

Personal Information Security Regulations Amended Again: New Compliance Deadline of March 1, 2010

August 2009

RENEE INOMATA

is Partner & Chair
of the Firm's Labor,
Employment &
Employee Benefits
Group.



Massachusetts General Laws, Chapter 93H, enacted in November 2007, requires (1) notification of data security breaches and (2) requirements to ensure the protection of personal information. Although the notification requirements became effective almost immediately, the final regulations issued to implement this law only recently clarified the prevention requirements. The final regulations (201 CMR 17.00) implementing Chapter 93H's requirements were issued in February. These regulations also incorporate Chapter 93H's sister statute, Massachusetts General Laws, Chapter 93I, which addresses destruction of documents and media containing personal information.

Businesses may now have until March 1, 2010 – rather than January 1, 2010 – to comply with the regulations for the protection of Personal Information. On August 17, 2009, the Massachusetts Office of Consumer Affairs and Business Regulation (OCABR) issued a notice of public hearing for revisions to the regulations for the protection of Personal Information. If they remain unchanged after the September 22, 2009 public hearing, in addition to extending the compliance date to March 1, 2010, the revised regulations will ease some of the technical requirements for compliance in order to address small business concerns about the burdens of the prior regulations and provide more clarity with respect to third-party service provider data protection

requirements. As with the prior iterations of the regulations, the newly revised regulations will apply to “Personal Information,” defined as the combination of the **first and last name**, or **first initial and last name**, of a Massachusetts resident **together** with any of the following:

- (a) social security number; or
- (b) driver's license or state identification card number; or
- (c) credit card or financial account number, such as a bank or retirement account number.

HOW WILL THE TECHNOLOGY REQUIREMENTS CHANGE?

The February 2009 version of the regulations had defined encryption as the “transformation of data through the use of an algorithmic process, or an alternative method at least as secure, into a form in which meaning cannot be assigned without the use of a confidential process or key, unless further defined by regulation by the Office of Consumer Affairs and Business Regulation.” The newly revised regulations do not require an algorithmic process or an alternative method at least as secure for encryption of Personal Information. Rather, data will only need to be transformed into “a form to which meaning cannot be assigned without the use of a confidential process or key.” Consequently, complicated and expensive software will not be necessary, particularly for smaller businesses which have smaller quantities of Personal Information, or which transmit Personal Information infrequently.

HOW WILL THIRD-PARTY SERVICE PROVIDER HANDLING OF PERSONAL INFORMATION CHANGE?

The newly revised regulations clarify, what were previously only described as “all

reasonable steps” to ensure that third-party service providers with access to Personal Information had the capacity, and were in fact implementing measures to protect Personal Information as required by the regulations. The revised regulations will require businesses to “(f) Oversee service providers, by: 1. Taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such personal information consistent with these regulations and any applicable federal regulations; and 2. Requiring such third-party service providers by contract to implement and maintain such appropriate security measures for personal information; provided, however, that any contract a person has entered into with a third-party service provider prior to March 1, 2012, shall be deemed to be in compliance herewith, notwithstanding the absence in any such contract of a requirement that the service provider maintain such protective security measures, so long as the contract was entered into before March 1, 2010.”

Simply put, businesses cannot carelessly turn over Personal Information to a third-party service provider. At a minimum, businesses will need to confirm that said third-party service provider is aware of the regulations' requirements, has the ability to comply, and in fact agrees to comply with the regulations.

ADDITIONAL CHANGES:

The newly revised regulations also eliminate two specific requirements from a Written Information Security Plan (WISP). The February 2009 regulations required that a WISP include, among other things:

- “Limiting the amount of personal information collected to that reasonably necessary to accomplish the legitimate purpose for which it is collected;

limiting the time such information is retained to that reasonably necessary to accomplish such purpose; and limiting access to those persons who are reasonably required to know such information in order to accomplish such purpose or to comply with state or federal record retention requirements”; and

- “Identifying paper, electronic and other records, computing systems, and storage media, including laptops and portable devices used to store personal information, to determine which records contain personal information, except where the comprehensive information security program provides for the handling of all records as if they all contained personal information”.

Although these two provisions have been eliminated, businesses will still need to consider similar elements as they are preparing their WISPs.

WHAT TO DO NOW:

The periodic revisions to the regulations, included repeated extensions in the compliance deadline, for 201 CMR 17.00, et seq., seem to argue against taking any action now; however, the revisions are not so substantial as to eliminate the need to review security measures for the protection of Personal Information. Notwithstanding OCABR’s efforts to ease some of the burdens on smaller businesses, compliance with the newly revised regulation will still require all businesses to (1) identify what Personal Information will need to be protected and how to protect such Personal Information; (2) have a written plan addressing protection of Personal Information; (3) educate their employees about complying with the written plan; and (4) confirming all third party service providers are also complying with the newly revised regulations.

*The Labor, Employment, & Employee Benefits Group provides compliance advice, drafts policies, conducts training, and defends employers against workplace claims and litigation. For more information please contact a member of Burns & Levinson’s Labor, Employment & Employee Benefits Group or email us at clientservices@burnslev.com. If you have questions regarding this Update, please contact **Renee Inomata** at rinomata@burnslev.com or **617.345.3340**.*

*If you would like to be added to or removed from the mailing list for Burns & Levinson Employment Updates or other Burns & Levinson publications, please send your name, email address and notice to clientservices@burnslev.com or call **Judy Crowley** at **617.345.3632**.*