Nonprofit 411: Five Important Features of the MA Data Security Law and Regulations

MAY 28, 2013 BY KAITLIN HENRY

By Samuel Nagler, Partner, Krokidas & Bluestein LLP

The silver lining of the recent high-profile security breaches is that most Massachusetts organizations are aware at least in a general sense of the Commonwealth's data security law (Massachusetts General Laws, Chapter 93H). However, many aspects of compliance are still not fully appreciated — or are misunderstood.

Large or small, profit or non-profit, all Massachusetts organizations which maintain "personal information" are accountable under the law. Whether you manage information on employees, clients, donors or others, here are five key facts about the data security law that you need to know:

1. Know what "personal information" must be protected. "Personal information" includes 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:

- *1.* Social security number;
- 2. Driver's license number or state issued identification card number; and
- 3. Financial account number or credit or debit card number.
-

If you maintain a database with any of the combinations described above—whether in your employee payroll system, client database, or fundraising database—you must take appropriate action to protect that data.

2. Know what a WISP is and what it must include. A Written Information Security Plan (WISP) is a comprehensive information security program your organization is required to develop, implement and maintain.

WISP requirements are too numerous to list here, but they can be found in the regulations on the Massachusetts Attorney General's website. One mandatory requirement is ongoing employee training—**including** the training of temporary and contract employees, and in certain instances, interns.

3. The requirements extend to your vendors. If you need to share personal information with any vendors, whether they are based in Massachusetts or elsewhere, you must perform the necessary due diligence to satisfy yourself that the vendor is capable of maintaining appropriate security measures as required by the data security law.

Your contract must also contain a specific requirement that the vendor implement and maintain appropriate security measures for protecting personal information. Neither the due diligence nor the contract provision alone is sufficient for compliance; both requirements must be satisfied.

4. Paper documents have legal requirements of their own. Since the most dramatic breaches are electronic, it can be easy to forget that there are clear rules for the disposal of paper documents as well. Massachusetts General Laws, Chapter 93I specifies that "paper documents containing personal information shall be either redacted, burned, pulverized or shredded so that personal data cannot practicably be read or reconstructed."

5.The law only applies to personal information of Massachusetts residents—46 other states have their own statutes. If you hold personal information for an employee or other individual who lives out of state, you will need to familiarize yourself with the requirements of their state of residence in order to ensure that your policies comply.

Data security law is complex and nuanced, but two key professionals can assist you with compliance and protection: your attorney and your insurance agent. Your attorney can advise you of the legal requirements, prepare your WISP and conduct training sessions. Your insurance agent can provide data security insurance coverage on your organization's behalf.

You would never leave your office door unlocked or your wallet unprotected in a public place—consider these legal requirements as similar precautions to reduce your risk of data loss.

FILED UNDER: SECTORNEWS ARCHIVE