Technical Support
INTERNATIONAL
Consulting and Computer Services

How To Guide: Guard Against HIPAA Privacy Breach Fines & Violations

In 2016, the Health Insurance Portability & Accountability Act (HIPAA) collected over 23 Million in Civil Money Penalties (CMPs) related to businesses violating patient data privacy provisions. Over half of the cases involved organizations who failed to even have a proper risk assessment conducted.

The cost for violating HIPAA privacy protections continue to grow, which is why we decided to provide a list of the most common violations, as well as how to avoid them.

Data Breaches

The Office for Civil Rights (OCR) maintains a "Wall of Shame" database of breaches that affected 500 or more individuals. Of the 325 cases reported in 2016, nearly **34% were a direct result of hacking or an IT related incident**. These are not always sophisticated attacks mind you, some were the result of a weak password, or exploiting a known vulnerability in the anti-malware/anti-virus software.

A few easy methods to ensure your network is less vulnerable to hacking include developing a strong password policy, and enforcing it. Other solutions include installing a proper Firewall protection solution for your company, and ensuring it has the latest security patches for optimal defense. We also highly recommend installing a solid Anti-Virus and Anti-Malware software with automatic updates turned on. It is important to prevent users from disabling the tools on their local company-owned machines as well.

Lost or Stolen Devices

Bring Your Own Device is here to stay, unfortunately it only compounds the complexity for protecting your patient health data. The best solution to allowing the freedom of mobile access for your employees while remaining compliant is as simple as having the information encrypted before, during, and after transmitting.

While encryption is not a direct requirement under HIPAA, there are examples where the OCR deemed insufficient protection of data by an organization, such as the compliance review against Concentra Health

Services. The OCR determined Concentra did not utilize basic encryption defenses to protect patient health data from being stolen from lost devices, resulting in a $1.7 Million Dollar fine.

Moral of the story? There is hardly a reason why any data should not be encrypted in the day and age of daily intrusion attempts.

Proper Disposal of Information

Regardless of the format, be it digital or physical paper, health information must be properly shredded and destroyed to protect the privacy of the parties. This includes machines and devices being disposed of, or decommissioned.

For example, did you know photocopiers can contain an internal hard drive capable of storing information locally on the machine? For businesses who routinely lease equipment and/or have their printer periodically replaced, the hard drive must always be wiped so that patient information cannot be recovered. A lesson Affinity Health Plan learned after returning their photocopiers to leasing agents, unknowingly compromising all the records they printed over the years. A $1.2 Million Dollar oversight that could have easily been avoided.

Subcontractors & Third-Party Disclosures

According to the Common Agency Provision within the HIPAA Omnibus Ruling, you are responsible for protecting patient health information while the data is stored in your premises or network, as well as any information shared with your third-party associates. With this shared liability, it is best to review the HIPAA compliance policies of any subcontractor prior to disclosing sensitive information or having them sign an agreement that leaves you liable for their potential negligence.

Training & Education

Proper training and staff education rounds out the top of our list, and for just reason. Employees are largely unfamiliar with the best practices and regulations surrounding HIPAA. It is a huge problem that puts many small businesses and practices at risk for hefty fines. Training for **all staff who handle patient information** should be a rudimentary component of every orientation, as well as developing an ongoing education plan so that staff are aware of the latest changes to the law.

The risk for even unknown violations reach up to $50,000 per violation (each record compromised) up to $1.5 Million annually. This is enough to bankrupt many Small or Medium sized businesses. Extending training to contractors and all employees is part of maintaining HIPAA compliance, and is just a great practice to ensure the best level of protection from willful violations.

Learn More

To learn more information from our team of experts, including establishing a proper risk assessment, Contact Us today!