

CREDANT Solutions for Compliance with the Massachusetts Data Security Law

Strict Requirements Include Mobile Device Encryption

REGULATORY OVERVIEW

Massachusetts' data security law (201 CMR 17.00), passed in March 2010, is widely viewed as one of the strictest in the United States. The law applies any organization that stores (on paper or electronically) personal information about a Massachusetts resident—regardless of where the organization is located—and requires disclosure if a database owner knows or has reason to know of a security breach.

One notable and specific requirement of 201 CMR 17.00 is that businesses must encrypt sensitive personal information stored on portable devices, such as handhelds and laptops, and on storage media such as memory sticks and DVDs. Any personal information that is transmitted over a public or wireless network must also need to be encrypted.

The law also mandates that by March 2012, companies must include language in their third-party contracts obligating their vendors to employ reasonable measures for protecting personal information.

Personal information is defined as a first name or initial and last name and any one of the following, in combination with any required security or access code that would permit access to an individual's Social Security number, driver's license or state ID card number, financial account number and credit card number

Exempted information includes:

- › Information that is available to the general public from federal, state or local government records.
- › A good faith but unauthorized acquisition of personal information by a person or agency (including government entities), for the lawful purposes of such person or agency, unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure.
- › Data that is redacted or secured by other methods rendering data unreadable or unusable from notification obligations.

In the event of a breach, organizations are required to notify the office of the attorney general and the Director of Consumer Affairs and Business Regulation.

THE COMPLIANCE CHALLENGE

201 CMR 17.00 requires every entity that owns or licenses personal information about a Massachusetts resident to develop a comprehensive information security program, and further outlines the elements a security program must have, including at least one employee to manage the security program; third-party security management; and technology to detect and prevent security failures. In addition, the law issues detailed requirements for computer security, including access control, password control and data encryption.

CREDANT SOLUTIONS

CREDANT data security solutions ensure that encryption and security requirements are consistently and efficiently enforced—regardless of where the data resides.

ONLY CREDANT ENABLES ORGANIZATIONS TO:

- › Encrypt and secure data across multiple, diverse platforms, from a single console.
- › Create automatic audit trails that offer proof of end-to-end data security.
- › Provide a transparent end-user interface that supports user productivity while keeping data safe.
- › Choose from full-disk encryption (FDE) or device-specific encryption, or a combination of both.

CREDANT data security solutions provide centrally managed, highly scalable and architecturally flexible security to manage all data end-points. With CREDANT, organizations can:

- › Prove that data stored on lost or stolen devices is encrypted.
- › Prevent data from leaving the organization unprotected on USB flash drives or other forms of removable media.
- › Safeguard data from unwarranted access, reducing risk of internal breaches.