Gesmer Updegrove LLP

ClientAdvisory

March 2010

Massachusetts Data Protection Regulations Take Effect

After three different drafts were circulated by the Commonwealth, the Massachusetts Data Protection Regulations have finally taken effect. As of March 1, 2010, any person or business with personal information about a Massachusetts resident must comply with a new regulatory scheme intended to protect that information from improper use or disclosure.

The Office of Consumer Affairs and Business Regulations originally promulgated the regulations in Fall 2008, mandating that those holding personal information about Massachusetts residents devise and implement specific, detailed policies to protect the security and integrity of that information. Virtually all Massachusetts businesses are covered, and the regulations also apply to entities outside the Commonwealth that hold Massachusetts residents' Social Security numbers, credit card numbers, driver's license numbers or financial account numbers.

The regulations have been controversial, particularly among members of the Massachusetts business community, who widely complained that they were inflexible, overly broad and expensive to implement.

The final version of the regulations were aimed at addressing some of those concerns, while still adhering to the fundamental goal of requiring business practices that minimize the risk of future data breaches.

The regulations apply to both paper and electronic records, and can cover such commonplace items as benefits records, payroll files, invoices evidencing customer payments, and databases that use Social Security numbers as unique identifiers. Virtually any business with a Massachusetts employee falls under the regulations' scope.

The regulatory requirements are extensive and detailed, and demand the adoption and maintenance of a written information security plan and designation of an individual to be responsible for it. The information security plan must:

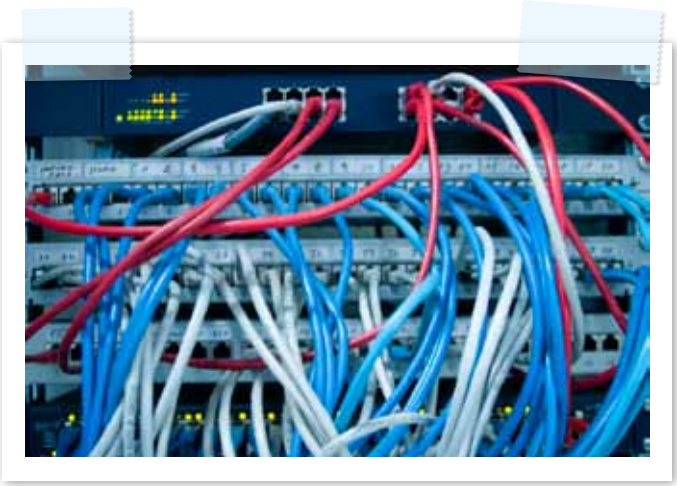
1. identify reasonably foreseeable risks to records containing personal information;

2. address policies regarding the storage and transportation of records outside of business premises;

3. mandate disciplinary measures for violations;

4. prevent access to personal information by former employees;

5. with respect to third-party service providers with access to a personal information, it must provide for due diligence and appropriate contractual terms to ensure that the contract will treat such information in a manner consistent with regulatory mandates;



6. require physical records containing personal information to be kept in locked containers or facilities;

7. provide for regular monitoring of the plan, and for updates when circumstances merit;

8. establish procedures for post-incident actions in the event of a data breach;

9. require secure user authentication protocols with respect to computer equipment that can access personal information;

10. impose access control measures such that only those individuals with a need can access electronic personal information records;

11. require the encryption of any personal information that is transmitted over the Internet, transmitted over an unsecured wireless network, stored on a laptop, or stored on a portable device such as a Blackberry;

12. provide for up-to-date anti-virus software, operating system security patches and firewall patches with respect to any computers that can access personal information; and

13. establish regular education and training of employees on the proper use of computer security systems and the importance of personal information security.

While the regulations are directly enforceable by the Attorney General, a business' failure to comply with them may leave it exposed in civil litigation, jeopardize insurance coverage, and put it at risk of breaching contractual representations and commitments.

If you would like to learn more, call Joseph Laferrera at Gesmer Updegrove LLP. He can be reached at joe.laferrera@gesmer.com or (617) 350-6800.