WILMERHALE

Protection of Personal Information: Massachusetts Data Breach Law Goes Into Effect on March 1, 2010

2010-02-26

Final regulations implementing Massachusetts' security breach law, Massachusetts General Law c. 93H, go into effect on **March 1, 2010**. The regulations are codified at *201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth*.

The regulations were revised in August 2009 to clarify compliance deadlines and the requirements for contracts with third-party service providers who handle the "personal information" of Massachusetts residents.

Companies that own or license sensitive personal information about residents of Massachusetts must adopt a compliant Information Security Program by March 1, 2010 to protect that information. New contracts for vendors or service providers who will access covered information that are executed after March 1, 2010 must obligate the service provider to implement safeguards that are consistent with the Massachusetts requirements. All vendor contracts must include these provisions by March 1, 2012.

Who is Covered?

The regulations apply to any entity that receives, maintains, processes, stores or otherwise accesses certain personal information about a resident of Massachusetts.

The regulations are not limited to entities that do business in Massachusetts, but are designed to cover any entity with access to the personal information of Massachusetts residents. There is, however, some ambiguity as to whether Massachusetts could hold an out-of-state company liable for its handling of covered information collected in another state.

What Information is Covered?

The regulations seek to protect "personal information" about Massachusetts residents. Under the regulations, personal information encompasses an individual's first name and last name or first

initial and last name in combination with any of the following sensitive information: (a) Social Security number; (b) driver's license number or state-issued ID; 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, excluding public records data.

The regulations cover personal information whether stored in electronic or paper form.

How to Comply

Under the regulations, a covered entity that owns or licenses personal information about a Massachusetts resident must develop, implement, maintain and monitor a comprehensive, written "Information Security Program" that is appropriate to (a) the size, scope, and type of the covered business; (b) the covered business's resources; (c) the amount of stored data; and (d) the need for security and confidentiality of consumer and employee information to be protected. As part of that program, the covered entity must:

- Implement administrative, technical, and physical safeguards to ensure the security and confidentiality of such records. In addition, these safeguards must be consistent with existing state and federal law requirements for protection of information "of a similar character" (e.g., HIPAA, GLBA);

- Designate one or more employees to be responsible for maintaining the Information Security Program;

- Identify and assess reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of records containing personal information, and evaluate and improve, where necessary, the effectiveness of current safeguards for limiting such risks;

- Train employees on information security, and discipline them for violations of the Information Security Program rules; and

- Oversee service providers by taking reasonable steps to select service providers capable of protecting information and requiring by contract each service provider to implement and maintain appropriate security measures for personal information.

The regulations specify a number of practices and procedures that must be included in a compliant Information Security Program:

- Determining whether and in what manner employees are permitted to keep, access, and transport records containing personal information **outside of business premises**;

- Restricting access to electronic records containing personal information on a need to know basis using complex and unique ID plus password for **each** user (i.e., no group IDs),

which must be securely stored and terminated promptly when no longer needed; up to date firewall protection, security patches, agent software, malware protection, and virus definitions; and logging/monitoring tools to detect intrusions and misuse;

- Monitoring regularly the compliance with, and the adequacy of, the Information Security Program, including those times in which there is a **material change in business practices, but no less frequently than annually**;

- Documenting all information security breaches and responses in accordance with a **written incident response plan** that includes mandatory post-incident review of events and describes any modification of information security practices; and

- **Using encryption to protect electronic records**, including, to the extent technically feasible:

    - Mandating encryption for records and files containing personal information that are transmitted across public networks, and encryption of all personal information transmitted wirelessly; and

    - Requiring encryption for all personal information on laptops or other portable devices or media (e.g., thumb drives, CDs, PDAs, etc.).

What's New?

The regulations were amended in August 2009 to clarify their impact on service providers who handle personal information about Massachusetts residents for covered entities and timelines for compliance:

- The rules have been amended to make clear they apply to any service provider who "stores" the personal information of Massachusetts residents in connection with providing service to a covered entity, in addition to service providers who receive, maintain, process or otherwise have access to such personal information.

- The regulations require that a covered entity who contracts with a third party to handle covered data must include provisions in their service contracts to safeguard that data in a manner that complies with the Massachusetts regulations and federal law. New contracts executed **after March 1, 2010** must comply with the data protection rules in the new regulations. Existing service provider contracts need not be amended immediately, but must be updated by **March 1, 2012**.

- The rules were amended to clarify that the U.S. Postal Service is not excluded from the definition of Service Providers.

Compliance Timelines

All covered entities should be in compliance with the regulations on or before **March 1, 2010**. As a result, covered entities should take the following steps to comply by that date:

- Establish a compliant Information Security Program.

- Ensure new vendor or service provider contracts executed after **March 1, 2010** comply with the data protection obligations in the new regulations. Existing service provider contracts need not be amended immediately, but must be updated by **March 1, 2012**.