PARTRIDGE SNOW & HAHN LLP

What's In Your WISP?

May 09, 2019

We routinely recommend to clients that they develop a written information security program ("WISP"), to safeguard sensitive information on a day-to-day basis. In fact, businesses (wherever located) that collect, store or use personal information about a Massachusetts or Rhode Island resident are required legally to develop and maintain a WISP. For purposes of these legal requirements, personal information can be as little as a first name, last name, and the last four digits of a social security number, credit card account number, or bank account number.

Business leaders need to understand that the WISP is a "program," not a "policy." A WISP should describe a system by which one runs the business on a day-to-day basis to safeguard sensitive information. Some clients treat WISPs as policies that they can have drafted, only to then be set aside and never reviewed again. Some businesses have copied a WISP from a form found on the Internet, or a form provided by another company, but have not taken the time to customize it for their business. Other companies want to say they have a WISP, but do not actually make any operational changes to implement the purported security programs described in the WISP. Recent amendments to Massachusetts law make these practices, as well as not having a WISP at all, much more risky.

Using the Massachusetts rules as an example, there are specific requirements for what your company's WISP should cover. Some of these include:

- The scope of the WISP as to what business and what employees (typically all) the WISP applies, and what personal information is collected by the business
- The identity of the information security coordinator for the company and his or her responsibilities for implementing the WISP, training and reporting to management
- The company's information security policies and procedures (the WISP can reference existing policies HR and IP policies, as applicable, and identify any additional policies)
- The administrative, technical and physical safeguards that the Company has implemented to protect personal information
- The procedures the Company has implemented to oversee vendors that have access to personal information on the Company's behalf
- The penalties/disciplinary actions for violating the WISP
- The schedule for reviewing and updating the WISP and security measures (at least annually)

If your business does not have a WISP in place or has not updated its WISP recently, we would be happy to discuss these requirements with you and assist you with your compliance obligations. Please contactColin A. Coleman, John E. Ottaviani, or Brian Reilly at Partridge Snow & Hahn LLP.

Related Articles

Does Your Company Have a WISP? Have You Updated It Lately?

Amendments to the Massachusetts Data Breach Notification Law Create Additional Notification and Response Requirements

How Vulnerable Is Your Business to a Cyber Attack or Data Breach?

Plan Now to Comply with the New Rhode Island Identity Theft Protection Act

https://www.psh.com/whats-in-your-wisp/