WISP – Written Information Security Program

August 25, 2016

What is a WISP?

A WISP is a written information security program. The Massachusetts data security regulations (201 C.M.R. 17.00 et seq., the "Massachusetts Regulations") that went into effect in 2010 require every company that owns or licenses "personal information" about Massachusetts residents to develop, implement, and maintain a WISP. The WISP must contain certain minimum administrative, technical, and physical safeguards to protect such "personal information".

Is this just for Massachusetts companies?

While other state and federal laws have similar requirements this article focuses on the Massachusetts Regulations, which apply to companies that own or license personal information about Massachusetts residents, whether or not the company is in Massachusetts.

What information must be protected under a WISP?

The Massachusetts Regulations require the protection of "personal information", which is defined as a Massachusetts resident's first name and last name (or first initial and last name) in combination with any one or more of the following data elements related to this resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account. Other laws vary in scope and require the protection of different classes of information.

What does the WISP require businesses to do?

Generally, businesses acting in accordance with a WISP must:

- Designate an individual to maintain and be responsible for the program;
- Identify any reasonably foreseeable data security risks;
- Protect and restrict access to paper and electronic forms of any personal information; and
- Oversee any third-party service providers and ensure that those service providers comply with the Massachusetts Regulations and other applicable regulations.

How can having a WISP be critical if a company experiences a data breach?

The Massachusetts Office of Consumer Affairs and Business Regulation has said that whether a company has a WISP and has followed it will be critical in assessing culpability in the event of a breach.

Can a company use a model WISP?

A WISP must be accurate. Therefore, it should not be a model copied from the Internet, as such a document is unlikely to reflect the company's particular risk profile and actual practices. The WISP will not be effective if it does not address the risks associated with the company that adopts it or if it claims practices that are not actually in place. Companies should work together to identify and address reasonably foreseeable risks and coordinate with their IT team in

particular to make ensure the WISP does not overreach and embodies practices that will work for the company in practice.

Do companies need a lawyer for this?

We encourage companies to work with counsel when they are preparing a WISP, as it must be customized to address the company's risk profile and actual practices — and take into account not only Massachusetts law, but also the law of any other state that applies, and any sector-specific privacy laws that govern the industry in which the company operates.

For more information, please contact one of the attorneys in the Privacy and Data Security Group: Faith Kasparian, Ryan Perry, Ann O'Rourke, Kevin Olson, Amanda Schreyer, or Michael Cavaretta.