

New Data Security Regulations Have Sweeping Implications For Massachusetts Businesses

Massachusetts' Data Security Breach Notification Law, Chapter 93H

October 31, 2008 marked the one-year anniversary of the Massachusetts law requiring notification of individuals victimized by data security breaches. The statute, Chapter 93H of the Massachusetts General Laws, is one of 46 such laws in the United States, and its terms are largely consistent with other states' laws.

Chapter 93H generally requires an individual, business or governmental agency with "personal information" relating to a state resident to provide notice in the event of a data security breach.

"Personal information" is defined as the name of a Massachusetts resident in combination with her Social Security number; driver's license or state ID number; financial account number; credit card number or debit card number. Basically, notification is required when personal information (either in unencrypted form, or in encrypted form with its key) has been used for an unauthorized purpose, or has been acquired by an unauthorized person.

The statute also calls for the implementation of regulations for the purpose of protecting the security, confidentiality and integrity of Massachusetts residents' personal information.

New Regulations To Protect Personal Information

The Massachusetts Department of Consumer Affairs and Business Regulations recently issued regulations in response to Chapter 93H's edict. Unlike the Commonwealth's

approach to the statute itself, however, the regulations represent a substantial departure from what has come before, and they impose potentially significant requirements that in many ways surpass what is required elsewhere in the country. These regulations, which may be found at [201 Code of Massachusetts Regulations \(CMR\) 17](#), become effective on May 1, 2009 (with some exceptions).

[T]he regulations represent a substantial departure from what has come before, and they impose potentially significant requirements that in many ways surpass what is required elsewhere in the country.

At their core, the new regulations call for any person (which includes corporations and partnerships, but not government bodies) who "owns, licenses, stores, or maintains personal information" about a Massachusetts resident to develop and implement a written "comprehensive data security program." This

ominous-sounding "information security program" requirement is not merely an amorphous obligation to be proactive in the care and maintenance of personal data. The regulations provide an extensive (though not exhaustive) list of items that must be included in the program. They provide that the manner in which these items are implemented is dependent upon the following factors:

- the size, scope and type of business involved;
- the resources available to it;
- the amount of stored data;
- the need for security and confidentiality.

Table of Contents

[About the Massachusetts Law](#)

[About the New Regulations](#)

[Requirements That Apply to All Personal Information](#)

[Requirements That Apply To Electronic Records Only](#)

[Effective Date and Scope](#)

In the abstract, this makes sense. But, as is evident from the detailed standards imposed for such information security programs, even the smallest businesses must shoulder a considerable load in safeguarding personal data. Those who believe that they can safely ignore the regulatory regimen because only a modest amount of personal data is at issue, or because few employees are available to specifically focus on this new mandate, do so at great risk.

Those minimum requirements for an information security program are broken down into two main categories: requirements applicable to personal information generally, and requirements applicable to personal information in electronic form.

.....
[T]hose who believe that they can safely ignore the regulatory regimen because only a modest amount of personal data is at issue...do so at great risk.
.....

General Information Security Program Requirements

All information security programs must include the following:

- a. **Designated employee.** The program must designate one or more employees to maintain the information security program. We recommend that a single individual be designated, although multiple persons may well be tasked with responsibilities relating to its implementation. Note that the requirement is not purely a technical one; smaller organizations may want to think twice before simply assigning this to the person with the most technical expertise. The role is, at its core, a policy creation and implementation one, and effectively requires even the most modest organizations to create a position resembling a Chief Privacy Officer.
- b. **Identify risks.** The program must identify and assess “reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of...personal information.” In addition it must provide for evaluating and improving the effectiveness of those

efforts. This section must involve employee training, as well as methods of detecting and preventing security system failures. While the threat analysis will vary widely from one situation to the next, the regulations give insight to what the government expects in the mitigation of risk. Here, particular attention should be given to how each and every employee (or contractor) will be included in the program’s implementation, whether through training or

otherwise. Training programs should be formalized, and records kept to evidence full participation of the workforce.

c. **Off-premises access.** The information security program must include policies for addressing whether and

how employees are permitted to use personal information “outside of business premises.” In general, the best approach here is to prohibit all but specified classes of employees from accessing or transporting personal information from the field. Those with particularized needs should be allowed such access only to the extent necessary for them to perform a necessary job function. Such records (whether in paper or electronic form) should be physically kept with and by the employee, locked in a secure cabinet or room, or maintained electronically in an encrypted form. In the telecommuting context, companies should give thought to VPN, Citrix or other technologies that secure electronic access between on-site and off-site computing devices. While these measures impose an added cost, providing unencrypted transmission of personal information data over the Internet is problematic, and at odds with the regiment mandated by the state.

d. **Disciplinary measures.** The program must provide that employees are subject to disciplinary measures for violations of the program rules. This is intended to ensure that all employees take the policy seriously, and

disciplinary measures should be consistent with that goal. The manner in which this is incorporated into the information security program should allow for significant flexibility, however, in terms of the specific actions that will be taken in the event of violation.

e. **Terminated employees.** Terminated employees must be prevented from accessing personal information “by immediately terminating their physical and electronic access to such records.” This is generally self-explanatory. Care must be taken in those situations where an employee is separated from employment, but continues to provide transition assistance. Either employment must be extended, or safeguards imposed so that the former employee does not have direct access to the personal information at issue.

f. **Third-party service providers.** Businesses must verify that service providers “have the capacity to protect...personal information.” This involves inserting appropriate language into vendor agreements which (a) obligate the service provider to appropriately safeguard the information; and (b) maintain its own written information security program. While such requirements will become part of the standard boilerplate, complicated scenarios may arise in connection with existing long-term contracts that lack such terms, and with out-of-state service providers that have not yet assembled their own written information security programs. These must be approached on a case-by-case basis, and the relative bargaining power of the parties may well dictate the relative risk that the parties will ultimately bear here. A review of vendor contracts is essential, and should be undertaken by all businesses.

g. **Limited access.** The information security program must limit (a) the amount of personal

information collected; (b) the length of time such information is kept; and (c) persons permitted to access such information. Information may only be kept to the extent necessary to accomplish its “legitimate purpose” or comply with applicable governmental requirements. While this concept is understandable in the abstract, implementation may well prove tricky. For example, in completing a retail transaction, may the retailer collect personal information for a legitimate but unrelated purpose? Is access by an employee for legitimate purposes unrelated to the rationale for the collection of the data permitted? Given the somewhat restricted definition of “personal information,” however, the most common question may be the extent

to which persons may be permitted to retain credit and debit card numbers of customers. “Indefinitely” does not appear to be an acceptable answer any longer.

h. **Identifying personal information records.** The written information security program

must provide for a method of identifying records and devices used to store personal information (unless all records are treated as personal information). Carefully implemented systems used to segregate personal information address this requirement. This may well require a reworking of databases and other established data processes, however, and must be carefully considered on a process-by-process basis.

i. **Physical access.** It must impose reasonable restrictions on physical access to records containing personal information.

.....
[C]omplicated scenarios may arise in connection...with out-of-state service providers that have not yet assembled their own written information security programs
.....



It must specifically address the manner in which such access is restricted and require the storage of such data in locked facilities or containers.

j. **Monitoring information security program.**

The information security program must provide for monitoring to ensure that it is operating “in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information.” This is meant to essentially ensure that the information security plan is more than a binder on a shelf, but is actually being implemented in a manner that ensures that its goals are being met. Along with (k) below, this sets out the fundamental job requirement for the individual designated in (a) above.

.....
This is meant to essentially ensure that the information security plan is more than a binder on a shelf, but is actually being implemented in a manner that ensures that its goals are being met.
.....

k. **Review of information security program.**

The companion to (j) above, this requires a regular review (no less than annually, but as often as business practices may require) of the program to accommodate new and unanticipated risks. Again, this is a major responsibility of the information security designee required by the regulations.

l. **Addressing data incidents.**

The program must provide for the documentation of actions taken in response to “a breach of security,” along with a post-hoc review to make any necessary changes in business practices. This goes beyond the mere notice requirement of Chapter 93H, and is akin to the “morbidity and mortality” reviews undertaken by hospitals to review mistakes that occurred during patient care to prevent a recurrence. Incorporation of this requirement into the written information security program may be straightforward, but the more important part here will be ensuring that an actual review takes place that

demonstrates an understanding of the magnitude of the incident. Given that Chapter 93H requires that the state be informed in the event of a data security breach, it is reasonable to expect the Attorney General to inquire into the outcome of some (or even most) incident reviews. Indeed, even with respect to events that do not rise to the level of a reportable incident, the conducting of such a

review may be an important way of substantiating the proactive manner in which data security issues are addressed within the organization. Assuming proactive measures are taken, such a record of review and response may be very helpful in the event of a subsequent, reportable breach.

Information Security Program Requirements Regarding Electronic Data

All information security programs must include the following, as it relates to electronic personal information:

a. **User authentication protocols.**

With respect to electronic personal information, users must be authenticated through the use of user IDs, passwords or other methods that control their access to the data. Authentication must involve:

i. the control of user IDs, so the organization can match user IDs with specific individuals. The sharing of user IDs among employees should be prohibited;

ii. use of passwords, biometric identifiers (such as fingerprint technology), or token devices (such as “rolling” RSA SecurID tokens). With respect to passwords, measures should be taken to ensure that passwords are difficult to guess (i.e., not words in dictionary; they incorporate letters, numbers and symbols; they meet

minimum length requirements, etc.). Additionally, thought should be given to forcing the occasional updating of passwords.

iii. control of password data, to ensure that passwords are encrypted or stored in a secure manner. Most modern password management systems and software operating systems store passwords in an encrypted format, so this should not impose an undue burden on most organizations.

iv. restricting access to active users on active accounts. In other words, access to personal information should be solely through use of user-based password-controlled log ins. For large organizations, in which all employees must “log in” to gain access to the corporate computer system, this may not present a break in current practice. For smaller organizations – for example, those that maintain customer credit card information on free-standing databases accessible from outside a corporate network log in – this will require a new approach. It appears that merely password protecting individual data files themselves may be an inadequate approach going forward.

.....
It appears that merely password protecting individual data files ... may be an inadequate approach going forward.
.....

v. blocking access after multiple incorrect login attempts. Again, for some organizations, existing software and data systems may already block access after multiple unsuccessful login attempts. The larger issue for some (small) organizations may be implementing a user-based access system. Once such a system is in place, addressing the issue of unsuccessful login attempts will often be relatively straightforward, and may be incorporated into the operating system.

b. **Secure access control measures**. Personal information must be restricted to individuals on a “need to know” basis, and must use unique user IDs and passwords to implement such restrictions. Software vendor “default” passwords may not be used. Again, this general approach is standard in the industry for enterprise-wide systems, but will represent a departure for organizations that still rely on individual PCs, thumb drives, and “sneaker net” to share information. Gone are the days when a list of customer names and credit card numbers could be passed from employee to employee on a CD-ROM or flash drive, apparently even if such information is encrypted.

c. **Encryption of transmitted records**. Personal information that travels wirelessly or across public networks (e.g., the Internet) should be encrypted. The language of this section suggests that the encryption requirement as it relates to public networks is only imposed “to the extent technically feasible,” which the encryption

requirement as it relates to wireless transmission applies to “all data.” The wireless component of the requirement will be manifest largely in connection with Wi-Fi networks, which should always be password protected in any business environment. WEP encryption should not be used on Wi-Fi networks, as it is very insecure, and has led to a number of data breach incidents. Other wireless technologies (Bluetooth, WiMax, etc.) have their own security and usage issues, which should be addressed separately. For example, Bluetooth may use less secure encryption algorithms than the Wi-Fi WPA standard, but it is viable over much shorter distances and is less likely to be used in the transmission of personal information, so the inquiry will differ when compared to Wi-Fi. Regarding transmission over the Internet, a number of protocols and techniques can protect login sessions, and you should consult with an IT professional to find

the one most compatible with your organization's resources and needs. Businesses must be aware that sending unencrypted information over the Internet (whether by email, through a web site or otherwise) is the equivalent of sending a postcard – the confidentiality of the content is dependant solely on the assumption that no one will choose to read it before it reaches its destination. Such an approach is wholly incompatible with the regimen being imposed in the new regulations.

d. **Monitoring of systems.** The information security plan must provide for the "reasonable monitoring of systems, for unauthorized use of or access to personal information." Consult an IT profession for information about how to best to implement this in your situation.

e. **Laptop encryption.** The regulations require that personal information stored on laptops or other portable devices be encrypted. This has gotten significant attention, and appears to be an overly broad approach to the problem of data security. For example, there is no exception in the regulations for laptops that are maintained on premises in a secure manner. Rather, the language appears directed to all portable devices (including all laptops), regardless of location or use, as long as they contain personal information. Some organizations will simply elect not to permit personal information

to travel by laptop, or migrate to employees Blackberries or similar devices. That may be the least expensive and most technically secure approach. Because the definition of personal information is rather narrow, such an approach may impose fewer hardships for many organizations than first feared, since many or most laptops may be immune from

the restrictions. But, for those organizations with a need to travel in the field with such information, care must be taken to properly equip such laptops (and other mobile devices at issue) with systems to meet the encryption requirement. The best approach for laptops is drive-level encryption, whereby everything on the hard drive is encrypted and decrypted automatically by the computer (either through hardware or software). While this may impose a greater expense than simply

encrypting individual files or directories, the more comprehensive approach avoids the scenario in which the employee stores frequently used personal information in an unsecure manner for convenience or speed of access. Note that merely using a Windows-based login does not meet this requirement; such security can be easily bypassed by removing the hard drive from the laptop and mounting it on a separate computer. The data is not encrypted, and it can be easily read.

f. **Security patches and firewall protection.** The information security program must provide for "reasonably up-to-date firewall protection and operating system security patches." Note that implementation of security patches is often intentionally delayed by IT departments to permit testing for compatibility with legacy systems. It is not clear what an organization's responsibilities

.....
The regulations require that personal information stored on laptops or other portable devices be encrypted....
[F]or those organizations with a need to travel in the field with such information, care must be taken to properly equip such laptops (and other mobile devices at issue) with systems to meet the encryption requirement.
.....



are when a particular security patch would cause problems with a live system. In general, IT departments should closely monitor vendor sites for security glitches and patches, in that this aspect of the regulations seems to shift responsibility for insecure operating system software to the user, to the extent patches are available.

g. **Anti-virus software.** The regulations require software that offers “malware protection,” and use up-to-date virus definitions. Just as a weed is simply an undesirable plant, malware is essentially no more than an undesirable piece of software. The term is not well-defined. While we all have a general understanding of what anti-virus and anti-spyware programs are intended to do, it is unclear whether lesser known and less robust products will be considered sufficient to meet the requirement of this paragraph. Moreover, users of Apple Macintosh products are often accustomed to running without separate anti-virus software, since very few viruses affect those computers. It is yet to be seen how broadly this requirement will be interpreted.

h. **Education and training.** “Education and training of employees on the proper use of the computer security system and the importance of personal information security.” This dovetails with (b) in the general section, which requires employee training generally.

Who Must Comply and When?

The deadline for compliance is May 1, 2009 (except for the encryption of mobile devices and certification of third-party providers, which have a January 1, 2010 deadline). Although this extends the original January 1, 2009 deadline, it is still quite aggressive.

The regulations generally apply to any non-governmental entity that maintains any “personal information” at all. Virtually all Massachusetts businesses will fall under its scope, if only because they maintain such information about their own employees. Moreover, the regulations do not expressly limit their application to businesses operating or incorporated in Massachusetts. Other corporations doing business with Massachusetts residents may well be subject to the regulatory regimen, although the scope has yet to be tested in court.

.....
Although [the May 1, 2009 deadline] extends the original January 1, 2009 deadline, it is still quite aggressive.
.....

It is not yet clear how the state will approach enforcement initially, although in similar circumstances (including the passage of Chapter 93H itself), government officials have expressed

a willingness to become increasingly stringent about enforcement with the passage of time. Businesses that miss the deadline or otherwise fall short of the standard set by the regulations will run a considerable and steadily increasing risk.

Further, while neither the regulations nor Chapter 93H provide for a private right of action, the standards they establish may well become a relevant benchmark in future civil cases.

Because many of the regulations’ requirements may require substantial lead time to implement, the smart executive will start thinking about compliance immediately.

The author, Joseph Laferrera, is a partner at the firm of Gesmer Updegrave LLP. He heads the employment law and data security practice groups at the firm. Any questions regarding the contents of this paper may be directed to him at joe.laferrera@gesmer.com.



The information provided herein is for informational purposes only, for clients and friends of Gesmer Updegrave LLP. It is provided “as is,” and the firm makes no representation as to the completeness or accuracy of its content. It does not constitute legal advice. Before making any legal decisions regarding the matters discussed in this white paper, you should consult with a qualified legal professional, who can provide advice tailored to your individual situation. This document does not create an attorney-client relationship between you and Gesmer Updegrave LLP or any of its attorneys. ©2008 Gesmer Updegrave LLP. All rights reserved.