The Bennett Law Firm
Client Update
Trusted Advisor to Management for Over 50 Years
Labor Relations ~ Employment Law ~ Business Litigation
Portland, ME (207) 773.4775 / Boston, MA (617)973.1550

MASSACHUSETTS STANDARDS FOR PROTECTION OF PERSONAL INFORMATION

In the wake of security breaches of several high profile companies a few years ago, the Commonwealth of Massachusetts enacted regulations designed to protect personal information of Massachusetts residents. Businesses should be mindful of this law and its legal requirements.

Does the law apply to your business?

The regulations are not explicitly limited to companies doing business in Massachusetts. If you handle personal information of Massachusetts residents, the regulations apply to your business and compliance is mandatory.

What is "personal information?"

Under the law, "personal information" to be protected includes a Massachusetts resident's name (either first and last name or first initial and last name) combined with a complete social security number, driver's license, or other state-issued number, a financial account number or a complete credit card or bank account number. This encompasses a wide variety of informational records - everything from employee, client, customer and investor records to supplier, patient and student records.

What do the regulations require?

The regulations require that businesses develop, implement, maintain and monitor a comprehensive, written information security program (WISP) to safeguard personal information contained both in paper and electronic form. While the WISP will vary depending upon the size and scope of your business, availability of resources, the nature and quantity of stored data, and the need for security and confidentiality of both consumer and employee information, the objective is to develop reasonable and effective administrative, technical and physical

safeguards for the protection of personal information belonging to residents of Massachusetts.

The regulations also require that you designate one or more employees as an information security coordinator and charge them with maintaining your information security plan. Responsibilities should include: implementation of the plan; initial and annual training of employees; regular testing of the plan's safeguards, and annual review of the scope of the plan.

The regulations also require businesses that use a third-party service provider to store and maintain personal information to take reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect personal information.

In developing a WISP, businesses should identify records containing "personal information" of Massachusetts residents; whether they are electronic or hard copy; define who has access and set reasonable restrictions to access, such as storage under lock and key of hard copies. The regulations require different safeguards for electronic data and laptops, such as use of encryption, depending upon the size and scope of your business and the availability of resources. If off-site use of personal information is necessary to your business operations, you should also develop security policies for employees relating to the storage, access and transportation of records outside of your business.

If you need assistance with these issues, please contact Peter Bennett (pbennett@thebennettlawfirm.com), or Joanne Simonelli (jsimonelli@thebennettlawfirm.com).