



THE NEW MASSACHUSETTS PRIVACY LAW: THE FIRST LAW YOU MAY VIOLATE IN 2010

INTRODUCTION

After several delays and clarifications, on March 1, 2010 Massachusetts General Law Chapter 93H and the accompanying regulation, (201 CMR 17.00: Standards for the Protection of Personal Information of Resident of the Commonwealth)¹ goes into effect. This regulation will place unprecedented information security requirements on every company that owns, licenses, stores or maintains paper or electronic personal information² concerning any Massachusetts resident. Unlike the current data breach laws, which are focused on actions that need to be taken after there is a data breach, this law includes numerous prescriptive, proactive measures intended to protect Massachusetts residents' personal information from breaches. More specifically, as stated in the regulation, "This regulation establishes minimum standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records. The objectives of this regulation are to insure the security and confidentiality of customer information in a manner fully consistent with industry standards; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer."

This law is applicable to any company dealing with the personal information of a Massachusetts resident. From a practical perspective, this law has a broad impact on many companies, as it is not practical, and not wise, to segment personal information based on residency and to apply different security measures only to that data protected by this law. As in the case of the first data breach law in California several years ago, all personal information possessed by a company will likely benefit from the requirements in the Massachusetts law. This regulation recognizes that compliance will vary depending on the size of the company, amount of personal information, the amount of available resources and the need for security and confidentiality of both consumer and employee information.

¹ <http://www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf>

² Defined in the regulation as "a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (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; provided, however, that "Personal information" shall 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."

LEGAL REQUIREMENTS

The regulation requires that certain policies, procedures and technology controls be in place to protect personal information on a continuous basis. Major requirements of this regulation require affected companies to:

- Maintain a Written Information Security Program (WISP);
- Designate one or more employees to maintain the information security program;
- Identify and assess 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 as exist in the company and at service providers³ (This will require that you know where personal information exists, or more specifically, where there is a personal information inventory.);
- Provide on-going training, including temporary and contract employees, for the proper use of the computer security system and the importance of personal information security;
- Implement policies with disciplinary action for non-compliance;
- Have a means for preventing and detecting system security failures;
- Develop security policies for employees relating to the storage, access and transportation of records containing personal information outside of business premises;
- Take reasonable steps to select and retain third-party service providers who are capable of, and agree in contract to, maintaining appropriate security measures to protect such personal information consistent with these regulations and any applicable federal regulations;
- Limit the collection, access to, and storage of personal information;
- Implement reasonable restrictions upon physical access to records containing personal information, and storage of such records and data in locked facilities, storage areas or containers;
- Regularly monitor 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;
- Review 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; and
- Maintain an incident response plan.

³ Defined in the regulation as “any person that receives, maintains, processes, or otherwise is permitted access to personal information through its provision of services directly to a person that is subject to this regulation; provided, however, that “Service provider” shall not include the U.S. Postal Service.”

There are also specific computer system security requirements included in the regulation as summarized below. Companies that electronically store or transmit personal information pertaining to a Massachusetts resident must:

- Control user IDs and other identifiers that provide access to computer systems;
- Have a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;
- Control system 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;
- Restrict access to active users and active user accounts only (e.g., no terminated employee should continue to have system access);
- Block access to the systems after multiple unsuccessful attempts to gain access, or place limitations on access to the particular system;
- Restrict access to records and files containing personal information to those individuals who need such information to perform their job duties;
- Assign unique identifiers plus passwords, (reasonably designed to maintain the integrity and security of the access controls) to each person with computer access. These should not be vendor supplied default passwords.
- Encrypt all transmitted records and files containing personal information that will travel across public networks, and encrypt all personal information to be transmitted wirelessly;
- Implement a process for the reasonable monitoring of systems, for unauthorized use of or access to personal information;
- Encrypt all personal information stored on laptops or other portable devices;
- Implement reasonably up-to-date firewall protection and operating system security patches, designed to maintain the integrity of the personal information in any files on a system that is connected to the Internet; and
- Maintain 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.

IS YOUR COMPANY IN COMPLIANCE?

As you reflect on the list of requirements think about whether your company will comply by March 1. If your company is subject to other requirements such as the Payment Card Industry Data Security Standard (“PCI DSS”) some of the elements in this regulation will already have been addressed as part of those compliance efforts. While a legitimate point of view is that the requirements in this regulation are reasonable and prudent, many companies will find it difficult to comply with all of the requirements as the reality of a challenging economic environment persists and resources tend to be dedicated to revenue generating and cost cutting activities. Nonetheless, all companies will need to address these requirements or face the consequences, both in a court of law and the court of public opinion. The State Attorney General may pursue civil penalties. In addition, affected individuals may pursue civil actions. Perhaps even more important, a violation will likely result in adverse publicity and degradation of your customer or employee trust and loyalty.

SUGGESTIONS

There is relatively little time remaining until this regulation becomes effective and if your company is not already compliant, activities to achieve compliance should be carefully prioritized. The following general suggestions will help you in your compliance efforts.

Personal Information Minimization - protecting all personal information in every existing location can be a very expensive strategy. The most impactful action you can take is also the most obvious – limit the amount of personal information that needs to be protected. A core business practice should be to only collect the minimum amount of personal information required to execute the business transaction, manage your workforce, or meet any applicable legal requirement. The less personal information that is collected and stored, the less that has to be protected and is at risk of breach. This can require simple or significant changes to current business processes and information systems but is worth the effort.

Eliminating Duplicate Information - duplicate personal information is a common occurrence and can be identified by conducting a personal information inventory. As an example, some golf country clubs maintain a payment authorization form with the member's credit card details and also keep a photocopy of the credit card. This practice is not only unnecessary, it also creates an extra paper record of the credit card that now must be protected and is subject to loss or theft. In addition, maintaining a photocopy of a credit card violates PCI DSS because the security code on the front or back of the card cannot be stored after transaction authorization.

Numerous instances of the same personal information can also be found in computer systems, files on desktops or laptops, network servers, back-up tapes, portable media such as flash drives, CDs or back-up tapes and also in paper records. Each of these instances of personal information must be protected and represents a data repository that can be lost or stolen. The cost to protect duplicate personal information can be substantial, not to mention the storage costs. Every reasonable effort should be made to minimize both personal information collected, and the locations where it is stored to meet your business and legal needs.

Personal Information Disposal - after identifying duplicate information, it is important that such duplications can be securely eliminated. For paper based records it is fairly straightforward, since a cross cut shredder or third party shredding service can be used to securely destroy this data. Information stored on electronic media such as desktops, laptops, servers, flash drives, etc., should be securely and permanently deleted. Technically, the information on these electronic devices could be restored with specialized software unless the disk space is overwritten or the device is destroyed. If the duplicate information targeted for deletion resides on electronic devices that are no longer needed such as old laptops, this information should be permanently deleted prior to hardware disposal. In either case, if you do not have internal IT resources that have access to the specialized software to permanently delete all the information, you should use a third party service provider that specializes in secure deletion of information from electronic devices. These service providers can also ensure that any devices to be disposed of, meet Environmental Protection Agency requirements.

Do What You Can as Fast as You Can - regardless of your current state, any tasks no matter how modest, that can be completed to strengthen your company's compliance are worthwhile. It is not always practical to complete all tasks as quickly as desired but delaying any action is not prudent. Instead, do as much as you can as fast as you can. As previously stated, the regulation recognizes that compliance activities will vary depending on the amount of available resources. You should anticipate that a regulator will likely expect more of your organization than mere company management.

Important Note: This paper is provided for informational purposes only, and is not intended and should not be considered to be legal advice.

About Navigate LLC

Navigate LLC is a business consultancy that is focused on providing pragmatic, comprehensive, high value strategic and tactical information privacy advisory services to the commercial and government sectors. Navigate was founded by Chris Zoladz who most recently served as the Vice President of Information Protection & Privacy at Marriott International, Inc. from 1999-2009. For more information on how Navigate LLC can assist your company, please call 240-475-3640 or send an email to info@navigatellc.net.

© Navigate LLC 2010.