MINTZ LEVIN
Mintz Levin Cohn Ferris Glovsky and Popeo PC

Privacy and Security Alert: When the Clock Strikes Midnight on January 1, 2009, Will Your Information Security Program Be Ready?

10/31/2008

As discussed in earlier alerts (here and here), starting on January 1, 2009, businesses will be held to a higher standard regarding the protection of Massachusetts residents' personal information and will now be required to implement written programs for the protection of personal information. The regulations set out in detail the required **minimum standards** to be met by persons or businesses who own, license, store, or maintain personal information about a Massachusetts consumer or employee (the "Standards"). Noteworthy in the scope of data protection regulations, the Standards apply to **paper** as well as to electronic records.

What You Need to Do

Comprehensive Written-Information Security Program

Computer System Security Requirements

Implementation and development of a written comprehensive security program and establishment of a security system covering businesses' computers are at the heart of the Standards and must be in place by January 1, 2009. The Standards provide a detailed list of comprehensive security program and security system requirements, including requirements for encryption of data on portable devices and in transit.

Comprehensive Written-Information Security Program

Section 17.03 of the Standards requires covered entities to "develop, implement, maintain and monitor a comprehensive, written information security program applicable to any records containing" protected information, which is consistent with industry standards ("Program"). A Program must contain "administrative, technical, and physical safeguards to ensure the security and confidentiality" of the records. Additionally, such safeguards must be consistent with the requirements established by any state or federal standards by which a given organization may be regulated.

The Standards specify **mandatory minimum** requirements for every Program. Each Program shall include:

- Designating one or more employees to maintain the Program
- Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality and integrity of the records containing personal information and evaluating and improving the effectiveness of the current safeguards for limiting such risks
- Developing security policies for employees as to whether and how employees should be allowed to keep, access and transport records containing personal information outside of business premises
- Imposing disciplinary measures for violation of the Program
- Preventing terminated employees from accessing records containing personal information by immediately terminating their access to such records
- Taking reasonable steps to verify that third-party service providers with access to personal information have the capacity to protect such personal information
- Limiting the amount of personal information collected to that reasonably necessary to accomplish a legitimate purpose for which it is collected; limiting the time such information is retained to that reasonably necessary to accomplish such purpose; and limiting access to such persons who are reasonably required to know such information in order to accomplish such purpose or to comply with state or federal record retention requirements
- Identifying records and devices used to store personal information, to determine which records contain personal information
- Reasonable restrictions upon physical access to records containing personal information
- Regular monitoring to ensure that the Program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information; and upgrading information safeguards as necessary to limit risks
- Reviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security of records containing personal information
- Documenting responsive actions taken in connection with any incident involving a breach of security or integrity of records

Computer System Security Requirements

The Standards also list mandatory **minimum** elements to be included in the security system (the "System"). Briefly, they include:

- Secure user authentication protocols
- Secure access control measures
- Encryption of transmitted records and files (to the extent feasible)
- Reasonable monitoring of systems (for unauthorized access to personal information)
- Encryption of all personal information stored on laptops or other portable devices
- Reasonably up-to-date firewall protection for files containing protected information on a system that is connected to the Internet
- Reasonably up-to-date versions of system security agent software, which must include malware protection and reasonably up-to-date patches and virus definitions
- Education and training of employees on the proper use of the System and the importance of personal information security

The Standards also specify features required for secure user authentication protocols and secure access control measures.

Recommendations for Compliance

Companies should begin **now** to audit and review its policies and procedures currently in place to determine what changes should be made in order to comply with the statute and Standards. Companies should also review termination policies of employees and their potential access to confidential information. They should also consider, when drafting contracts or entering into independent consultant agreements, obtaining written verification that the other party has a compliant Program in place. Lastly, companies must ensure encryption of all personal information stored on computers, laptops, Blackberries, iPhones, and other portable devices. It should be noted that it remains unclear what is considered a "portable device" under the Standards. This term could include USB drives, cell phones, PDAs, and even Blackberries.

What If I'm Not Located in Massachusetts?

The Standards apply to your company. The Standards apply to any business—wherever located—that owns, licenses, maintains, or stores the "personal information" of Massachusetts

residents. The Massachusetts rules are the first in the country to have such comprehensive and broad coverage applicable to all types of organizations, no matter where located.

Penalties for Failing to Comply

It is crucial for businesses to understand and comply with the newly enacted data breach legislation to avoid potentially severe monetary penalties. Massachusetts, unlike the majority of states, provides for civil penalties in cases of noncompliance with its data breach notification statute, Massachusetts General Laws, Chapter 93H. In particular, a civil penalty of $5,000 may be awarded for each violation of Chapter 93H. In addition, under the portion of Chapter 93H concerning data disposal, businesses can be subject to a fine of up to $50,000 for each instance of improper disposal. The Massachusetts Attorney General may bring an action under Chapter 93A, the Commonwealth's consumer protection statute, which permits the imposition of significant fines, injunctive relief, and attorneys' fees. Last but not least, Massachusetts consumers may also seek damages under Chapter 93A, which in some cases, may be trebled.

Therefore, while implementation of the Standards might require additional expenditures and seem costly, potential fines might result in greater financial damage to a business, not to mention the likely negative publicity.

January 1, 2009 is right around the corner.

We can help.

Mintz Levin's Privacy and Security Group assists clients in developing, implementing, and evaluating privacy and information security programs to comply with federal and state requirements. We can assist with the review or development of policies and procedures to comply with the Standards and can help develop new policies and training programs. Watch for an upcoming Mintz webinar on compliance with the Standards.

For further information on the topic covered in this Alert, please contact one of the attorneys listed below or the Mintz levin attorney who ordinarily handles your legal affairs.

Cynthia Larose, CIPP
(617) 348-1732
CLarose@mintz.com

Elissa Flynn-Poppey
(617) 348-1868
EFlynn-Poppey@mintz.com

Julia M. Siripurapu
(617) 348-3039
JSiripurapu@mintz.com
