

[Back](#)

Article published Dec 20, 2009

New Mass. law impacts data privacy

I testified before Congress last spring, and more recently, to the Massachusetts Office of Consumer Affairs and Business Regulation on the new data privacy laws being enacted in the Commonwealth. As 2009 nears a close, it's critically important that you be aware of the impact of the Massachusetts law on your business.

On March 1, 2010, 201 CMR 17.00 will go into effect and businesses across the United States will need to be in compliance. You may wonder why a business located outside Massachusetts will need to comply with the law. It's quite simple. Massachusetts has enacted the most stringent data privacy law in the country, which basically says that if you do business with a resident of or company from the Commonwealth, you will be required to protect the private information of those residents or companies.

So, a business located in New Hampshire that does business in Massachusetts needs to be in compliance.

What exactly does being in compliance mean? It means you have taken the necessary steps to protect that personal information. The law defines personal information as "first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such 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; provided, however, that 'Personal information' shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public."

Also of significance is the fact that these protections pertain to not just electronically stored and transmitted information but also hard copy formats. So, if you store this type of information in file cabinets, those file cabinets must be able to be secured and their access monitored. In other words, this law applies to both high- and low-tech forms of private data. Educating and training employees who come in contact with this type of information will be critically important.

For a business to comply with this law, it needs to develop a written information security policy, or WISP. This policy document will address all the aspects of this law, including training for all personnel, so it will be very important to develop a comprehensive training program that identifies what data your business works with that will be covered by this law and how that data must be handled. Additionally, personnel will need to be trained on how they can communicate this information, electronically or otherwise, and how to properly destroy it. You no sooner want to send private information via insecure e-mail than toss it in the office dumpster. Both are violations of the law.

From a technology standpoint, there are several, affordable technologies that will address the requirements of the law.

E-mail encryption technologies are available that make it easy and cost effective to securely e-mail private information to those that you need to communicate it to. There are also many options to encrypt your portable computers that will contain this type of information as well as USB keys that may be used in the company. The key is to employ technologies that allow you to centrally manage this, so you can track these devices and ensure they are used properly.

When it comes to mobile phones, it gets a little more complicated, but you should only allow mobile devices that may be centrally managed and remotely wiped should they become lost or stolen, to ensure that no private data is lost.

The Massachusetts law is setting the bar for the rest of the country and it is only a matter of time before more states enact similar laws. Several already have variations on the Massachusetts law, but again, it is the most stringent, for now. It's also likely that we will see some type of umbrella legislation emerge at the federal level, we just don't know when yet.

So, my advice for the New Year is to talk with your trusted IT partner and make a plan for what you need to do to be compliant in advance of March 1. The penalties start at \$5,000 and go up very rapidly, so the cost of compliance will pale in comparison to the potential risk of not. Best wishes for a happy and safe holiday season and New Year.

MJ Shoer is president and virtual chief technology officer of Jenaly Technology Group, Inc., a Portsmouth-based outsourced IT services firm. He may be reached at mshoer@jenaly.com.
