MURPHY HESSE TOOMEY & LEHANE LLP

Attorneys at Law

Client Advisory
October 2009

Data Security Law
MGL Chapter 93H and 201 CMR 17.00

For a discussion of these and other issues, please visit the update on our website at www.mhtl.com/law . To receive mailings via email, contact information@mhtl.com .

Massachusetts has recently adopted a new data security law. Massachusetts General Law Chapter 93H and its accompanying regulations, 201 CMR 17.00 *et seq*, are known as the Massachusetts Data Breach Notification Law. The deadline for compliance is March 1, 2010, by which time all businesses will need to create a Written Information Security Program (WISP). The law also requires immediate notification to individuals whose personal information has been compromised as a result of a security breach and includes requirements for the disposal of personal information.

Who is Covered?

Most offices and business are covered by the new law. Every person that owns, licenses, stores or maintains personal information about a resident of the Commonwealth must comply with these laws.

What Will Happen If I Do Not Comply?

The Attorney General can pursue civil penalties under MGL Ch. 93A. Residents may also pursue civil claims for violations. Ensuring that you comply with the new data security law will protect your business from potential breaches, and spare it the time, cost, and embarrassment that accompany attendant claims.

What is "Personal Information"?

The law defines "personal information" as a resident's first and last name or first initial and last name in combination with any 1 or more 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, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account. "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.

What is a "Security Breach"?

"Security breach" is defined as the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the Commonwealth. It is not necessary that the unauthorized acquisition or use is of personal information itself; as long as the data is "capable of compromising" personal information then it constitutes a security breach. Note that if you acquire personal information in good faith but without authorization and for lawful purposes, it is not a breach of security unless you use the personal information in an unauthorized manner or engage in further unauthorized disclosure.

When is the Notice Obligation Triggered?

The notice obligation is triggered when you know or have reason to know of a security breach or that personal information was acquired or used by an unauthorized person for an unauthorized purpose.

When Do I Have to Give Notice?

You must provide notice as soon as practicable and without unreasonable delay. The only circumstance in which notice may be delayed is when a law enforcement agency determines that providing notice might impede a criminal investigation. The law enforcement agency must have notified the attorney general of this in writing and must have informed you of this determination. Once the law enforcement agency informs you that there is no longer a risk that notice will impede any criminal investigation, you must provide notice.

To Whom Do I Have to Give Notice, and What Does Notice Consist of?

If you maintain or store (but you do not own or license) data including personal information, you must give notice to and "cooperate with" the owner or licensor of the data. Cooperation includes informing the owner or licensor of the breach of security or unauthorized acquisition or use, the date or approximate date of the breach, the nature of the breach, and any steps you have taken or plan to take relating to the incident. In cooperating, you do not have to disclose confidential business information or trade secrets, and you do not have to provide notice to a resident that may have been affected by the breach of security or unauthorized acquisition or use.

Phone (617) 479-5000 Fax (617) 479-6469
www.mhtl.com

If you own or license data including personal information, you must give notice to: 1) the Attorney General; 2) the Office of Consumer Affairs; and 3) the resident. When you give notice to the attorney general and OCA, and any consumer reporting agencies or state agencies, you must include the nature of the breach, the number of residents of the Commonwealth affected by the breach at the time of notification, and any steps you have taken or plan to take relating to the breach. When you give notice to the resident, you must include the consumer's right to obtain a police report, how a consumer requests a security freeze and the necessary information to be provided when requesting the security freeze, and any fees required to be paid to any of the consumer reporting agencies. You do not have to inform the resident of the nature of the breach or the number of residents of the Commonwealth affected by the breach.

How Do I Notify Someone of a Breach?

Notice includes written notice; electronic notice (if provided consistent with the provisions regarding electronic records and signatures in § 7001 (c) of Title 15 of the United States Code and chapter 110G); or substitute notice.

What is "Substitute Notice"?

You can provide substitute notice if you can demonstrate that the cost of providing written notice will exceed $250,000, or that the affected class of Massachusetts residents to be notified exceeds 500,000 residents, or that you do not have sufficient contact information to provide notice. Substitute notice is generally for security breaches of such a large scale that written notice would be impracticable. If you uncover such a breach you can provide substitute notice by taking *all* of the following three steps: 1) electronic mail notice, if you have electronic mail addresses for the members of the affected class of Massachusetts residents; *and* clear and conspicuous posting of the notice on your home page if you maintain a website; *and,* 3) publication in or broadcast through media or medium that provides notice throughout the Commonwealth.

What Kind of Program Am I Required to Adopt, and By When?

By March 1, 2010, you must have a Comprehensive Written Information Security Program (WISP) in place. The law recognizes that there is not a one-size-fits-all WISP. Compliance depends on the size, scope and type of your business; (ii) the amount of resources available to you; (iii) the amount of stored data; and, (iv) the need for security and confidentiality of both consumer and employee information.

Phone (617) 479-5000 Fax (617) 479-6469
www.mhtl.com

WISP General Requirements:

- Must be comprehensive
- Must be reasonably consistent with industry standards
- Must contain administrative, technical, and physical safeguards

Specific Requirements:

State regulations require that you: 1) appoint an employee to maintain the program; 2) identify risks to personal information, evaluate current safeguards, and make necessary improvements (this step may include employee trainings, compliance monitoring; upgrading information systems; storing records in locked facilities; and improving means for detecting, preventing and responding to security breaches); 3) limit the amount of personal information that you collect and maintain to accomplish a legitimate purpose; 4) limit the amount of personal information that you retain to that which is reasonably necessary to accomplish the legitimate purpose; 5) limit access of the personal information to those who are reasonably required to know.

Additionally, the regulations require that your WISP includes security policies for employees who telecommute; disciplinary procedures for rule violations; and policies for preventing terminated employees from accessing personal information. It must address how you will take reasonable steps to ensure that third-party service providers can protect any personal information to which they have access. Your WISP also must provide for inventorying where personal information is kept and monitoring employee access to personal information.

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) you must review the scope of your security measures. Your WISP must include this provision.

You are also required to document responsive actions that you have taken in connection with any incident involving an actual or potential 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. Your WISP must address this requirement.

Phone (617) 479-5000 Fax (617) 479-6469
www.mhtl.com

Computer System Security Requirements:

The regulations impose minimum security system requirements for your computers. The areas that you should focus on include authentication; restricting access; encryption; and firewall and virus protection.

1. *Secure user authentication protocols* including: control of user IDs and other identifiers; a secure method of assigning and selecting passwords consisting of at least seven letters and numbers; control of data security passwords to ensure that such passwords are kept at a location separate from that of the data to which such passwords permit access; 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 a unique identification plus a password, which is not vendor supplied, to each person with computer access.

3 *Encryption* of all transmitted records and files containing personal information, including those in wireless environments, that will travel across public networks.

4. *Periodic monitoring* of networks and systems, for unauthorized use of or access to personal information, and recording the audit trails for users, events, dates, times and success or failure of login.

5. *Periodic review* of audit trails restricted to those with job-related need to view audit trails.

6. For files containing personal information on a system that is connected to the Internet, there must be *firewall protection* with up-to-date patches, including operating system security patches. A firewall must, at a minimum, protect devices containing personal information from access by or connections from unauthorized users.

7. The most *current version of system security agent software* which must include antispyware and antivirus software, including 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 which includes security software that is set to receive the most current security updates on a regular basis.

Phone (617) 479-5000 Fax (617) 479-6469
www.mhtl.com

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

9. *Restricted physical access* to computerized records containing personal information, including a written procedure that sets forth the manner in which physical access to personal information is restricted. When notified of any unauthorized entry into a secure area by either an employee or any other unauthorized person, the integrity of the computerized records must be reviewed.

How Do I Properly Dispose of Personal Information?

MGL Chapter 93I addresses the disposition and destruction of records. It requires that you dispose of *paper documents* containing personal information by redacting, burning, pulverizing or shredding so that personal data cannot practicably be read or reconstructed; and that you dispose of *electronic media and other non-paper media* containing personal information by destroying or erasing so that personal information cannot practicably be read or reconstructed.

* * * * * * * * * * *

If you have additional questions about the new Massachusetts Data Security Law, contact Donald Graham at dgraham@mhtl.com or the attorney assigned to your account.

This alert is for informational purposes only and may be considered advertising. It does not constitute the rendering of legal, tax or professional advice or services. You should seek specific detailed legal advice prior to taking any definitive actions.

Phone (617) 479-5000 Fax (617) 479-6469
www.mhtl.com