Client Alert

Standards for the Protection of Personal Information of Residents of the Commonwealth

By:Michael J. Cavaretta
March 17, 2009

What are the regulations?

Perhaps the most far-reaching personal information data security regulations in the country.

To whom do they apply?

All individuals, corporations, associations, partnerships and other legal entities (regardless of where they are located) who/that own, license, store or maintain personal information about a Massachusetts resident.

What constitutes "personal information"?

A Massachusetts resident's first name and last name or first initial and last name in combination 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.

What do the regulations require?

The development, implementation, maintenance and monitoring of a comprehensive, written information security program ("WISP") applicable to all records containing the personal information of Massachusetts residents.[1]

What are requirements for the WISP?

It must be reasonably consistent with industry standards and contain administrative, technical and physical safeguards to ensure the security and confidentiality of records containing the personal information of Massachusetts residents.

Among other things, the WISP must include the following:

- Designating an individual to be responsible for the program;
- Minimizing the use, retention and access of and to personal information;
- Protecting and restricting access to paper records and electronic records (including through password, encryption, and firewall technology); and
- Ensuring that third parties with access to personal information comply with the requirements.

Detailed descriptions of the elements that must be included in the WISP are described on Attachment A to this document (below).

What is the deadline for compliance?

January 1, 2010.

How will compliance be evaluated?

Whether the WISP is in compliance with the regulations will be evaluated taking into account:

(a) the size, scope and type of business of the party obligated to safeguard the personal information;

(b) the amount of resources available to the party;

(c) the amount of stored data; and

(d) the need for security and confidentiality of both consumer and employee information.

How will the regulations be enforced?

The regulations will be enforced by the Massachusetts Attorney General. In addition to civil fines assessed by the Attorney General, there is the potential for private (individual and class action) lawsuits, MGL Chapter 93A unfair and deceptive trade practice actions, and FTC unfair and deceptive trade practice actions. There is also the potential for failure to comply with the regulations constituting prima facie negligence.

Where can I get additional information?

The OCABR website contains some useful resources, including:

201 CMR 17.00 Compliance Checklist

Frequently Asked Questions Regarding 201 CMR 17.00

Attachment A:
Written Information Security Program (WISP) Requirements

A WISP must be reasonably consistent with industry standards for information security programs and must contain administrative, technical and physical safeguards to ensure the security and confidentiality of records containing the personal information of Massachusetts residents.

Specifically, the WISP must include (but need not be limited to) the following:

1. Designating one or more employees to maintain the WISP;

2. Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any records containing personal information;

3. Evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting identified risks, including but not limited to:

a. ongoing employee (including temporary and contract employee) training;

b. employee compliance with policies and procedures; and

c. means for detecting and preventing security system failures.

4. Developing security policies for employees that take into account whether and how employees should be allowed to keep, access and transport records (physical and electronic) containing personal information outside of business premises.

5. Imposing disciplinary measures for violations of the WISP rules.

6. Preventing terminated employees from accessing records containing personal information by immediately terminating their access (physical and electronic) to such records, including deactivating their passwords and user names.

7. With respect to third-party service providers with access to personal information:

> a. taking all reasonable steps to verify that they have the capacity to protect such personal information in the manner provided for in the regulations, and
>
> b. taking all reasonable steps to ensure that they are applying to such personal information protective security measures at least as stringent as those required to be applied to personal information under the regulations.

Written agreements and certifications are no longer required under the regulations, but requiring contractors to make appropriate representations and warranties in their service agreements is still advisable.

8. Limiting the amount of personal information collected to that reasonably necessary to accomplish the legitimate purpose for which it is collected.

9. Limiting the time personal information is retained to that reasonably necessary to accomplish the legitimate purpose for which it is collected.

10. Limiting access of personal information to those persons who are reasonably required to know such information in order to accomplish the legitimate purpose for which it is collected or to comply with state or federal record retention requirements.

11. Identifying which paper, electronic and other records, computing systems, and storage media (including laptops and portable devices) contain personal information, or providing for the handling of all records as if they all contained personal information.

12. Placing reasonable restrictions on the physical access to records containing personal information, including a written procedure that sets forth the manner in which physical access to such records is restricted, and storing such records and data in locked facilities, storage areas or containers.

13. Regularly monitoring to ensure that the WISP 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.

14. 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.

15. Documenting responsive actions taken in connection with any incident involving a breach of security, and conducting mandatory post-incident reviews of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

16. Establishing and maintaining a security system covering computers, including any wireless system, that electronically stores or transmits personal information that, at a minimum, will have

the following elements:

a. Secure user authentication protocols including:

i. control of user IDs and other identifiers;

ii. a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;

iii. 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;

iv. restricting access to active users and active user accounts only; and

v. blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system.

b. Secure access control measures that:

i. restrict access to records and files containing personal information to those who need such information to perform their job duties; and

ii. 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.

c. To the extent technically feasible, encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly.

d. Reasonable monitoring of systems, for unauthorized use of or access to personal information.

e. Encryption of all personal information stored on laptops or other portable devices.

f. 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.

g. 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.

h. Education and training of employees on the proper use of the computer security system and the importance of personal information security.

Footnote.

1. Not included in the regulations, but required under MGL Chapter 93H Section3, is the obligation to report known security breaches and unauthorized use of personal information.

Breaches and unauthorized use must be reported to the Massachusetts Attorney General, the Massachusetts Office of Consumer Affairs & Business Regulation ("OCABR"), and the owners of the personal information affected.