

MFA Perspective

201 CMR 17.00: The Massachusetts Privacy Law

Compliance is Mandatory... Be Thorough but Be Practical

**DEADLINE FOR FULL COMPLIANCE HAS BEEN EXTENDED
FROM JANUARY 1, 2010 TO MARCH 1, 2010**



MOODY, FAMIGLIETTI & ANDRONICO
Certified Public Accountants & Consultants

201 CMR 17.00: THE MASSACHUSETTS PRIVACY LAW

— Deadline for Full Compliance Has Been Extended from January 1, 2010 to March 1, 2010 —

Compliance is Mandatory... Be Thorough But Be Practical

In the wake of security breaches at such high profile companies as TJX and Hannaford Supermarkets, the Commonwealth of Massachusetts enacted a law (201 CMR 17.00) designed to protect state citizens' personal information. This law, which has already been revised and postponed three times, now requires all covered entities to achieve full compliance by March 1, 2010. This new deadline, announced on August 17, 2009, provides an extra two months for companies to achieve compliance.

While past breach-notification laws addressed what must happen in the wake of a security breach, the new Massachusetts regulations are intended to prevent personal information from being breached in the first place. The focus of the new regulations centers on implementing security measures designed to "prevent" intentional wrongdoing and inept internal data handling protocols.

This is a justified exercise, as the problem is a dangerous one that is not limited to the large public companies. If unchecked, it will continue to spread and leave Massachusetts residents exposed to any number of fraudulent activities. According to the State Office of Consumer Affairs and Business Regulation ("OCABR"), in a little over a year's time, the State received over 450 notifications of breaches affecting over 700,000 residents. Over 60% of these cases were due to criminal activity while the remainder was a result of employee error or careless internal handling of personal data. Almost 75% of the compromised data was neither password-protected nor encrypted.

The State is therefore placing an emphasis on prevention and, through this new law, mandating that sensitive information be handled according to protocol to help ensure its safekeeping.

NOTEWORTHY DETAILS OF THE NEW MASSACHUSETTS PRIVACY LAW

The latest rendition of the regulations (August 2009) adopts a risk-based approach to information security and takes into consideration business size and the amount of personal data being handled. The regulations no longer mandate every aspect of an information security program but rather offer a level of flexibility in compliance for small businesses. They direct businesses to establish a plan that takes into account their size and scope of business, availability of resources, nature and quantity of data stored, and the need for security and

confidentiality of both consumer and employee information.

THE CURRENT SCOPE OF THE NEW MASSACHUSETTS PRIVACY LAW

It's important to be able to decipher the new regulations and extract the salient information before embarking on any compliance efforts. First and foremost, it's crucial to understand the scope of the law and whether or not the law applies to your specific organization. Below is a brief synopsis of the key points:

- The regulations apply to those engaged in commerce. More specifically, it applies to all persons that "own or license" personal information from a resident of the Commonwealth. To further clarify, the State has defined "owns or licenses" to mean:

"Receives, maintains, processes, or otherwise has access to personal information in connection with the provision of goods or services or in connection with employment."

- Under the law, "personal information" to be protected includes a Massachusetts resident's name (either first and last name or first initial and last name) combined with a complete social security number, driver's license, or other state-issued number, a financial account number or a complete credit card or bank account number. This encompasses a wide variety of informational records - everything from employee, client, customer and investor records to supplier, patient and student records. What it does not include is any information that is lawfully obtained from publicly available information or from federal, state or local government records lawfully made available to the general public. A person's date of birth is an example of publicly available information that would not be protected under this law.
- The regulations are not explicitly limited to companies doing business in Massachusetts; whether located in RI, ME, CT, NH or any other state for that matter, if any personal information of Massachusetts residents is being handled, these regulations apply.

FAILURE TO COMPLY

Are there consequences for non-compliance? Absolutely!

Many facets of the new Massachusetts Privacy Law increase a company's exposure to lawsuits. The ramifications of not complying become quite real should an information breach occur. In such a case, if it is determined at the examination that the law's compliance requirements have not been met, the Massachusetts Attorney General can file suit with the company.

In addition, civil penalties could be imposed for non-compliance with Massachusetts' data breach notification statute (Massachusetts General Law 93H.) A civil penalty of \$5,000 may be awarded for each violation of 93H. Furthermore, under the portion of 93H concerning data disposal, businesses can be subject to a fine of up to \$50,000 for each instance of improper disposal.

Other "softer" consequences of failure to comply include damages to a company's reputation as well as the time and resources required to determine the cause and extent of a breach, notifying affected individuals of a breach, and implementing corrective action to ensure a breach does not occur in the future.

THE TIME TO GET STARTED IS NOW - COMPLIANCE WILL TAKE CONSIDERABLE EFFORT

When it's all said and done, the most significant aspect of the August 2009 revised regulations is really just that companies now have an additional two months to comply. While the State's new risk-based approach to information security attempts to balance consumer protections with business concerns by providing a level of flexibility for small businesses, the basic premise and intent of the law has not changed. While it may seem like you have plenty of time to address this compliance requirement, MFA urges companies not to underestimate the complexity of the new regulations and strongly recommends companies, especially those with little or no security infrastructure, immediately begin taking steps toward compliance as the mere existence of these new state regulations adds to an organization's risk.

MFA's experience in working with clients to achieve compliance has shown that the best course of action is to begin by conducting an organizational assessment as soon as possible. This detailed evaluation of your current information security policies will yield a full understanding of the gaps between current policies and regulatory requirements and will provide ample time to align resources to develop and implement a practical course of action for compliance.

CREATING A WRITTEN INFORMATION SECURITY PLAN (WISP) IS A KEY COMPONENT OF COMPLIANCE

Under 201 CMR 17.00, the Massachusetts Privacy Law, applicable individuals and businesses must develop, implement, maintain and monitor a **comprehensive, written information security program (WISP)** to ensure the security and confidentiality of personal information in both **physical and electronic format**. The actual scope and complexity of a WISP

will vary depending on an organization's size and scope of business, availability of resources, nature and quantity of data stored, and the need for security and confidentiality of both consumer and employee information.

While navigating one's way through the creation of a WISP, it's important to stay focused on the overall objective which is to develop reasonable and effective administrative, technical and physical safeguards for the protection of personal information belonging to residents of Massachusetts. Certain provisions of the new regulations are very specific; making it relatively easy to understand what is required in order to be compliant. Unfortunately, there are also a number of provisions that are somewhat ambiguous. To assist in preparing companies for compliance, MFA has outlined a list of recommended action items that should be addressed in a WISP by March 1, 2010.

1. Information Assessment

- **Identify Records Containing Personal Information of Massachusetts Residents.** Under the August 2009 revised regulations, it is no longer necessary to "inventory" all paper and electronic records containing personal information although, in reality, in order to properly implement a risk-based approach to information security, you will still need to identify which records contain personal information so that you can properly handle and protect that information.
- **Understand Your Current Information Handling Processes.** Review your current processes for collecting, retaining and using personal information belonging to Massachusetts residents. While the August 2009 revised regulations no longer require you to specifically include this information in your WISP, as part of your efforts to ensure compliance with the Massachusetts Privacy Law, you will need to gain a full understanding of the amount of personal information collected, the length of time it is retained, and who in the organization has access to it.
 - What personal information is collected?
 - In what form (hardcopy and electronic) is personal information being collected?
 - What becomes of this collected information?
 - What becomes of the completed forms used to initially collect the personal information?
 - If the personal information is stored electronically, who has access to it?
 - How is this information disposed of after it is no longer needed?

- **Shore Up Loose Ends and Document Them.** If the above process flow audit identifies any loose ends with regard to unauthorized access or unauthorized use of personal information, institute and document corrective actions to shore up these loose ends and ensure that reasonable restrictions on access are in place, including safeguards for limiting your risk of both internal and external threats.
- **Limit the Amount of Personal Info Collected.** Examine the personal information collected. Is it limited to the amount reasonably necessary to accomplish your legitimate business purposes or to comply with state or federal regulations? While not mandated under the August 2009 revised regulations, it is good business practice to limit the collection of personal information to only that which you absolutely need.
- **Retain Info Only as Long as Necessary.** Maintain personal information records only as long as needed. Again, this is no longer mandated by the regulations but rather is good business practice.
- **Designate a Data Security Coordinator.** The Massachusetts Privacy Law explicitly states that one or more of your employees must be designated as an information security coordinator and charged with maintaining your information security plan. The responsibilities of the coordinator(s) should include:
 - Initial implementation of the plan
 - Initial training of employees including temporary and contract employees (annually thereafter)
 - Regular testing of the plan's safeguards
 - Annual review of the scope of the plan or whenever there is a material change in business practices that may affect the security or integrity of records containing personal information
 - Evaluating the ability of third party service providers to comply with 201 CMR 17.00

2. Personal Information Access

Under the August 2009 revised regulations, you no longer need to include in your WISP a written procedure that sets forth the manner in which physical access to such records is restricted. It merely states that you need to have reasonable restrictions on physical access to records containing personal information. As such, MFA recommends the following best practices be implemented to reasonably restrict access.

- **Keep It Under Lock & Key.** All hard copy records containing personal information belonging to Massachusetts citizens should be stored in locked facilities, storage areas or containers.
- **Restrict Access to Info.** Access to records containing personal information, whether in hardcopy or electronic format, should be limited to those who require it in order to perform any part of their job function.
- **Establish Policies for Off-Site Use of Personal Information.** Develop security policies for employees relating to the storage, access and transportation of records containing personal information outside of your business premises.
- **Guard Against External Threats.** Up-to-date security tools, firewall protection, malware protection, antivirus definitions and operating system security patches should be in place for all systems processing personal information.
- **Visitor Procedures — Tighten Up Access to Your Facilities.** Depending on the size and layout of your facilities, it may be prudent to restrict visitor access to one entry point for each building in which personal information is stored. Barring that, at a minimum, you should establish visitor procedures that include requiring visitors to present a photo ID, sign in and wear a visible “Guest” tag or badge. In addition, it’s always a good policy to require visitors to be escorted in all areas of the facility where personal information is stored.

3. Computer Security Requirements – “Technically Feasible” is the Key Here

The State has acknowledged that technical feasibility plays a large role in what businesses, especially small businesses, can do to protect data. Under the August 2009 revised regulations, all computer security requirements of 201 CMR 17.00 still apply to a business **IF** they are “technically feasible”. The State has defined “technically feasible” to mean that if there is a reasonable means through technology to accomplish a required result, then that reasonable means must be used.

As part of your WISP, you must establish and maintain a security system covering your computers, including any wireless systems, that, at a minimum, and to the extent “technically feasible”, includes the following elements.

- **Secure User Authentication Protocols.** These protocols must include control of user IDs and other identifiers; a reasonably secure method of assigning and selecting passwords; control of password security; restricting access to active users; and blocking access after multiple attempts.
- **Secure Access Control Measures.** These measures must include restricting access to records and files containing

personal information to those who “need to know” to perform their jobs as well as assigning unique IDs and passwords (not shared nor vendor supplied default passwords.)

- **Monitoring for Unauthorized Use or Unauthorized Access.** Reasonable monitoring of systems for unauthorized use of or access to personal information is required. There are a variety of methods and tools available in order to effectively monitor and protect against unauthorized activity - intrusion detection tools, application logs, server firewalls, network security logs and file system auditing, to name a few.
- **Firewall Protection and OS Patches.** For files containing personal information on a system that is connected to the Internet, you must implement and maintain “reasonably up-to-date” firewall protection and operating system security patches.
- **Viruses and Malware.** You must implement and maintain “reasonably up-to-date” versions of system security agent software that includes malware protection and “reasonably up-to-date” patches and virus definitions. Additionally, you must be set up to receive the most current security updates on a regular basis.

4. Encryption

Laptops, portable devices, backup tapes, email and public network and wireless transmissions containing personal information require encryption where it is “reasonable and technically feasible”. What the State has done as part of its August 2009 revised regulations is amend the definition of encryption to make it technology neutral and thus leave the door open for businesses to adopt new encryption standards and technologies as they evolve.

- **Encrypt Transmitted Records Containing Personal Info.** If it is technically feasible to do so, outgoing emails containing personal information, as well as any personal information traveling across public networks or transmitted wirelessly, should be encrypted. If it is not “technically feasible” to encrypt, you are not exempt from your duty to protection such personal information. In such instances, the State would expect you to implement best practices by not sending unencrypted personal information in an email.
- **Encrypt Portable Devices Containing Personal Info.** Not all portable devices need to be encrypted. Only those portable devices that contain personal information should be encrypted and, again, only if it is “technically feasible”. The State recognizes that at this point in the development of encryption technology, there is little, if any, accepted encryption technology for most portable devices (cell phones, Blackberries, iPhones, Netbooks, etc.) However, the State

does stress that while it may not be possible to encrypt such portable devices, personal information should not be placed at risk in the use of such devices. Note: Laptops are an exception to this as technology is available to encrypt laptops.

- **Don't Ignore Your Web Site.** Company or third party web portals onto which the personal information of Massachusetts citizens is entered should be verified as being secure.

5. Vendor Management

- **Evaluate the Capacity of Your Third Party Service Providers.** The regulations require you to take reasonable steps to select and retain third party service providers who are capable of maintaining appropriate safeguards to protect personal information. Such security measures should be consistent with those set forth under 201 CMR 17.00 and any applicable federal regulations.

The State defines a service provider 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. Simply put, this includes any vendors who handle personal information of Massachusetts citizens on your behalf (e.g., background check services, payroll services, life and health insurance providers, 401K administrator services, credit card processing firms, etc.) Note: It specifically excludes the U.S. Postal Service.

- **Third Party Service Providers Must Be Contractually Obligated to Implement and Maintain Appropriate Security Measures.** The August 2009 revision to the regulations has added back in the requirement for businesses to enter into written contracts with their third party service providers requiring them to implement and maintain appropriate measures for protecting personal information. The revised regulations provide a 2-year window in which businesses will need to amend all applicable third party service provider contracts. All contracts entered into prior to March 1, 2010 will be deemed to be in compliance with this obligation until March 1, 2012, even if no such language exists in the contract.

6. Employee Issues

- **Train Employees on an Ongoing Basis.** On an ongoing basis, train employees (inc. temporary and contract employees) on the proper use of computer security system and the importance of personal information security.
- **Document Employee Attendance at Training Sessions.** As a standard practice, all attendees at these training sessions should certify their attendance at the meeting and their familiarity with the company's requirements for protection of personal

information.

- **Impose Disciplinary Measures for Violations.** You must establish and enforce disciplinary measures for employees who violate the security program's rules.
- **Prevent Terminated Employees from Accessing Personal Information.** You must have measures in place to prevent terminated employees from accessing records containing personal information. It is good practice to immediately terminate their physical and electronic access to such records, including deactivating their passwords and user names.

7. Ongoing Monitoring

- **Regular Monitoring of Information Security Program.** The new Massachusetts Privacy Law requires companies to conduct regular reviews of their information security policies for relevancy and operational effectiveness as well as regular reviews of organizational adherence to the established operational protocols. The regulations state that these reviews must be conducted on an annual basis (at a minimum) or whenever there is a material change in business practices that may affect the security or integrity of records containing personal information.

SOME FINAL THOUGHTS ON THE MASSACHUSETTS PRIVACY LAW

While it is welcome news that the Massachusetts Office of Consumer Affairs and Business Regulation ("OCABR") has once again delayed compliance, the additional two months it gives companies does not mean one should delay efforts toward compliance. March 1, 2010 will arrive sooner than one may think. The design and implementation of a comprehensive written information security program can require considerable time and resources, as well as careful planning and oversight. Companies that delay run the risk of being in dangerous territory when the deadlines pass.

Begin by evaluating your existing information security policies – you can do that yourself or you may wish to seek an independent assessment. You might very well find that your existing policies cover many aspects of the new regulations, particularly if your company is already compliant with HIPAA, PCI or the myriad of financial information security regulations in place today. However, some companies will find they are a long way off from compliance and will most certainly have their work cut out for them.

Once a proper assessment has been completed and the gaps between current policies and regulatory requirements have been identified, you can realistically gauge the scope of work and decide whether or not outside assistance is necessary in order to meet the compliance date of March 1, 2010. Leveraging the expertise and resources of a third party can, in many instances, be a wise decision that may in the long run be the best way to ensure your organization's compliance.

FURTHER INFORMATION

For further information on the new Massachusetts Privacy Law, please link to the following documents.

- [MFA Alert: The Latest on the Massachusetts Privacy Law \(201 CMR 17.00\)](#)
- [August 2009 Revised Regulations \(201 CMR 17.00\)](#)
- [Redlined Version of August 2009 Regulations \(201 CMR 17.00\)](#)
- [Frequently Asked Questions Regarding 201 CMR 17.00](#)
- Understand how MFA can help in your efforts toward compliance: [MFA's Privacy and Data Protection Services](#)

FOR MORE INFORMATION, PLEASE CONTACT:

Matthew Pettine, CGEIT, CISA, ASE, MCSE, MCDBA
Managing Director
mpettine@mfacornerstone.com
(978) 557-5354

Material Discussed in this Perspective Issue is meant to provide general information and should not be acted on without obtaining professional advice tailored to your firm's individual and specific needs. This information is for general guidance only and is not a substitute for professional advice.

IRS CIRCULAR 230 DISCLOSURE: To ensure compliance with requirements imposed by the IRS, we inform you that any U.S. tax advice contained in this communication (including any attachments) is not intended or written to be used, and cannot be used, for the purpose of (i) avoiding penalties under the Internal Revenue Code or (ii) promoting, marketing or recommending to another party any transaction or matter addressed herein.



MOODY, FAMIGLIETTI & ANDRONICO
Certified Public Accountants & Consultants

MFA - Moody, Famiglietti & Andronico, LLP
1 Highwood Drive, Tewksbury, MA 01876
(978) 557-5300 www.mfa-cpa.com