Helping benefit plan sponsors put information into action
EmployeeBenefit news

Legal Alert: The new Massachusetts data security requirements: Additional obligations or more of the same?

By Cynthia J. Larose, Esq.

July 24, 2009

Legal requirements to protect and secure the personal information of individuals are increasing in number and in scope. Effective Jan. 1, 2010, any business that "owns, licenses, maintains or stores" the "personal information of a Massachusetts resident" is required to develop a written information security plan and establish a security system that will protect the personal information in transit (across public networks, such as the Internet) or at rest (in storage, or portable devices, or on hard drives).

The "Standards" are listed under Title 201 of the Code of Massachusetts Regulations, Section 17.00.

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.

The security 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. The most important components of each program are:

- 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;
- Reasonable restrictions upon physical access to records containing personal information;
- 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; and
- 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. 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; and
- Education and training of employees on the proper use of the system and the importance of personal information security.

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

Recommendations for compliance

Employers should begin now to audit and review their policies and procedures currently in place to determine what changes should be made to comply with the statute and Standards. Companies should also review termination policies of employees and their potential access to confidential information.

When drafting contracts or entering into consultant agreements, employers should consider 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, including USB drives.

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.

Comparison to HIPAA/ARRA: New federal security breach notification law

There is no "federal pre-emption" clause in the Standards. Most data breach notification statutes have a provision that states if a covered entity is required by a federal or other regulatory agency to comply with data security or data notification, compliance with the provisions of the primary regulator will be deemed compliant with the state law.

Because this section is absent from the Standards, entities with "protected health information" covered by HIPAA that is also "personal information" of a Massachusetts resident will be required to meet both sets of compliance standards. Fortunately, that may not be as difficult as it sounds.

The American Recovery and Reinvestment Act of 2009 added a data breach notification provision to HIPAA. This provision requires a covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses or discloses unsecured protected health information to notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired or disclosed as a result of a breach.

This notification requirement, like the Massachusetts requirements, applies to all unsecured protected health information whether in electronic, paper or other form.

In April, as required by ARRA,the Secretary of Health and Human Services issued guidance to define what constitutes secured protected health information within the meaning of ARRA.

In short, a breach of secured protected health information that is protected by one of the encryption methodologies specified in the HHS guidance, like the secured "personal information of a Massachusetts resident," falls into the "safe harbor" under the HHS guidance.

Unlike the Standards, the HHS guidance makes specific reference to the National Institute of Science and Technology Standards as providing an acceptable method of encryption and providing a "functional safe harbor" for encryption and destruction of data.

Extension of certain HIPAA security rules to "business associates"

HIPAA provisions on administrative safeguards will soon apply directly to HIPAA business associates "in the same manner that such sections apply to the covered entity."
Civil and criminal penalties for improper disclosure of health information also will apply to "business associates," exposing them to the same liability as HIPAA "covered entities."

These penalties top out at 10 years in jail and fines of $250,000 for improper use of protected health information.
Civil and criminal penalties for improper disclosure of health information also will apply to "business associates," exposing them to the same liability as HIPAA "covered entities."

Bottom line

The bottom line is, if you are a "business associate" for purposes of HIPAA, the new federal regulations will extend your liability and risk for securing health information in much the same manner as the Massachusetts Standards apply to "personal information." Employers in Massachusetts will need to seek advice on coordinating their compliance program to avoid duplication of effort.

Cynthia J. Larose can be reached at cjlarose@mintz.com.