March 1, 2012 Deadline for Compliance with Massachusetts Security Regulation 201 CMR 17.00

by Francoise Gilbert, JD, CIPP/US[1]

Since March 1, 2010, companies doing business in Massachusetts or holding certain personal data of Massachusetts residents must have in place a written information security plan (a "WISP") that complies with the requirements of the Massachusetts Security Regulation, 201 CMR 17.00 (the "Regulation"). In addition to this deadline, the Regulation provided for a second deadline, of **March 1, 2012**, for compliance with certain provisions of the Regulation that address interaction with service providers. By March 1, 2012, companies must have changed their procedures and amended their contracts with service providers to fulfill their oversight obligations when using subcontractors or service providers to process personal data that are protected under the Massachusetts Regulation.

Specifically, the Regulation requires companies to oversee their 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 consistent with the Regulation and any applicable federal regulations; and

- Requiring such third-party service providers by contract to implement and maintain appropriate security measures for personal information. These measures must be consistent with the requirements in the Regulation.

---

1 © 2012 IT Law Group – All rights reserved

Francoise Gilbert focuses her legal practice on information privacy and security, cloud computing, and data governance. She is the managing director of the IT Law Group (www.itlawgroup.com) and serves as the general counsel of the Cloud Security Alliance. She also keeps a blog on privacy and security issues (www.francoisegilbert.com). She was named one of the country's top legal advisors on privacy matters in a recent industry survey and, for several years, has been recognized by Chambers, Best Lawyers, and Ethisphere as a leading lawyer and trusted advisor in the field of information privacy and security. Gilbert is the author and editor of the two-volume treatise Global Privacy & Security Law (www.globalprivacybook.com), which analyzes the data protection laws of 65 countries on all continents.

Francoise can be reached at fgilbert@itlawgroup.com or +1 650 804 1235.

All contracts with service providers that were executed before March 1, 2010 must have been updated by March 1, 2012, to include a requirement that the service provider implement and maintain appropriate security measures that are consistent with the Regulation.

Among other obligations, all businesses must develop a security program, encrypt all personal information that is transmitted across public networks or wirelessly, and must encrypt all personal information stored on laptops or portable devices. The requirements apply both to the data controllers who have direct relationship with the individuals or direct control over the personal information, and to their service providers who process these data on behalf of the data controllers.

In view of this upcoming compliance date, we provide below the list of requirements that govern all companies that process Massachusetts residents' personal information that are protected under the Regulation.

Background

When Massachusetts passed comprehensive identity theft legislation in October 2007, the legislature charged the Executive Office of Consumer Affairs and Business Regulation (OCABR) with promulgating regulations designed to establish minimum standards for how businesses must protect and store personal information of residents of the Commonwealth. OCABR promulgated the Standards for the Protection of Personal Information of Residents of the Commonwealth, codified as 201 CMR 17.00 et seq., which became effective on March 1, 2010.[2]

The Regulation implements the provisions of M.G.L. c. 93H relative to the standards to be met by businesses that own, license, store or maintain personal information about a resident of Massachusetts. It establishes minimum standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records. The regulation also intends to ensure the security and confidentiality of personal information; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft or fraud against the residents of Massachusetts.

Fines

Violators may be subject to a $5,000 civil penalty for each violation. How "violations" will be counted for computing the penalty is not yet clear. If violations are counted on a per-record basis, businesses with thousands of records could face fines of millions of dollars.

[2] Available at: http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf

What information is protected?

The regulation protects “personal information", defined as a Massachusetts resident's first name, or first initial, and last name in combination with his/her:

- Social Security number,
- Driver's license number,
- State-issued identification card number, or
- Financial account number, or credit, or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident’s financial account.

However, “personal information” does not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the public.

Who is subject to the law?

Most businesses that interact with Massachusetts residents or have employees in Massachusetts are affected. The regulation applies to every “person that owns, licenses, stores or maintains personal information about a Massachusetts resident.” These individuals may be employees, customers, consumers, business contacts, prospects, or third parties. What counts is the nature of the personal data held by the “person.” The term “person” is defined as a natural person, corporation, association, partnership, or other legal entity, other than an agency, or other branch of the Commonwealth.

Sliding scale

The regulation anticipates that compliance will be measured depending on the size and nature of the business, the nature of the data, the resources available to the business, and the need for security and confidentiality of the consumer and employee information. Thus, the safeguards contained in such program must be appropriate to:

- The size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program;
- The amount of resources available to such person;
- The amount of stored data; and
- The need for security and confidentiality of consumer and employee information.

These safeguards must also be consistent with the safeguards for protection of personal information and information of a similar character set forth in any state or federal regulations by which the person who owns or licenses such information may be regulated.

Comprehensive, written, information security program required

Companies are required to develop, implement, maintain, and monitor a comprehensive, written information security program that is consistent with industry standards. The program must contain administrative, technical, and physical safeguards to ensure the security and confidentiality of the personal information in the custody of the organization. Companies must establish and maintain a security system covering their computers and wireless systems. The safeguards must be consistent with the safeguards for the protection of personal information set forth in any state or federal regulations by which the company may be regulated. The regulation identifies twelve requirements:

✓ *Appointment of a responsible person*

At least one employee must be responsible for maintaining the information security program.

✓ *Asset and risk assessment*

Internal and external risks to the security, confidentiality, and/or integrity of all personal information must be identified and assessed. Companies must evaluate and improve, where necessary, the effectiveness of the current safeguards for limiting such risks. For example, companies should evaluate:

- Ongoing employee training;
- Employee compliance with policies and procedures; and
- The means for detecting and preventing security system failures.

✓ *Identification of all devices*

In order to determine which records contain personal information, companies must identify all electronic and other records, computing systems, and storage media, including laptops and portable devices used to store personal information.

✓ *Development of a written information security plan*

The regulations require companies to develop written security policies for employees that define when and how employees can keep, access, and transport records containing protected personal information outside of the business premises.

✓ *Limitation to the collection, retention, and access to information*

The collection, retention, and access to information must be limited to that which is reasonably necessary to accomplish the legitimate purpose for which the personal information was collected.

✓ *Restrictions on physical access*

Access to records containing personal information must be restricted. Companies must follow written procedures that set forth the manner in which physical access to such records is restricted. They must store records in locked facilities, storage areas, or containers.

✓ *Incident response documentation*

In case of a breach of security, companies must document the responsive actions taken during and after the breach in order to make changes in business practices relating to the protection of personal information. “Breach of security" is defined as the “unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by the company that creates a substantial risk of identity theft or fraud against the residents of the Commonwealth of Massachusetts”.

✓ *Service providers*

When retaining a service provider that will have access to personal information, a company must make sure that the third party has the capacity to protect the personal information. It must contractually bind the service provider to maintain safeguards for personal data. Before permitting access to personal information, the company must obtain from the service provider a written certification that it has a written, comprehensive information security program that complies with the regulations. In practice, this means addressing the following requirements:

- Conducting due diligence of vendors before engagement;
- Using reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such personal information consistent with these regulations and any applicable federal regulations.
- Requiring third-party service providers by contract to implement and maintain appropriate security measures for personal information, consistent with the requirement in the Regulation.

The requirement above has been in place for all contracts for the processing of protected data that were executed since March 1, 2010. All contracts entered into before March 1, 2010 must be updated by March 1, 2012.

✓ *Terminated employees*

If an employee is terminated the company must also terminate the employee's physical and electronic access to records containing personal information. For example, the company should deactivate the employee's passwords and user names.

✓ *Monitoring*

Regular monitoring of the information security program is required to ensure that it is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information. Information safeguards must be periodically upgraded as necessary to limit risks.

✓ *Periodic review and adjustment*

Companies are required to review the scope of the security measures **at least annually** or whenever there is a material change in their business practices that may reasonably implicate the security or integrity of records containing personal information.

✓ *Enforcement*

Disciplinary measures must be imposed in the event of a violation of the rules set out in the company's information security program.

Specific security measures for computer systems

In addition to the general measures described above, the Regulation also establishes computer security requirements for entities that own or license personal information about residents of Massachusetts, and electronically store or transmit such information. The regulations require that the entity establish and maintain a security system covering its computers, including wireless systems, that at a minimum, and to the extent technically feasible, uses the following specific technical, physical, and administrative measures to ensure the security and confidentiality of the personal information in the computers and wireless system of the company.

✓ *Technical security measures*

Companies must ensure that the personal data they hold are protected from unauthorized use by encrypting all data and using firewall and security software.

- **Encryption of all data:**

  - Encryption of all records and files containing personal information that will travel across public networks, or that will be transmitted wirelessly.

  - Encryption of all personal information stored on laptops or other portable devices;

"Encryption" is defined as the “transformation of data through the use of an algorithmic process, or an alternative method at least as secure, into a form in which meaning cannot be assigned without the use of a confidential process or key, unless further defined by regulation by the office of consumer affairs and business regulation”.

- **Use of firewall and security software:**

When files containing personal information are stored 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.

- **System security agent software**

Reasonably up-to-date versions of system security agent software must be used. The software must include malware protection and reasonably up-to-date patches and virus definitions. Alternatively, it is permitted to use 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.

- **Security monitoring**

Use of Security monitoring and intrusion detection mechanisms

✓ *Physical security measures*

Access to personal data must be physically restricted by using secure user authentication and access control measures.

- **Secure user authentication protocols:**

Companies must provide secure user authentication protocols, including:

- Control of user IDs and other identifiers;
- A reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;
- Control of data security passwords to ensure that the passwords are kept in a location and/or format that does not compromise the security of the data they protect;
- Restricting access to active users and active user accounts only; and
- Blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system.

- **Secure access control measures:**

Companies must have in place secure access control measures that:

- Restrict access to records and files containing personal information to those who need such information to perform their job duties; and
- Assign unique identifications plus passwords that are not vendor supplied default passwords to each person with computer access, and that are reasonably designed to maintain the integrity of the security of the access controls.

✓ ***Administrative measures***

- Companies must also monitor their systems for unauthorized use of, or access to, personal information;
- Companies must educate and train their employees on the proper use of the computer security system and the importance of personal information security.

* * * * * * *

This publication is issued periodically to keep client of the IT Law Group and other interested parties informed of current legal developments that may affect, or be of interest to them. It is designed to give general information on the developments actually covered. It is not intended to be a comprehensive summary of recent developments in the law, or treat exhaustively the subjects covered. The comments contained herein do not constitute legal opinion and should not be regarded as a substitute for legal advice.

About the IT Law Group

The IT Law Group assists clients in complying with data privacy and security laws in the United States and around the globe, and in negotiating and structuring cloud computing arrangements. We have listed in Best Law firms.

Francoise Gilbert is the founder and managing director of the IT Law Group, and the author and editor of ***Global Privacy and Security Law*** a two volume legal treatise that analyses the data protection laws of 65 countries on all continents. She has received accolades from the prestigious Chambers, Best Lawyers, Best Law Firms, Ethisphere, and Who's Who in Ecommerce, Internet, and Privacy, and has been voted one of the top privacy advisors in the country in a recent industry survey.

For further information, please contact:

Francoise Gilbert
+1 650-804-1235
fgilbert@itlawgroup.com

