

Your Employee Benefits

Produced by *Employee Benefit News*

What you need to know about “HIPAA,” but didn’t know to ask

By Kelley M. Blassingame

Want to see your company HR/benefits manager cringe? Walk up to him or her and simply say, “HIPAA.” Chances are they are not yet over the many hours of work it took to help bring your organization into compliance with the law’s medical privacy rule, which went into effect April 14.

Since the rules are designed to protect you and the security of your personal health information, it stands to reason that you should be as informed about HIPAA as your benefits staff, health plan and medical providers. So here’s your HIPAA crash course.

First off, you may be wondering what in the world HIPAA (say it like like the pros — HIP-uh) stands for. It’s short-speak for the Health Insurance Portability and Accountability Act, signed into law in 1996 by President Clinton. While the law assures you numerous rights regarding your health coverage and medical information, the privacy rule specifically addresses your right to keep your protected health information (PHI) secure and limited to only the people who need it.

So why does your employer need to comply with HIPAA? Because your company actually has greater access to your PHI than you might think. When you enroll for health coverage, make a medical claim, participate in a wellness or disease management program, contact your company EAP or use any other employer-sponsored health service, your employer generally accesses PHI in some way. And although by the letter of the law your employer is not a “covered entity” (an organization bound by the privacy standards), your health plan is. In your company’s role as the sponsor of that health plan, your employer is responsible for instituting certain safeguards for your PHI, as well as honoring the various privacy rights entitled to you under the privacy rule.



“This is definitely a pro-employee law,” says Chris Lipski, director of the HIPAA for Employers initiative led by consulting firm Ernst & Young LLP. “The concrete rules empower employees and assures them that employers aren’t misusing their health information.”

Right to consent

The greatest right afforded you under the HIPAA privacy rule is the right to give or revoke consent for the use or disclosure of your personal health information to carry out treatment, payment or health care operations. Basically, you get the final say-so over who gets to use your medical information and what they may use it for. Your consent needs to be in writing, and must be revoked in writing as well. However, it’s important to be aware that your employer or health care provider needs to obtain consent just once, whether for related or unrelated conditions, and will only need to obtain consent again if you revoke it at some point.

Right to restriction

The privacy rule requires covered entities to make reasonable efforts to limit use and disclosure of PHI to the fewest people necessary. This requirement is called the “minimum necessary” provision. Although some HIPAA experts say there are some gray areas as to what constitutes “reasonable efforts” and which parties are among the “minimum necessary,” you can be assured that for the most part your employer needs to create or strengthen practices to protect PHI and prevent unnecessary or inappropriate access.

Right to freedom from marketing

Among your other privacy protections, the privacy rule prohibits your PHI to be used for marketing purposes without

your consent, setting specific standards about what communications are considered marketing. For example, if you suffer from hypertension, and your employer sends you information about an anti-hypertension drug now covered by your health plan, it is not considered marketing. However, should your employer offer the information to the company that manufactures the drug, it is considered marketing. There are other caveats to HIPAA's marketing provisions, including receiving sample products at the doctor's office (not marketing), but the long and short of the rule regarding marketing is no covered entity may disclose or sell your PHI to a third-party without your consent.

Applying your privacy rights

Prior to April 14, you should have received notice from your employer explaining your new rights under the HIPAA privacy rule and the policies the organization has in place to secure your PHI. This notice is a good starting point to begin figuring out how your medical privacy rights will apply at your workplace. If you have not received or misplaced this required notice, contact your company's privacy official. The privacy official, the individual responsible for ensuring your organization's HIPAA compliance, is likely a senior HR manager or a member of the legal team, according to Lipski.

"This is the person who tracks uses and disclosures of PHI and established the mechanisms in place to enforce rights," he says. "This is also the person who could be named in a legal complaint if rights are violated," noting the official's high stake in helping you understand your privacy rights.

Once you identify and contact your privacy official, you may also want to request a copy of the PHI your employer has access to. Next, "you'll want to ask who else has access to the information, how they use it, and what procedures are in place to protect it," advises Kevin Haugh, vice president of product management for ProAct Technologies. Haugh has written widely about HIPAA and provided advisory services to the U.S. Centers for Medicare and Medicaid Services (CMS), which crafted the privacy rule. "Until now, this information was used pretty liberally, and the rule protects PHI to a much greater degree."

Should you believe those protections have been violated in any manner, you have legal recourse. CMS is the federal agency responsible for HIPAA privacy enforcement, and therefore the agency to contact about perceived violations. Your privacy official should also be alerted, as they can be named personally in a lawsuit. As a medical privacy breach has the potential to span several laws, depending on the violation, "your case could have civil or criminal charges, and be tried in state or federal court," Haugh says.

A surge in employers named in HIPAA lawsuits is not expected, experts say. Rather, a surge in your awareness would more likely spur even tighter security of PHI, which benefits both you and your company. "In the past, there was a fear among employees that anyone in their company could access their medical information," Lipski observes. "The privacy rule is designed to make sure that doesn't happen, and make employers and employees both feel more safe." — K.B.