# CLIENT ALERT: Massachusetts Data Security Regulations Finalized For March 1, 2010 Compliance Deadline

On November 4, 2009, the Office of Consumer Affairs and Business Regulation ("OCABR") issued a press release stating that the revised Massachusetts Data Security Regulations have been finalized and filed with the Secretary of State and are now available on the OCABR website. *See generally, 201 C.M.R. 17.00, et seq.* Therefore, employers that own or license personal information must be in compliance with the Standards for the Protection of Personal Information of Residents of the Commonwealth ("regulations") established by the OCABR by March 1, 2010.

In 2007, Massachusetts, like forty-four other states, enacted data security laws. These laws provided for the development of regulations designed to protect the personal information of Massachusetts residents. The regulations take a risk-based approach and mandate that employers develop, implement, and maintain a comprehensive written information security program to protect personal information.

There have been minor revisions to the regulations since the version released in August of this year. The final version of the regulations has modified the definition of a "person" covered by the regulations to include employers that "store" personal information. Also, the final version expressly includes the United States Postal Service in the definition of "Service Provider." The final version has kept the mandate that employers require third-party service providers by contract to implement and maintain appropriate security measures to protect personal information. However, if such contracts are entered into before March 1, 2010, these contracts do not have to be amended to comply with the regulations until March 1, 2012. For more on the previous version, *see* Morgan, Brown & Joy's previous Client Alert: "Mass Data Security Regulations Compliance Deadline Delayed Again Until March 1, 2010" dated September 14, 2009.

**What Has Changed**

**Who is Covered**

In the previous version of the regulations, those who "store" personal information were excluded. The final version expressly includes those who "store" personal information, as well as own, license, receive, maintain, process, or otherwise have access to personal information in connection with the provision of goods or services or in connection with employment. This means that employers that collect, maintain, or store personal information including, but not limited to, employee records, are subject to the data security law and its regulations. The regulations apply to the personal information of all Massachusetts residents. The regulations also apply to any employer that has personal data of Massachusetts residents, regardless of whether the employer's business is located in Massachusetts.

**Service Providers**

The data security law and its regulations also apply to service providers. A service provider is an entity that is permitted to access personal information through its provision of services to an employer covered by the law. An example would be an information technology (IT) service provider. In the final version of the regulations, the definition of "Service Provider" has been changed to include one who "stores" personal information, in addition to receives, maintains, processes or otherwise is permitted access to personal information through its provision of services to anyone subject to these regulations. If an IT service provider stores personal data offsite for an employer, it must comply with the law.

The final version of the regulations expressly includes the United States Postal Service in its definition of "Service Provider." The Postal Service was excluded in the last version. The regulations do not specify that employers must contractually require the Postal Service's compliance with the regulations, as with other third-party service providers. However, the risk-based approach mandated by the OCABR does require employers to oversee service providers and take steps to prevent the unauthorized access of personal information. As many employers use the Postal Service to transmit personal data, they should monitor potential risks inherent in this process.

**Contracts With Third-Party Service Providers**

The earliest version of the regulations required employers covered by the law to obtain a contract with a third-party service provider that stated the service provider's compliance with the data security regulations. However, because of the burdensome nature of this requirement the OCABR omitted it from its first revised version of the regulations. Then, when the OCABR revised the regulations in August 2009, the contractual requirement was reinstated. This requirement has remained in the final version of the regulations. However, if such contracts are entered into before **March 1, 2010**, these contracts do not have to be amended to comply with the regulations until **March 1, 2012**.

**What Has Not Changed**

**Security Program**

Employers covered by the data security laws and regulations must have in place a written "Comprehensive Information Security Program." This program must have administrative, technical, and physical safeguards to ensure the confidentiality of records that contain personal information. This requirement was modified in August to state that the program should be tailored to the size, scope, and type of business. This means that a small business, with a smaller amount of personal information to protect and more limited resources to protect it will not be held to the same standard as a larger corporate entity with a greater amount of personal information to protect and the means to do so.

The Comprehensive Information Security Program shall include, but is not limited to:

- Designation of one or more employees to maintain the program.
- Risk assessment of all paper, electronic, or other records that contain personal information, including evaluating and improving the effectiveness of existing safeguards; this may include:
    - ongoing employee training;
    - monitoring, ensuring, and enforcing employee compliance with all policies and procedures;
    - a means of detecting and preventing security failures.
- Development of security policies for employees that take into account whether and how employees are allowed to keep, access, and transport records containing personal information outside of business premises.
- Discipline of employees that violate the security program.
- Prevention of terminated employees from accessing records containing personal information.
- Placement of reasonable restrictions on physical access to records that contain personal information, including implementing a written procedure that describes how such access is restricted and the secure storage of such records.
- Monitoring the operation of the program and upgrading the information safeguards in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information.
- Review of the program annually or more frequently if there is a change in business practices that may reasonably implicate the security and integrity of the records that contain personal information.

- Documentation of actions taken in response to a security breach, as well as any changes made in the policy or other business practices as a result of the breach. (Chapter 93H requires notification to the Attorney General and the OCABR in the event of a security breach or unauthorized use/acquisition of personal information.)
- Oversight of Service Providers by:
    - Taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect personal information as required by these regulations and any applicable federal regulations.
    - Require such third-party service providers by contract to implement and maintain appropriate security measures to protect personal information.

**Computer System Security Requirements**

As part of the written information security policy, there *must be* a security system in place that covers all computers, including any wireless system. However, the computer system security safeguards were modified in August to require them only "to the extent technically feasible." At a minimum, these safeguards shall include:

- Secure user authentication protocols including control of user IDs, secure assignment and selection of passwords, restricting access to passwords, restricting access to active and authorized users only.
- Secure access control measures that permit access to records and files that contain personal information for only those persons that must access such information to carry out their job duties, assignment of unique computer identifications and passwords that are reasonably designed to preserve the integrity of the security controls.
- Encryption of all files and records that contain personal information, which will travel across public networks and, encryption of all data containing personal information that will be transmitted wirelessly. Encryption of all personal information stored on laptops or other portable devices;
- Reasonable monitoring of systems for unauthorized use of access to personal information.
- Where files containing personal information are on a system connected to the internet, the system *must have* reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information.
- 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 by up-to-date patches and virus definitions, which is set to receive the most current security updates regularly.
- Employees must be trained and educated on the proper use of the computer security system and the importance of personal information security.

**Compliance Will Be Measured on a Case-by-Case Basis**

This overview of the data security laws and regulations touches on the *minimum* required of employers that employ Massachusetts residents. Compliance with these regulations will account for the size, scope, and type of business; the amount of resources available to the business; the amount of stored data to protect; and the need for security and confidentiality of consumer and employee information. Again, the deadline for compliance is **March 1, 2010**. If you have questions or concerns about the data security laws and regulations, please contact your MBJ attorney.

(For more information, see Morgan, Brown & Joy's previous Client Alerts: "Massachusetts Data Security Regulations: Deadline for Compliance Delayed Until January 1, 2010," dated February 17, 2009 and "Municipalities Must Comply with Portions of Massachusetts Data Security Law," dated June 26, 2009).

*Rachel Muñoz, Esq. is an attorney with Morgan, Brown & Joy, LLP and may be reached at (617) 523-6666 or at rmunoz@morganbrown.com.  Morgan, Brown & Joy, LLP focuses exclusively on representing employers in employment and labor matters.*

This article was published on December 21, 2009.