



SHEEHAN PHINNEY BASS + GREEN PA
Attorneys at Law

Client Advisory

***Update: Massachusetts Data Security Regulations
Amended to Require Implementation of
Comprehensive Information Security Measures by March 1, 2010***

**Maria E. Recalde and Mark J. Ventola
Sheehan Phinney Bass + Green PA**

December 8, 2009

Massachusetts regulations implementing the provisions of its Data Security Breach Law, Mass. G.L. c. 93H (the "Security Regulations") were recently amended, and the effective date was extended to March 1, 2010. The Security Regulations establish minimum standards to be met in connection with the safeguarding of "personal information" of Massachusetts residents contained in both paper and electronic records. They require *all* individuals, for-profit and non-profit organizations, among others, that own, license, store or maintain personal information about a resident of Massachusetts, *whether or not they are located in Massachusetts*, to adopt a comprehensive, *written* information security program. The information security program must include the establishment and maintenance of a computer security system covering an organization's computers, including any wireless systems.

Initially set to take effect on January 1, 2009, the compliance deadlines were first extended to *January 1, 2010 and more recently, to March 1, 2010*. Though the new compliance deadline provides additional time to implement the required information security measures, compliance efforts should not be delayed given the very specific requirements of the Security Regulations.

Scope

The Security Regulations have broad coverage, applying to any natural person or entity that owns, licenses, stores, maintains, processes or has access to any personal information of a Massachusetts resident, whether or not the person or entity has operations in Massachusetts. "Personal information" is defined as any combination of a Massachusetts resident's first and last name, or first initial and last name, with any of the following: (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. "Personal information" does 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.

Information Security Program Requirements

The Security Regulations require the development, implementation, maintenance and monitoring of a comprehensive, *written* information security program applicable to any records containing personal information, whether in *paper or electronic* form.

255 State Street
Boston, MA 02109
617.897.5600

1000 Elm Street
Manchester, NH 03101
603.668.0300

Two Eagle Square
Concord, NH 03301
603.223.2020

Two Maple Street
Hanover, NH 03755
603.643.9070



SHEEHAN PHINNEY BASS + GREEN PA
Attorneys at Law

The information security program must contain administrative, technical and physical safeguards to ensure the security and confidentiality of the records containing personal information. The safeguards contained in such program must be consistent with the safeguards for protection of personal information and information of a similar character set forth in any state or federal regulations by which the person who owns, licenses, stores or maintains such information may be regulated.

The most recent amendments to the regulations adopt a risk-based approach that requires the safeguarding of personal information to be appropriate to the size, scope, type of business, resources available, amount of personal information involved, and need for protection. This “risk-based” approach was intended to ease the burden of these regulations upon small businesses.

Whether an information security program is in compliance with the Security Regulations must be evaluated taking into account (i) the size, scope and type of business of the person obligated to safeguard the personal information under such program, (ii) the amount of resources available to such person, (iii) the amount of stored data, and (iv) the need for security and confidentiality of both consumer and employee information. Accordingly, such standard should permit small businesses to adopt reasonable information security programs. Every comprehensive information security program, however, *must* include:

- (1) **Designating one or more employees** to maintain the comprehensive information security program.
- (2) **Identifying and assessing** reasonably foreseeable internal and external **risks to the security**, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and **evaluating and improving**, where necessary, the effectiveness of the current **safeguards** for limiting such risks, including but not limited to: (i) ongoing employee (including temporary and contract employee) training; (ii) employee compliance with policies and procedures; and (iii) means for detecting and preventing security system failures.
- (3) **Developing security policies for employees** that take into account whether and how employees should be allowed to keep, access and transport records containing personal information outside of business premises.
- (4) **Imposing disciplinary measures** for violations of the comprehensive information security program rules.
- (5) **Preventing terminated employees from accessing records** containing personal information.
- (6) **Overseeing service providers** by taking reasonable steps to assure that they are capable of using measures that will protect personal information. Third party service providers must be required by contract to implement and maintain security measures to protect personal information. It appears, however, that any contract with a third party provider is deemed compliant until at least March 1, 2012.



SHEEHAN PHINNEY BASS + GREEN PA
Attorneys at Law

- (7) **Reasonable restrictions upon physical access to records** containing personal information and storage of such records and data in locked facilities, storage areas or containers.
- (8) **Regular monitoring** to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information; and upgrading information safeguards as necessary to limit risks.
- (9) **Reviewing the scope of the security measures** at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information.
- (10) **Documenting responsive actions** taken in connection with any incident involving a breach of security, **and mandatory post-incident review** of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

Computer System Security Requirements

In addition to the requirements to implement a comprehensive written information security program, every covered person or entity that owns, licenses, stores or maintains personal information about a Massachusetts resident and electronically stores or transmits such information shall include in its comprehensive information security program the establishment and maintenance of a security system covering its computers, including any wireless system, which, to the extent technically feasible, has the following elements:

- (1) **Secure user authentication protocols** including:
 - Control of user IDs and other identifiers;
 - A reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;
 - Control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;
 - Restricting access to active users and active user accounts only; *and*
 - Blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system.
- (2) **Secure access control measures** that:
 - Restrict access to records and files containing personal information to those who need such information to perform their job duties; *and*
 - Assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls.



SHEEHAN PHINNEY BASS + GREEN PA
Attorneys at Law

- (3) **Encryption of all transmitted records and files containing personal information** that will travel across public networks, and encryption of all data to be transmitted wirelessly.
- (4) **Reasonable monitoring of systems** for unauthorized use of or access to personal information.
- (5) **Encryption of all personal information stored** on laptops or other portable devices.
- (6) For files containing personal information on a system that is connected to the Internet, there must be **reasonably up-to-date firewall protection** and operating system security patches, reasonably designed to maintain the integrity of the personal information.
- (7) **Reasonably up-to-date versions of system security agent software** which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.
- (8) **Education and training of employees** on the proper use of the computer security system and the importance of personal information security.

To the extent they have not yet done so, all covered individuals and entities that own, license, store or maintain personal information of a Massachusetts resident, as defined in the Security Regulations, immediately should commence a review of their current security policies and procedures to determine whether they are and/or will be in compliance as of March 1, 2010, and develop the training programs necessary to comply with the Security Regulations requirements. Failure to comply may result in, among other things, the imposition of fines of up to \$5,000.00 for violation.

* * *

Mark J. Ventola is a shareholder at Sheehan Phinney Bass + Green PA. He is a member of the Labor and Employment Group. He may be reached at mventola@sheehan.com or 617.897.5630.

Maria E. Recalde is a shareholder at Sheehan Phinney Bass + Green PA. She is a member of the Intellectual Property and Technology Practice Group. She may be reached at mrecalde@sheehan.com or 617.897.5620.