

CLIENT ADVISORY

**MASSACHUSETTS ENACTS NEW DATA
SECURITY BREACH NOTIFICATION ACT**

Massachusetts recently enacted “An Act Relative to Security Freezes and Notification of Data Breaches” (the “Act”), requiring companies, entities or people possessing personal information to take affirmative steps in the wake of a security breach. Specifically, the Act requires the company or entity to provide notice to affected Massachusetts residents whose personal information has been subject to a security breach. The Act also includes requirements for requesting security freezes and data destruction, and directs a state agency to adopt regulations directed at safeguarding personal information. The Act will become effective on February 3, 2008. The Act significantly increases healthcare organizations’ exposure to civil actions by individuals and the Massachusetts Attorney General (“AG”) with regard to the security of their patient and employment records.

Protected Personal Information

The Act applies to persons or agencies that own or license personal information, as well as to persons or agencies that maintain or store personal information on behalf of others (collectively, “Covered Entities”). This means that any Covered Entity that owns, licenses, maintains or stores personal information needs to be aware of the new law and be prepared to respond in the event of a breach.

Under the Act, protected personal information includes the first name and last name or first initial and last name of a resident of the Commonwealth in combination with the resident’s (1) social security number, (2) driver’s license number, (3) state identification number, (4) financial account, debit or credit card number in combination with or without any required security code, access code, or password that would permit access to a resident's account. If the personal information involved in a security breach was encrypted using 128-bit or higher algorithmic encryption and the encryption key was not also compromised, notice of the security breach is not required. Finally, personal information does not include information lawfully obtained from a public source.

Although most other state breach notification laws are limited to personal information maintained electronically, the Act protects data, including personal information, regardless of physical form or characteristics. Therefore, the unauthorized access to or use of paper files containing personal information would trigger the notice requirement under the Act.

Breach Notice Requirements

The Act applies a subjective reasonableness test for determining the circumstances when a Covered Entity must give notice to an individual after a security breach. Under the Act, if a Covered Entity experiences a security breach that is “capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the Commonwealth,” the affected resident must be notified of

the breach. The “substantial risk of identity theft or fraud” refers to those breaches of security that create only a remote risk to the consumer. Such breaches do not require notice. However, if a Covered Entity knows or has reason to know that personal information is lost or acquired by an unauthorized person or used for an unauthorized purpose, the Act requires notice regardless of whether there is a likelihood of harm. This mandate goes beyond the requirements of many other state breach notice laws, which permit covered entities to avoid providing notice if a breach does not create a risk of harm.

The Act requires Covered Entities to provide notice of a security breach to both the Massachusetts resident affected and to the AG. The notice to the Massachusetts resident must include the following: (1) disclosure that a security breach occurred; (2) the consumer’s right to obtain a police report; (3) how a consumer requests a security freeze and the necessary information to be provided when requesting the security freeze; and (4) any fees required to be paid to any of the consumer reporting agencies. The Act specifically provides that the notice to the Massachusetts resident “shall not” include the nature of the breach or unauthorized access or use, or the number of residents affected. Notice may be provided in the following forms: (1) written notice; (2) electronic notice, if notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001(c) and G.L. c. 110G; or (3) substitute notice, if the Covered Entity required to provide notice demonstrates that the cost of providing written notice will exceed \$250,000, or that the affected class of Massachusetts residents to be notified exceeds 500,000 residents, or that the person or agency does not have sufficient contact information to provide notice.¹

The required notice under the Act to the AG is processed through the Director of Consumer Affairs and Business Regulation (“DCABR”) of the AG’s office. Unlike the notice to the Massachusetts resident affected, notice to the DCABR must include the nature of the breach or unauthorized access or use, the number of residents affected, and what actions the Covered Entity is taking to address the incident.

The Act provides that notice to the affected Massachusetts resident(s) and the DCABR must be provided as soon as possible and without unreasonable delay. However, delay in providing notice is permitted when law enforcement determines notification would hinder a criminal investigation provided that the law enforcement agency notifies the Covered Entity and AG of that determination.

The AG may bring an action against a Covered Entity to remedy a failure to provide appropriate notice under the Act. Furthermore, while the Act does not specifically authorize a private right of action, the Act does not state that enforcement rests exclusively with the AG.

Data Destruction Requirements

The Act also requires Covered Entities to take certain steps when disposing of records containing personal information, whether in paper or electronic form. Records containing personal information must be destroyed so that personal information “cannot practically be read or reconstructed.” Covered Entities are permitted to use third parties to destroy such records. The third parties, however, must implement and monitor compliance with policies and procedures to prohibit unauthorized access to or use of personal information in the course of the collection, transportation or destruction of the information. Covered Entities purchasing these services should obtain written assurances from the third party that it is in compliance. Covered Entities that improperly dispose of records may be fined \$100 per individual affected, up to a maximum of \$50,000 per event.

¹ “Substitute notice”, consists of all of the following: (1) electronic mail notice, if the Covered Entity has electronic mail addresses for the members of the affected class of Massachusetts residents; (2) clear and conspicuous posting of the notice on the home page of the Covered Entity if the Covered Entity maintains a website; and (3) publication in or broadcast through media or medium that provides notice throughout the Commonwealth.

Recommendations

The Act will have a significant impact on health care providers. Although health care providers are already required to comply with the HIPAA Privacy and Security Rules, the Act will actually expand upon the responsibilities of health care providers in regard to protected health information. For example, under the HIPAA Privacy Rule, Covered Entities are required to provide an individual (when requested by the individual) with an Accounting of Disclosures setting forth to whom the individual's protected health information had been disclosed to outside of the Covered Entity's treatment, payment, and health care operations. Such disclosures include unauthorized access to or use of an individual's protected health information. Beyond listing such unauthorized access or use of protected health information on the Accounting of Disclosures, there is no requirement of the Covered Entity to notify the individual who is the subject of the protected health information. Under the Act, Covered Entities will be required to notify the individual about the unauthorized access to or use of their protected health information.

The Act directs the DCABR to adopt regulations that would require a Covered Entity to safeguard any personal information about a resident of the Commonwealth that the Covered Entity owns or licenses. It will take some time before the DCABR adopts those regulations. In the interim, in order to comply with the Act before February 3, 2008, Covered Entities need to review and revise, as necessary, their policies and procedures pertaining to: (1) security breaches of personal information and (2) data/ document retention and destruction.

* * *

The Rogers Law Firm will continue to monitor any new developments with respect to the Massachusetts Data Security Breach Notification Act and will provide updates accordingly. In the meantime if you have any questions regarding the Act, please do not hesitate to contact any of the attorneys at The Rogers Law Firm.

This Client Advisory is published by The Rogers Law Firm to keep its clients informed of developments in health law. The Client Advisory should not be construed or relied upon as legal advice or legal opinion on any specific facts or circumstances. If you have any questions or concerns regarding the Client Advisory or would like legal advice or legal opinion concerning a specific matter, please do not hesitate to contact any of the attorneys at The Rogers Law Firm, at (617) 723-1100.