LernerDavid | Deciphered®
INTELLECTUAL PROPERTY LAW

2022 Privacy Law - Tips That Could Save Your Company From Financial Penalties

Today, January 28, is recognized in the U.S. (and in more than 47 countries) as International Data Privacy Day (IDPD). This day serves as an annual reminder for companies to reevaluate their data privacy and security practices to ensure compliance with current standards and to prepare for coming changes in privacy and data protection laws.

Similar to what is happening in other states around the country, New Jersey is currently witnessing a rise in the enforcement of privacy and data protection laws. In just the last six months, the New Jersey Attorney General and the New Jersey Division of Consumer Affairs have announced the conclusion of three investigations targeting companies that allegedly failed in their duty to protect personal data of their customers and website visitors including personal identifiable information (PII), protected health information (PHI), and electronic protected health information (ePHI), resulting in more than $1,000,000 in penalties.

One investigation of a New Jersey healthcare provider found that a workstation security breach and weak server security led to multiple instances of unauthorized access to the personal data of more than 14,000 patients over a six-month period. Among the dozens of alleged violations of the New Jersey Consumer Fraud Act, the federal Health Insurance Portability and Accountability Act ("HIPAA") Security Rule, and HIPAA's Privacy Rule, the investigation found that the provider failed to encrypt ePHI stored on a third party server, failed to conduct a comprehensive risk assessment, and failed to execute business associate agreements (BAAs) with third-party providers. The company agreed to pay $495,000 in civil penalties and costs as part of a settlement.

Some data security measures required by the NJ Division of Consumer Affairs and NJ Attorney General are outlined below. Implementing these measures may help your company avoid regulatory investigations and possibly avoid a large financial penalty.

1. Develop and implement a comprehensive information security program that includes regular updates to keep pace with changes in technology and security threats.

Hackers continue to discover new ways to disrupt business even as new data security technology is developed. Maintaining data security therefore must be a perpetual endeavor for any size organization. Strategic planning helps a company appropriately address daily information security threats.

2. Train employees concerning information privacy and security policies, as well as the proper handling and protection of personally identifiable information and protected health information.

A well-educated workforce is critical to any comprehensive security policy. Companies need to provide routine, ongoing data security training for their employees and key executives to teach about potential threats and measures that they can take personally to defend against these threats. Proper training helps employees recognize signs of potential issues in real time, and what corrective action to take to avoid costly mishaps that may lead to the loss or undesired disclosure of confidential company information.

3. Develop and implement a written incident response and data breach notification plan to prepare for and respond to data security incidents.

A company's brands are vulnerable to data breaches such that these breaches can have a very real and devastating effect on a company's reputation. The average cost of a data breach, according to a recent IBM report, is a whopping US $4.24 million. Developing and implementing an incident response plan will enable your business to handle a data breach more quickly and efficiently while minimizing possible damages and costs.

4. Implement personal information safeguards and controls, including encryption, logging and monitoring, access controls, a risk assessment program, and password management.

By instituting these security procedures, a company protects its information that otherwise could be unintentionally damaged by an individual user of a company's valued data trove or potentially accessed by a hacker who may harm the company or even its employees. Individual users may also feel more confident in using the company's data services when information is maintained in a secured manner.

These recent NJ investigations send a strong message to businesses that such privacy lapses come with significant financial consequences. Businesses should use International Data Privacy Day to review their Privacy and Cybersecurity policies. Lerner David has experienced attorneys, including Certified Information Privacy Professional (CIPP), well-versed in Privacy Law and Cybersecurity compliance that can tailor a plan that best suits your business needs.
Find out more at https://www.lernerdavid.com/practices/privacy-law