



AMENDMENTS TO THE MASSACHUSETTS DATA SECURITY REGULATIONS: STANDARDS FOR THE PROTECTION OF PERSONAL INFORMATION¹

Significant data security breaches and identity thefts involving hundreds, sometimes thousands, of individuals now make headlines nearly every day. In an effort to stem the increasing incidence of such events, which cost businesses, financial institutions, and individuals billions of dollars a year, the Office of Consumer Affairs and Business Regulation (OCABR) has promulgated a set of regulations designed to protect Massachusetts residents' Personal Information.² The regulations, set forth at 201 C.M.R. 17.00, require every business in Massachusetts to develop, implement, and maintain a comprehensive, written data security program ("Program").

After much public input, OCABR released a significantly amended version of the regulations on August 17, 2009. These amendments again extend the compliance date. They also limit the scope and specificity of some requirements contained in earlier versions of the regulations, and they are now neutral as to specific technological methods of protecting data. On the other hand, they resurrect the requirement of obtaining contracts with third-party service providers concerning the handling of Personal Information. This document gives an overview of the material changes to the regulations. It should be read in conjunction with our previous summary of the original Massachusetts Data Security Regulations, which can be found at www.hrwlawyers.com.

A. 201 CMR 17.01: Purpose and Scope

The amended version of the regulations appears to narrow the category of entities covered. The previous version of the regulations applied to "persons who own, license, *store or maintain* personal information" of Massachusetts residents. This version strikes the words "store or maintain." Nevertheless, those who store or maintain Personal Information will still be required to comply with the regulations if they fall within the definitions of either one who "owns or licenses" Personal Information or one who acts as a "service provider" in relation to Personal Information.

¹ This document was prepared for educational purposes only. It should not be relied on as legal advice. Consult with counsel before making any decisions with respect to the issues discussed in this document.

² "Personal Information" is specifically defined in the applicable statutes and regulations as the first name or initial and last name of a Massachusetts resident plus one of the following numbers: Social Security number, driver's license number, state-issued identification card number, credit card number, debit card number, or financial account number.

Importantly, the amended regulations also now explicitly apply to employers: the definition of “owns or licenses” is “receives, maintains, processes or otherwise has access to personal information in connection with the provision of goods or services or in connection with employment” (emphasis added). This seems to conflict with other changes in the regulations that appear to narrow the regulation’s purpose to one of protecting only *customers* and *consumers*. Specifically, the stated purpose now is “to insure the security and confidentiality of *customer information*” and to “protect against ... substantial harm or inconvenience to any *consumer*.” Nevertheless, the better reading is that OCABR means to include employment information given the inclusion of highlighted addition above of “in connection with employment” and other information released by OCABR and given that the regulations still apply to “personal information” generally.

B. 201 CMR 17.03: Duty to Protect and Standards for Protecting Personal Information

The revised regulations still require that any person or company that owns or licenses Personal Information develop, implement, and maintain a written program that addresses administrative, technical, and physical safeguards, but they now permit the Program to be contained “in one or more readily accessible parts” and require that they be consistent with any applicable federal regulations, which suggests that to the extent a business already has a policy in place that covers a requirement of the regulations, such as a HIPAA policy, it is not necessary for that business to include those provisions again in its written information security program under the regulations. Many businesses may find it most efficient to create one comprehensive data security plan that covers all the various data security to which it is subject.

In addition, several provisions previously required to be in the written program have been removed from the regulations, including, notably, requirements to “limit[] the amount of personal information collected to that reasonably necessary to accomplish the legitimate purpose for which it was collected” and to “identify[] paper, electronic and other records ... to determine which records contain personal information.” Although the removal of these requirements simplifies compliance, it may still be advisable to follow them as best practices.

Though these changes lessen the requirements of compliance, the current iteration of these regulations reinstates the burdensome requirement that every company enter into a contract with each third-party service provider it employs governing the way the service provider handles the company’s Personal Information. This change is modeled after the third-party vendor provision contained in the FTC’s Red Flags Rules. It is unclear from the language of the amendments whether this provision will impact contracts entered into on or after March 1, 2010 or March 1, 2012.

C. 201 CMR 17.04: Computer System Security Requirements

The revised regulations still specify certain technical requirements for electronic storage, use of, and access to Personal Information, but qualify that they are required only “to the extent technically feasible.” Moreover, the definition of “encrypted” has been rendered technically neutral by removing the language requiring that encryption occur “through the use of an algorithmic process or an alternative method at least as secure.”

On the topic of what must be encrypted, the OCABR document entitled “Frequently Asked Questions Regarding 201 CMR 17.00” offers some guidance. This document explains that laptops containing personal information must be encrypted since encryption for laptops is technically feasible, whereas encryption is not yet actually required for most other portable devices, such as cell phones, PDAs, blackberries, net books, and iPhones, because there is little, if any, generally accepted encryption technology for these devices. As for back-up tapes, the OCABR document explains that back-up tapes must be encrypted on a going-forward basis and that existing back-up tapes must be encrypted, if it is technically feasible, if they are transported from their current storage.

D. 17.05 Compliance Deadline

The amendments extend the compliance deadline from January 1, 2010, to March 1, 2010.

E. How Do These Amendments Affect You As a Business Owner and/or Employer?

Even with these amendments, the Massachusetts Data Security Regulations are still some of the broadest in the country. Any person or entity that owns or licenses (which, by definition, includes any person that maintains or has access to) Personal Information of a Massachusetts resident must comply by March 1, 2010, which again includes obtaining contracts from third-party vendors.

The OCABR will be holding a public hearing on Tuesday, September 22 at 10 a.m., and a member of the HRW Data Security Team will be there to seek clarification of, and possibly other changes to, these amendments.