Part 2 – DO I NEED A WISP AND WHAT IS A WISP? Deadline Approaching for yours

February 26, 2012 by Travis Crabtree

In part one, we talked about whether you need a Written Information Security Plan or WISP and the importance of the March 1, 2012, deadline for vendor compliance. Now, we discuss what exactly is in a WISP?

Generally speaking, it is supposed to cover the development, implementation, maintenance and monitoring of the collection and use of personal information. It is a written policy that designates a person in charge, places safeguards in place to prevent data breaches and outlines a procedure if one happens.

Fortunately, the law says the level of detail of your WISP depends on the amount of personal information you maintain. You, very likely, don't have to follow the same WISP as Raytheon.

Specifically, a WISP should:

- Designate an individual to be responsible for the program;
- Minimize the use, retention and access of and to personal information;
- Protect and restrict access to paper records and electronic records with passwords, encryption and firewalls; and
- Ensuring that your vendors have safeguards.

It's that last one that may introduce you to the need for a WISP by a request for companies for whom you work. At first glance, the WISP requirements seem burdensome. In actuality, it really just requires you to formalize reasonable procedures you likely already have in place or should have in place.

For more information on the requirements, check out the Massachusetts Office of Consumer Affairs & Business Regulation's website which has a compliance checklist and a small business guide.

Tags: data security, online privacy, WISP