not use or further disclose the PHI other than as permitted or required by the plan documents or as required by law; 2) ensure that any agents to whom you provide the PHI will abide by the same restrictions applicable to your business; and 3) not use the PHI for employment-related actions and decisions.

So, what steps should your business take as a sponsor of a HIPAA-covered health care plan? At a minimum, it should:

If your business sponsors a group health plan that has at least 50 members and is not self-administered, then your plan is likely a "covered entity" under HIPAA, even though your business is not.

- Make sure an individual has been appointed as the compliance person in charge of making sure that you have written policies and practices in place to confirm interactions with the plan and receipt, and that treatment of PHI are HIPAA compliant;
- Make sure members of your workforce who may receive PHI from the plan are properly trained to protect and use PHI;
- Make sure your workforce is properly trained to immediately report any actual or suspected breaches of PHI security and privacy requirements; and
- Make sure all of your efforts (and policies) are documented, regularly reviewed and updated.

One of the most important tasks mentioned above that your business should undertake as a HIPAA-covered plan sponsor is to develop, document and implement an action plan in the event the PHI that your HIPAA-covered health plan provides to you is improperly disclosed or used for an improper purpose. Under HIPAA-covered health plans, plan sponsors must also certify that they will "report to the group health plan any use or disclosure of the information that is inconsistent with the uses or disclosures provided for of which it becomes aware." Prompt and accurate reporting of PHI privacy and security breaches is important because it allows the plan to analyze the underlying facts to determine, among other things, if there was an actual breach; whether the breach should be reported and to whom; what steps should be taken to mitigate any damages; and what steps to take to prevent future such breaches. Needless to say, HIPAA entails a complex set of rules, and noncompliance can carry substantial sanctions. You should consult with legal counsel for assistance to determine whether, and how, HIPAA may impact your workplace and what other steps should be taken. ■

Gabriela Sanchez is a Shareholder at Lane Powell, where she counsels clients on compliance with federal and state laws and regulations governing long term care and senior housing providers. She also provides risk management advice and strategies to businesses with respect to HIPAA/HITECH compliance in various jurisdictions, including Oregon, Washington, Nevada, Arizona and Montana. Gabi can be reached at 503.778.2172 or sanchezg@lanepowell.com.

Jeff C.D. Brecht is a Counsel to the Firm at Lane Powell, where he focuses his practice on representing assisted living providers, nursing homes and other long term care providers in a broad array of regulatory, licensure, contract, and collection lawsuits and administrative hearings. He advises post-acute providers with respect to a wide variety of regulatory compliance and workplace issues. Jeff also represents clients in business and trust and estate litigation, as well as employer defense. Jeff can be reached at 503.778.2162 or brechtj@lanepowell.com.