

GILMORE, REES & CARLSON, P.C.

CLIENT ADVISORY

NEW REGULATIONS REGARDING DATA SECURITY IMPACT MOST MASSACHUSETTS BUSINESSES

Any business that stores, in paper or electronic form, any “personal information” about a Massachusetts resident, must comply with new regulations that require the creation and implementation of a written security plan to protect that personal information.

“Personal information” is defined by the regulations as the first and last name or first initial and last name of a Massachusetts resident paired with a social security number, driver’s license or state-issued ID number, bank or other financial account number, or credit or debit card number. This includes, for example, the personal information of employees; therefore, if your business retains the social security numbers of employees for tax purposes, then your business is subject to these new regulations. There is no exception to these regulations for small businesses.

The regulations, entitled Standards for the Protection of Personal Information of Residents of the Commonwealth, become effective on January 1, 2010. *All changes to your business practices required under these new laws must be in place by that date.*

Comprehensive Written Information Security Program (WISP)

Every business that stores the personal information of a Massachusetts resident must prepare a WISP. This comprehensive report must be prepared in response to an internal analysis of how and to what extent personal information is stored by the business. Management should determine whether practices can be altered in order to lessen the amount of personal information collected as well as how that information can be better protected. In creating the WISP, every business must:

- Identify each physical or electronic location where personal information is stored.
- Implement administrative, technical and physical safeguards for personal information protection.
- Identify an individual to maintain and supervise implementation and performance of the WISP.
- Mandate and carry-out employee training and procedures for monitoring employee compliance pertaining to personal information.
- Limit the amount of personal information collected and the time such

information is retained by the business to that reasonably required to accomplish legitimate business purposes.

- Verify that any third-party service providers with access to personal information apply similar protective measures for personal information, and insert such requirements into any third-party contracts.
- Institute procedures to monitor operation of the WISP and upgrade it as necessary.

Electronic Records Requirements

If you determine that your business stores or maintains personal information in electronic format, additional protocols and procedures must be adopted under the WISP. These include:

- Secure authentication protocols for all computers, servers and software that store or use personal information.
- Unique identifications and passwords for each individual with computer access.
- Appropriate encryption of all digital files containing personal information that are transmitted over public networks or transmitted wirelessly.
- Additional safeguards for all laptops and portable devices which store personal information.
- Reasonably up-to-date firewall protection and system security agent software, as well as all patches and virus definitions.

Enforcement

It is unclear at this point how and to what extent Massachusetts will audit business entities to ensure compliance under the new regulations. However, the attorney general is authorized to bring suit against violators, and such claims may be brought under Chapter 93A, which allows for treble damages. Clearly any failure to comply could have very serious (and expensive) consequences for your business. In addition, such a failure could be deemed a breach of the terms of your insurance policies, leaving you financially exposed to all claims resulting from such a breach.

Compliance

Each business will be impacted by these regulations in a different way. However, at a minimum every business must draft and adopt a Written Information Security Program. If you need more information about these regulations, or what your business must do to be in compliance, please contact us.