

Massachusetts Extends the Deadline for Compliance with Data Security Regulations Until March 1, 2010

How does this impact you and your business? Do you have personal information about Massachusetts residents on your computer system or in your paper files, such as name, social security number, driver's license number, or bank account or credit card information? If so, you may be required under Massachusetts 201 CMR 17.00, *Standards for the Protection of Personal Information of Residents of the Commonwealth* to develop and maintain a comprehensive written information security program covering records containing such personal information.

The regulation seeks to establish minimum standards, ensure security and confidentiality, and protect and prevent unauthorized access or use of personal information. The goal is to reduce incidents of identity theft amongst Massachusetts residents. Affected persons and businesses must implement and maintain a written information security program to safeguard personal records by the March 1, 2010 deadline.

The program must be consistent with industry standards and include the following, at minimum under 201 CMR 17.00:

1. Designating one or more employees to maintain the comprehensive information security program;
2. Identifying and assessing 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, 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.
3. Developing security policies for employees that take into account whether and how employees should be allowed to keep, access and transport records containing personal information outside of business premises.
4. Imposing disciplinary measures for violations of the comprehensive information security program rules.
5. Preventing 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.
6. Taking all reasonable steps to verify that any third-party service provider with access to personal information has the capacity to protect such personal information in the manner provided for in 201 CMR 17.00; and taking all reasonable steps to ensure that such third party service provider is applying to such personal information protective security measures at least as stringent as those required to be applied to personal information under 201 CMR 17.00.
7. Limiting the amount of personal information collected to that reasonably necessary to accomplish the legitimate purpose for which it is collected; limiting the time such information is retained to that reasonably necessary to accomplish such purpose; and

tonneson+co

Certified Public Accountants & Consultants

401 Edgewater Place, Suite 300, Wakefield, MA 01880-6208 t. 781.245.9999 f. 781.245.8731 www.tonneson.com

limiting access to those persons who are reasonably required to know such information in order to accomplish such purpose or to comply with state or federal record retention requirements.

8. Identifying paper, electronic and other records, computing systems, and storage media, including laptops and portable devices used to store personal information, to determine which records contain personal information, except where the comprehensive information security program provides for the handling of all records as if they all contained personal information.
9. Reasonable restrictions upon 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 storage of such records and data in locked facilities, storage areas or containers.
10. Regular monitoring 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.
11. 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.
12. Documenting responsive actions taken in connection with any incident involving a 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.

Under 201 CMR 17.00, people or businesses that store or transmit personal information electronically must meet these additional system requirements:

1. Secure user authentication protocols including:
 - a. control of user IDs and other identifiers;
 - b. a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;
 - c. 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;
 - d. restricting access to active users and active user accounts only; and
 - e. 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:
 - a. restrict access to records and files containing personal information to those who need such information to perform their job duties; and
 - b. 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;
3. 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.

4. Reasonable monitoring of systems, for unauthorized use of or access to personal information;
5. Encryption of all personal information stored on laptops or other portable devices;
6. 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.
7. 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.
8. Education and training of employees on the proper use of the computer security system and the importance of personal information security.

The extension of the original deadline gives people and businesses more time to review their existing business operations and policies to determine if these new regulations apply. If so, the proper steps to develop and implement a new or revised plan consistent with Massachusetts regulations should be undertaken in the near term in order to be compliant for the approaching March 1, 2010 deadline.

If you have any questions about how your business is impacted by these new data security regulations, please contact your Tonneson + Co representative for more information.