

Six Things You Need to Know About Massachusetts' New Data Security Regulations

1. The new regulations exist, although you may not have heard of them.

In October 2008, the Commonwealth of Massachusetts issued sweeping new regulations designed to protect "personal information" about Massachusetts residents. The regulations demand a comprehensive data security program of any business holding the Social Security number, credit card number or bank account number of any Massachusetts resident.

The regulations have received some press coverage in Boston-area business publications, but word is spreading slowly. Many affected businesses remain unaware of their existence, and of the sweeping changes they require in the way information is used, stored and protected.

2. The Regulations apply to virtually all Massachusetts businesses, and many businesses outside of Massachusetts.

The regulations apply to any entity holding "personal information" about a Massachusetts resident. Since Massachusetts businesses maintain their employees' Social Security numbers, they must comply.

In addition, the regulations reach businesses outside of Massachusetts, if they hold any Massachusetts resident's "personal information." So, for example, they would apply to a New York company providing payroll account services, if *any* of the payroll records are of Massachusetts residents.

There is no minimum threshold. Information about even one resident requires full compliance.

3. The regulations apply to paper records, as well as electronic ones.

The regulations do contain many requirements specific to electronic records and computer systems. However, there are also a number of requirements that apply to paper records as well. Paper records containing "personal information," for example, must be kept in a locked container or facility.

4. Even businesses with a good security track record and robust computer systems may need to implement significant changes.

Unlike laws recently enacted in Massachusetts and elsewhere, the new regulations do not simply require action in the event of a data breach. Instead, the regulations include detailed technical and legal requirements that must be implemented even if security problems never arise.

Simply exercising reasonable care is not enough. For example, sending a Massachusetts resident's Social Security or credit card number by email – a common practice – will violate the regulations unless the information is encrypted. Similarly, having such information, unencrypted, on a laptop or PDA (such as a BlackBerry or iPhone) is also a violation.

5. Responsibility cannot just be outsourced.

Not only must affected businesses comply themselves, they must ensure that their third-party services providers also comply. This demands, among other things, that special provisions be included in contracts with all service providers that have access to "personal information."

6. Risks of noncompliance are broad.

Although the regulations themselves may be enforced only by the Commonwealth of Massachusetts, ignoring the regulations may create significant exposure in other contexts as well. For example, many insurance policies require a representation that the insured is in compliance with applicable laws and regulations; ignoring the new regulations may put critical coverage at risk. Also, trial lawyers may try to portray the regulations as a new standard of care, and use non-compliance to try to establish negligence or unfair business practices in data breach cases.

If you would like more information on this topic, please contact the head of the firm's Data Security Practice Group, Joe Laferrera, at joe.laferrera@gesmer.com.

This information is provided "as is." No representations are made regarding completeness, accuracy or applicability. It does not constitute legal advice and creates no attorney-client relationship. This may be deemed advertising under M.R.P.C. 7.3(c). All rights reserved. ©2008 Gesmer Updegrove LLP.