HIPAA Privacy and Security Mistakes Employers Make

Issue Date: March 2019

Introduction

Employers often wonder what they need to do to ensure that their health plans comply with HIPAA, and there are plenty of resources containing instructions and guidance to this effect. But sometimes the best way to illustrate what should be done is talking about the things that should be avoided. This issue brief will outline some of the most common mistakes employers make with respect to the privacy and security of the health plans they sponsor.

The HIPAA Framework

HIPAA privacy and security requirements apply to "covered entities," which include providers, insurance companies, and employer-sponsored group health plans. Because the health plans themselves are covered entities, the employers who sponsor them are not technically the legal entities subject to HIPAA. But employers, as plan sponsors, are the entities who are (from a practical perspective) responsible for ensuring that their health plans comply.

There are types of employer-sponsored plans, including medical, dental, vision, prescription drug, HRAs, and FSAs. Wellness programs offered as part of a group health plan (or that are themselves health plans), and EAPs that provide medical care are also considered covered entities.

HIPAA applies to health plans regardless of whether they are fully-insured or self-funded, but in some cases, plan sponsors of fully-insured plans who have limited access to their plan's PHI will have fewer compliance obligations. This is because the insurance company (also a covered entity) will end up assuming most of the responsibilities with respect to the plan.

HIPAA also applies directly to "business associates." (But as we'll note later – a business associate's compliance obligations do not override the plan sponsor's obligation to ensure that a compliant agreement is in place!)

Mistakes Employers Make

With the above framework in mind, below are some of the most common HIPAA privacy and security mistakes employers make with respect to the health plans they sponsor:

Mistake No. 1: Not Considering All Plans Offered

As noted above, it's not just the medical plan that employers need to worry about! Many health plans offered by employers are subject to HIPAA privacy and security requirements. Employers must review all the plans they sponsor to determine which are in scope. If an employer only pays attention to its medical plan, then PHI associated with other plans may not be adequately protected. And if employers sponsoring fully-insured medical plans who have limited access to their plan's PHI are relying on the "lighter" compliance requirements that apply, there could be a problem if the employer also sponsors a self-funded plan (e.g., an HFSA).
Best Practice: Plan sponsors should review every plan they sponsor to determine which plans are subject to HIPAA privacy and security requirements. HIPAA permits plan sponsors to designate their various plans as a single Organized Health Care Arrangement, or OHCA, which allows the plan sponsor to undertake just one compliance effort on behalf of all plans.

Mistake No. 2: Just Doing Part of HIPAA

Contrary to what we sometimes hear, there's no certification program out there that an entity can complete that deems an entity HIPAA compliant. The compliance process is much more organic, and employers need to be careful not to fall into the trap of thinking that one or two compliance efforts are sufficient.

Simply providing training, appointing a Privacy or Security Official, and just having a Notice of Privacy Practices is not enough. Employers must have written policies and procedures in place that are appropriately implemented and overseen. In considering and addressing all the privacy and security requirements, it will be easy to see how the pieces all work together, and how each part is just one small piece of a larger whole.

Best Practice: To ensure total compliance, employers should look at all the requirements that apply to health plans. The best resources for this information can be found on OCR's website (https://www.hhs.gov/hipaa/for-professionals/index.html); in the template policies and procedures that are available from a variety of resources; and in OCR's most recent audit protocol (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html).

Mistake No. 3: Relying Solely on the Administrator (TPA) for Compliance

For employers that sponsor self-funded health plans, there is no regulatory exception to their compliance obligations as there is for sponsors of some fully-insured plans. This is true even if the plan sponsor delegates the majority of its plan administration obligations to its TPA. The plan sponsor is still responsible for making sure the relevant policies and procedures are in place, and that it has appropriately addressed all the compliance requirements under HIPAA privacy and security rules. It may be delegating many of these things to the TPA via a business associate agreement, but that doesn't mean that the employer can ignore them.

Best Practice: First, an employer needs to understand what the covered entity's duties are under HIPAA. Then it must determine which of those responsibilities will be delegated to the TPA. The ways in which the TPA is expected to handle PHI and administer the plan should be clearly spelled out in a business associate agreement between the plan and the TPA.

Mistake No. 4: Not Conducting a Security Risk Analysis

The Security Rule requires that all covered entities (and business associates) conduct a risk analysis. The purpose of the risk analysis is to review the employer's security controls in light of HIPAA's requirements, and to make a determination about the level of risk there is to its plan's PHI. Failing to conduct an adequate risk analysis (and taking appropriate mitigation steps for issues identified as higher risk) can increase the entity's risk of a breach and exposure to civil penalties. When we look at one of the major causes of many of the breach settlements that have occurred over the past few years, failure to conduct a risk analysis is one of the most commonly cited failures.

Best Practice: The Security Rule does not tell entities how they must conduct a security analysis. Typically, the process will involve identifying the universe of systems/applications where ePHI is stored/maintained/transmitted, and looking at existing security controls that are in place as compared to the controls contained in the security rule. The entity should make a determination about the level of risk it believes it has with respect to its electronic PHI and should both develop a mitigation plan accordingly and review the risk analysis periodically to make any necessary updates.

Mistake No. 5: Misidentifying PHI

PHI is a tricky concept. This is because protected health information is technically only individually identifiable health information that is transmitted or received by a covered entity. In practical terms, what this means is that when we talk about PHI in the context of employer-sponsored health plans, we're talking only about individually identifiable information that is part of the employer's health plan's records. But an employer may handle individually identifiable information for many reasons that have nothing to do with its health plan. For example, employers might collect the results of drug tests as a condition of hire or may require medical certifications from

doctors to support a request for leave under FMLA. If an employer is using medical information in its role as employer, and not for purposes of administering its plan, that information is *not* PHI. It may be the exact same type of information – e.g., a claim – but if it's not coming from the employer's health plan records, then it's not PHI in the hands of the employer. Handling this kind of employer information carefully is still important, but it is not subject to HIPAA.

On the other end of the spectrum, there is the problem of employers thinking that information isn't PHI unless it contains detailed claims information – e.g., has a diagnosis code or discusses treatment. The definition of PHI is very broad – it can refer to just a name or a date of birth. Again, if the information is individually identifiable and comes from the health plan records, then no matter how "generic" it might seem, it's PHI.

Both these mistakes can cause problems – employers may worry needlessly over HIPAA implications if they're dealing with health information that isn't PHI. And on the other hand, employers may misuse or fail to safeguard information that *is* PHI simply because they don't believe that it is.

Best Practice: Review the types of information handled and determine what is and is not PHI. For information that is PHI, ensure that required safeguards (privacy and security) are implemented appropriately. (Remember that other confidentiality requirements may apply to information that is not PHI.)

Mistake No. 6: Failing to Identify Business Associates

Employers usually have several relationships with various contractors and vendors. There is often a lot of confusion about whether these relationships constitute a business associate relationship. Sometimes employers will try to play it safe by putting business associate agreements (BAAs) in place with almost every vendor. Other employers may have relationships with vendors whom they don't realize are business associates.

In short, a business associate (BA) is any entity that performs plan administration on behalf of the covered entity – e.g., claims adjudication, support for an application or system that stores/maintains/transmits PHI, assisting with claims/benefits issues, etc. When a vendor needs to access PHI in order to carry out plan administration functions, they are a BA and a compliant agreement is necessary. Vendors who are not performing plan administration functions are not BAs and should not have access to PHI. The risk of not having a BAA in place with a business associate is that the covered entity is sharing PHI with that vendor without first ensuring that the vendor has appropriate safeguards in place.

Best Practice: Employers should review the contracts they have in place to see which vendors perform plan administration functions and have access to PHI as part of their services. A compliant BAA should be in place with any such vendors.

Mistake No. 7: Not Tailoring the Notice of Privacy Practices

The Notice of Privacy Practices is the document that describes what an individual's rights are with respect to their PHI. It also informs the individual how the plan uses and discloses PHI and what its legal obligations are with respect to the PHI. Since plans will have unique practices for using and disclosing PHI, it's important that the NPP be appropriately modified to accurately describe these practices. In addition, the NPP should be clear about which plans (e.g., medical, dental, vision) it applies to. Employers often rely on an NPP provided by their health insurance carrier that does nothing to address HIPAA obligations of other plans the employer sponsors (e.g. dental, health FSA, HRA, etc.).

Best Practices: Examine all plans offered and ensure that the Notice of Privacy Practices encompasses all plans subject to HIPAA. Work with legal counsel to ensure that any model NPP is appropriately tailored to reflect the plan's actual operations/practices. If the employer chooses to rely upon a carrier's NPP for a fully-insured plan, then it should review the notice to make sure the information is an accurate reflection of the employer's plan's operations.

Mistake No. 8: Providing Privacy Training Only

Training is required under both the Privacy and Security Rules. There isn't any prescribed format for training, so plan sponsors have some flexibility in how the develop their trainings. But sometimes employers will focus so much on privacy principles that they'll forget to address the required security components, which include identifying and avoiding malware, training employees on the company's password policies, and so forth. In addition, although privacy training really needs to be provided only to employees who are responsible for plan administration, and who have access to PHI in that role, security training should ideally be provided to all employees, since everyone is using the company's electronic systems that are vulnerable to attacks/viruses.

Best Practices: A Plan Sponsor should provide privacy training that focuses on appropriate uses/disclosures and safeguards of PHI to staff who are responsible for interacting with PHI on a regular basis. Separately, whoever oversees the organization's corporate security awareness training should ensure that it addresses the HIPAA required elements. Note that the Security Rule requires that periodic reminders/updates be issued as part of an organization's overall security awareness program. So in between more formal trainings, entities should ensure that they are educating employees about various security awareness principles.

Conclusion

Navigating HIPAA compliance can be complicated. We hope that by highlighting some of the more common mistakes we see with respect to employer-sponsored health plans, we can shed some light on the important things employers must do to protect their plans' information.