HIPAA, Data Breaches and What You Should Know (Even If You're Not a Healthcare Company)

When it comes to compliance, most everyone agrees that the privacy regulations set forth by the Health Insurance Portability and Accountability Act (HIPAA) are critical and worthy of being upheld – even if doing so means extra effort (and expense) by those entrusted to handle such personal data and information. For healthcare organizations, a full commitment to HIPAA compliance is obligatory but there are other groups that are similarly implicated. Those include organizations that may handle significant volumes of PHI for health plans provided to large employee populations, as well as organizations that offer level-, or "self-" funded insurance plans.

So whether you are a healthcare organization, a company that offers a self-funded insurance plan to their employees, is considering doing so, or is simply an organization that has a decent number of employees participating in the company-sponsored health plan, it is wise to make sure that you're fully in the know. And, with that, fully understand the expectations, responsibilities and best-practices associated with safeguarding patients' and/or employees' personal data.

So, What is a Data Breach Anyway?

Most are surprised to find that the majority of breaches are actually not software breaches. In other words, they are not the result of some computer genius in a Cyrano de Bergerac mask, exploiting password weaknesses in order to sell others' personal data to foreign spies or blackmail their helplessly breached corporate prey. While those types of things do happen, the instances are rare. Instead, we find that the vast majority of breaches are what are called "hardware breaches" which happen, simply, because of employee carelessness. For an example, some major hospital network contractor leaves his unencrypted laptop in the car and has it stolen. Yes, a very unfortunate and expensive, "whoops."

The thing is, it is easy to imagine an employee of a restaurant chain who also happens to offer a self-funded insurance plan make the same mistake – suddenly, all the medical information of all those national restaurant chain employees hangs in the balance. This is where things can really get sticky. Fortunately, there are some sure-fire ways to prepare and safeguard an organization, as well as its patients'/employees' most private and personal information. Because when there is a breach, no matter how it comes to pass, is bad for everyone.

So, Who Actually Enforces HIPAA?

The HHS Office for Civil Rights (OCR), does the job of enforcing HIPAA regulations. And based upon 2018 data, alone, they are staying busy. Just last year, HIPAA enforcement activity totaled $28.7 million levied against organizations for breaches of protected information, including one for $165M, the largest single settlement ever. What's more, the OCR has what they call a "wall of shame" where they list all breach reports over the past two years and unfortunately, it appears that 2019 is already moving in the wrong direction at an epic clip.

It should also be said that just a few years back, the OCR was content to investigate only reported breaches. Not so, today. In the current environment, OCR is mandated to be proactive, identifying organizations that could potentially be vulnerable, auditing and then taking some form of corrective action if deemed appropriate.

Steps HIPAA-Implicated Companies Must Take to Prepare

1. **Assess Your Risk** – Company leaders must evaluate all the hardware and software that handles protected health information in any way. They must determine who has access, how the system is protected from hacking, natural disasters, as well as theft.
2. **Encryption** – It is imperative that this critical data is properly encrypted, thereby elimination (or at least greatly reducing) the chances that an unfavorable entity could purposefully misuse it.
3. **Training** – If your staff isn't fully trained, you may quickly find yourself in trouble. Do it at onboarding and provide refreshers at regular intervals, thereafter (no less than twice per year.) All staff should be able to identify phishing emails, understand proper password maintenance and how to secure their computing devices and when it is necessary.

Recommendations for Organizations Providing Sizable Traditional or Self-Funded Insurance Plans to Employees

HIPAA compliance for self-insured group health plans can be complicated as it may be difficult to determine whether a company is subject to the legislation. Further, compliance requirements vary from depending on business-type, business model and number of employees. So, here are some quick tips to get prepared:

1. **Hire or Appoint a "Privacy and Security Officer" -** Their role is to identify where, why, and to what extent PHI is created, received, maintained or transmitted (as it pertains to the group health plan). This will touch multiple departments.
2. **Develop HIPAA-Compliant Privacy Policies –** These are to establish the organizations recognized uses, permissions and disclosures of PHI. The policies should also include verbiage around third-party administrators who also must be entered into a HIPAA Business Associate Agreement.
3. **Develop HIPAA-Compliant Security Policies -** Covered Entities are required to "implement administrative, physical and technical safeguards to ensure the integrity of electronic PHI." As stated in the section above, a Security Officers should conduct a risk assessment followed by the implementation of suitable safeguards.
4. **Develop a Breach Notification Policy –** Even companies who put in commendable effort may receive an "unauthorized disclosure of PHI." What must be avoided is wondering what course of action to take once that's happened. Instead, have a breach notification policy in place to alert employees that information may have been compromised.
5. **Training –** Just like any healthcare company, employee training is vital. Handling this early and often mitigates a huge portion of risk.

Act Quickly Should a Breach Occur

Even the best laid plans sometimes fall victim to unforeseen circumstances and mistakes. In such scenarios, it is important to respond and mitigate data loss quickly, so as to limit exposure. The OCR provides its own quick-response checklist that gives a good outline of the necessary steps to take. This should be common knowledge for all action employees.

HRWS at Your Service

Whether you are an HRWS Broker Partner or one of their enrolled clients, know that you do not have to navigate this difficult compliance landscape alone. We have years of experience and subject-matter experts on hand to guide you through the entire process. Whether you're a company's dedicated compliance officer with a specific question, an HR officer tasked with procuring training, or a brokerage seeking a comprehensive solution for a client we handle everything with symphonic precision. If you're connected with HRWS you are way ahead of the pack.

Just keep in mind, HIPAA compliance, whether you are a healthcare organization, provide a self-insured or sizable traditional healthcare plan to employees - or are otherwise implicated – remember we are just a phone call or email away. Get started with your comprehensive HIPAA compliance and data breach solution today.