



Date: November 6, 2008

## **201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth of Massachusetts**

### Should you be concerned?

#### 1.0 What is 201 CMR 17.00 ?

Massachusetts adopted regulations on Sept. 22, 2008, that will require businesses, wherever located, that store or use information about Massachusetts residents, to implement comprehensive information security programs by Jan. 1, 2009. It is a new law that needs to be met by persons who own, license, store or maintain personal information about a resident of the Commonwealth of Massachusetts. This regulation establishes minimum standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records.

#### 2.0 Overview of compliance requirements

Every person that owns, licenses, stores or maintains personal information about a resident of the Commonwealth shall develop, implement, maintain and monitor a comprehensive, written information security program applicable to any records containing such personal information. Such comprehensive information security program shall be reasonably consistent with industry standards, and shall contain administrative, technical, and physical safeguards to ensure the security and confidentiality of such records.

#### 3.0 Is your Business Affected by this new regulation?

If you store a Massachusetts resident last name and first name on computer or on paper AND also store any of the following information, this is considered “personal information” and the new law is applicable to you business.

1. Social Security number
2. Driver's License number
3. Financial Account number (credit card, debit card)
4. Access code that would allow you to access that person financial information

“Personal information” is defined as information including 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;

#### 4.0 What do you need to do internally to meet these requirements?

The requirements may differ based on types and sizes of businesses but a good set of recommendations that you can deploy and implement internally are:

- A. Designate one employee to design, implement and coordinate the maintenance of the comprehensive information security program;
- B. Identify and assess internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information in each relevant area of the business's operations
- C. Develop a security policy for employees who tele-commute that take into account whether and how such employees should be allowed to keep, access and transport data containing personal information.
- D. Consider implementing disciplinary measures for violations of the comprehensive information security program rules.
- E. Prevent terminated employees from accessing records containing personal information by immediately terminating their physical and electronic access to such records, including deactivating their passwords and user names.
- F. Take all reasonable steps to verify that third-party service providers with access to personal information have the capacity to protect such personal information, including (i) selecting and retaining service providers that are capable of maintaining safeguards for personal information; and (ii) contractually requiring service providers to maintain such safeguards. Prior to permitting third-party service providers access to personal information, the person permitting such access shall obtain from the third-party service provider a written certification that such service provider has a written, comprehensive information security program that is in compliance with the provisions of these regulations.
- G. Collect the minimum amount of personal information necessary to accomplish the legitimate purpose for which it was collected; retain such information for the minimum time necessary to accomplish such purpose; and permit access to the smallest number of persons who are reasonably required to know such information in order to accomplish such purpose.
- H. Inventory all paper, electronic and other records, computing systems, and storage media, including laptops and portable devices used to store personal information, to identify those records containing personal information.
- I. Regularly monitor and audit employee access to personal information in order 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.
- J. 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.
- K. Document all responsive actions taken in connection with any incident involving a breach of security and document all post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

## 5.0 How can TSI assist you in implementing these regulations?

For the past seven years, TSI has played a very active role in assisting our clients with implementing security policies that are mandated by various compliance requirements such as PCI-DSS, GLBA and HIPAA. Our engineers are trained and on the latest security best practices and we use the latest security tools to validate our findings and implement security policies at our client's companies.

We can assist you with the IT requirements needed to meet these new regulations:

As part of our services, we will:

- ✓ Secure user authentication protocols making sure all users have distinct ID's and passwords
- ✓ Configure your system policies so all passwords will require of at least seven letters and numbers
- ✓ Develop and implement a configuration database to ensure that such passwords are kept at a location separate from that of the data to which such passwords permit access.
- ✓ Block access to suspicious users after unsuccessful attempts to gain access.
- ✓ Restrict access to records and files containing personal information to those who need such information to perform their job duties.
- ✓ Assign a unique identification plus a password, which is not vendor supplied, to each person with computer access.
- ✓ Implement encryption for all transmitted records and files containing personal information, including those in wireless environments.
- ✓ set-up and configure monitoring of your 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.
- ✓ Train your designated staff on how to review all audit trails and security logs.
- ✓ Make sure that your firewall is properly configured and updated with the latest firmware.
- ✓ Insure that all PC's and Servers containing personal information and connected to the Internet, have the latest up -to-date patches, including operating system security patches.
- ✓ Review your current version of system security agent software including antispysware and antivirus software, including up-to-date patches and virus definitions.
- ✓ Provide basic training manual for employees on the proper use of the computer security system and the importance of personal information security.

**If your business needs to comply with these regulations and are re interested in exploring what TSI can do for you, please call us at 508-543-6979 or contact us via email at: [info@tsisupport.com](mailto:info@tsisupport.com)**