know HIPAA
(952) 400-1100 | knowhipaa.com

How to talk to your clients about HIPAA

Know HIPAA has distilled the complex HIPAA regulations into 5 key messages. You can use these to start the conversation then offer one of our HIPAA compliance tools to help resolve any issues.

1. An employer is subject to HIPAA whenever they have access to an employee's individually identifiable health information

HIPAA calls this Protected Health Information (PHI) and it includes:

- Information that an organization has access to through their role as a health plan sponsor or;
- Information on an external entity's employees which the organization has access to because of the services provided to that entity. HIPAA refers to this relationship as a Business Associate (BA).

Self-funded employers aren't the only ones subject to HIPAA rules. Most small employers with fully insured health plans are also subject to HIPAA to some extent.

- Some offer plans that are considered self-funded plans such as HRAs, Health FSAs, or a self-funded dental plan.
- Others end up having access to PHI through the way they administer their plan.
- Only employers with all fully insured plans, and who have access to summary health information and enrollment data only, have more limited compliance obligations.

2. HIPAA restricts the use of an employee's health information.

HIPAA allows the use of PHI for most of the things necessary to effectively administer the organization's group health plan. For most other purposes, the employer must obtain an authorization from the affected individuals. **This also means that employers may not use PHI for any other *employment* related purposes without the employee's authorization.**

3. HIPAA is a risk mitigation strategy.

Becoming compliant protects the employer from

- Civil and/or criminal liability if a breach of PHI occurs
- Random audits by HHS and the remedial penalties associated with them
- Liability for the malicious actions of a rouge employee

4. What must an employer actually do to be considered in compliance with HIPAA?

For an employer to be in compliance, they must establish written HIPAA policies and procedures that govern the plan's use of PHI.

The employer will also need to take a number of other steps including, but not limited to:

- Designate Privacy and Security Officials
- Determine what organizations and vendors are acting as business associates and enter into written agreements
- Implement reasonable physical and technical safeguards to protect PHI
- Create/Update Plan Documents, Notice of Privacy Practices, Business Associate Agreements, etc.
- Conduct a Security Risk Assessment
- Provide HIPAA Training for Employees Who Handle Protected PHI