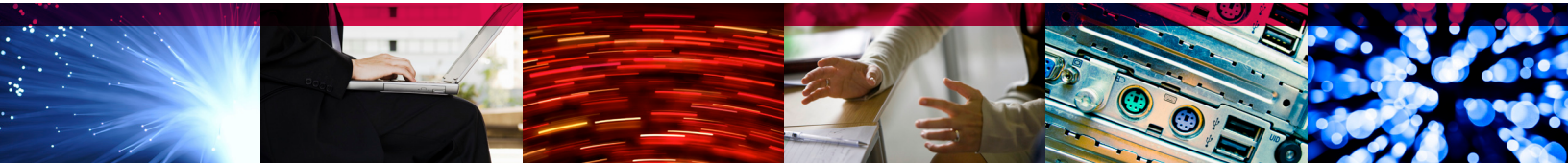


Do You Do Business in Massachusetts? Five Things to Know about 201 CMR 17 and Data Protection.



As of March 1, 2010, the Massachusetts General Law and its new regulations require that any company that stores or uses personal information about a Massachusetts resident must develop a written, regularly audited plan to protect the individual's personal information.

The law, known as 201 CMR 17, establishes minimum standards to be met in connection with the safeguarding of every individual's personal information contained in both paper and electronic records. Every company that owns or licenses personal information about a resident of Massachusetts must develop, implement and maintain a written, comprehensive information security program that is appropriate for the amount of stored data. Businesses need to secure not only their own networks, but they are responsible for ensuring their vendors/contractors are equally compliant and secure environments.

Here Are Five Things to Know about 201 CMR 17 and How It Can Impact Your Business:

1. Your information security program must be in writing. Everyone who owns or licenses personal information must have a written plan detailing the measures adopted. And, you must comply with 201 CMR 17 regardless of privileged or confidential communications.
2. Customer information must be encrypted if it contains personal information of customers or employees such as names, addresses, Social Security or credit card numbers. Password protection does not equate with encryption. For example – if data is password protected when stored on a laptop and transmitted wirelessly that is NOT enough to satisfy this encryption requirement. The data must be altered into an unreadable form; password protection does not alter the condition of the data as required.
3. The regulation requires encryption of portable devices that contain personal information of customers or employees.
4. There is no maximum period of time for which companies should retain documents containing personal information. As a good business practice, companies should limit the amount of personal information collected to that which is reasonably necessary to accomplish the legitimate purpose for which it is collected.
5. If you own or license personal information about a Massachusetts resident, you must comply with HIPAA while also complying with 201 CMR 17. To clarify: HIPAA compliance does not replace complying with 201 CMR 17.

White Paper

Do You Do Business in Massachusetts? Five Things to Know about 201 CMR 17 and Data Protection

(continued)

What Is SAS 70 Type II Certification?

The Statement on Auditing Standards (SAS) No. 70, for Service Organizations, developed by the American Institute of Certified Public Accountants (AICPA), is a widely recognized auditing standard. SAS 70 Type II certification demonstrates that i365 has passed a thorough, objective audit of its organizational control activities and objectives. SAS 70 compliance is often related to Sarbanes-Oxley requirements.

The independent SAS 70 auditor produces two kinds of “Service Auditors Reports”: Type I and Type II. Type I reports describe the organization’s controls at a specific point in time (for example, January 1, 2010). Type II, a more thorough and comprehensive audit, includes the organization’s description of controls as well as a detailed testing of controls over a minimum six-month period.

EVault and 201 CMR 17 Compliance

EVault® data protection, from i365, A Seagate Company, helps you address 201 CMR 17 compliance requirements. Whether you utilize an EVault software, SaaS, or appliance-based solution, you receive a simple, safe, affordable online backup and recovery service with SAS 70 Type II certification, which can greatly assist you in your compliance audits.

As a result, with EVault data protection you can be confident our data center processes are verified to meet or exceed industry standards for security, maintenance, and business continuity. All data collected and stored by EVault systems is transmitted and stored using up to 256-bit NIST-certified AES encryption using Cryptographic Algorithm Implementation V1.0. Encrypted at the source, backup data remains encrypted during the transmission over the wire and at rest in the vault. This assures that the transmission of data between the client and the electronic vault is totally secure. Only authorized personnel in your organization can decrypt the data (not even i365 has access to the encryption keys), ensuring the privacy of your customers’ personal information.

With EVault, you can set your own retention schedules at any level by customizing retention policies to meet your business needs, while also ensuring compliance.

We Can Help

i365’s data protection experts will review your backup, disaster recovery and data retention requirements. We will recommend changes and assist you with the creation of an appropriate written data retention and compliance policy.

For More Information

Visit www.i365.com/edpm, email conciierge@i365.com, or call 1.877.901.DATA.

i365 marks are either trademarks or registered trademarks of i365 Inc. or one of its affiliated companies in the United States and/or other countries. Microsoft marks are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks or registered trademarks are the property of their respective owners.



Headquarters | 3101 Jay Street, Suite 110 | Santa Clara, CA 95054 | **T.** 877.901.DATA | www.i365.com