

Client Advisory | August 2009

## Amended Massachusetts Security Regulations and Extension of Effective Date

On August 17, 2009, the Massachusetts Office of Consumer Affairs and Business Regulation (OCABR) issued a press release announcing important amendments to 201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth (the Regulations), and a third extension of its effective date from January 1, 2010 to March 1, 2010.



Theodore Augustinos,  
Partner



Mark E. Schreiber,  
Partner



Soceth Sor,  
Associate

In addition to extending the effective date, the amendments (i) clarify the risk-based approach to the Regulations, (ii) coordinate the requirements for third-party vendors with similar requirements of federal law, and (iii) require appropriate encryption technology to the extent technically feasible. The OCABR also offered further guidance through additional Frequently Asked Questions (FAQs) issued along with the amendments. The OCABR also called a public hearing scheduled for September 22, 2009 in connection with the Regulations.

As reported in our [previous Client Advisories](#), the Regulations require any business, regardless of size and location, that owns, licenses, stores or maintains “personal information” of Massachusetts residents, including customers, employees, and others, to develop a written information security program (WISP) or revise its existing security policies, to amend third-party contracts, and to implement encryption and other safeguards to satisfy the Massachusetts requirements. Personal information means first name and last name or first initial and last name plus a Social Security number, driver’s license number, financial account number or credit card of any Massachusetts resident, including employees, customers, vendors, or insureds.

In an effort to ease the burden on small businesses, the OCABR amended the Regulations to make clear that the Regulations are risk-based in both implementation and enforcement, stressing the notion that there is no one-size-fits-all WISP. Compliance with the Regulations will

be judged on a case-by-case basis to take into account the following factors: (i) the size, scope and type of business handling the information; (ii) the amount of resources available to the business; (iii) the amount of stored data; and (iii) the need for security and confidentiality of both consumer and employee information. This risk-based approach brings the Regulations in line with both the enabling legislation and applicable federal law, including the Safeguards Rule (16 CFR Part 314) promulgated by the Federal Trade Commission, which requires financial institutions to have a security plan to protect personal consumer information.

The Regulations have also been amended to make third-party vendor requirements consistent with federal law. Under the amended Regulations, companies must oversee their third party vendors by:

- i. 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
- ii. requiring such third-party service providers by contract to implement and maintain such appropriate security measures for personal information.

Another notable change to the Regulations includes making the encryption requirement flexible. In keeping with the risk-based approach, the Regulations are now technology neutral, meaning they do not require specific encryption technology. Further, encryption

is required only to the extent “technically feasible.” The phrase “technically feasible” is defined in the FAQs to mean “if there is a reasonable means through technology to accomplish a required result, then that reasonable means must be used.”

The new FAQs also clarify important issues, including the following:

- i. Portable devices that contain personal information of Massachusetts residents must be encrypted where it is reasonable and technically feasible to do so.
- ii. An account is a financial account, and thus must be protected under the WISP, if unauthorized access could result in an increase of financial burden or a misappropriation of monies, credit or other assets.
- iii. An insurance policy number is a financial account number if it grants access to a person’s finances, results in an increase of financial burden, or a misappropriation of monies, credit or other assets.

- iv. Compliance with HIPAA does not eliminate a company’s obligation to comply with the Regulations if the company owns or licenses personal information of a Massachusetts resident.
- v. Backup tapes must be encrypted prospectively, and existing backup tapes must also be encrypted under certain circumstances.

While the effective date of the Regulations has been postponed to March 1, 2010, there is a considerable amount of work that companies, including many located outside Massachusetts, will need to do to comply.

[Click here](#) to view the official press release announcing the amendments and extension of effective date; [click here](#) to view the FAQs; and [click here](#) to view the amended Regulations.

---

*“In keeping with the risk-based approach, the Regulations are now technology neutral, meaning they do not require specific encryption technology.”*

---

BOSTON MA | FT. LAUDERDALE FL | HARTFORD CT | MADISON NJ | NEW YORK NY | NEWPORT BEACH CA | PROVIDENCE RI  
STAMFORD CT | WASHINGTON DC | WEST PALM BEACH FL | WILMINGTON DE | LONDON UK | HONG KONG (ASSOCIATED OFFICE)

This advisory is for guidance only and is not intended to be a substitute for specific legal advice. If you would like any further information please contact:

Mark E. Schreiber, Partner and Chair, Privacy Group  
Theodore P. Augustinos, Partner  
Laurie Kamaiko, Partner  
Richard Hopley, Partner  
Pat Concannon, Counsel  
Joseph Geoghegan, Associate  
Socheth Sor, Associate  
Sam Tacey, Solicitor

617.239.0585  
860.541.7710  
212.912.2768  
+44.207.556.4532  
617.239.0419  
860.541.7749  
860.541.7773  
+44.207.556.4528

mschreiber@eapdlaw.com  
taugustinos@eapdlaw.com  
lkamaiko@eapdlaw.com  
rhopley@eapdlaw.com  
pconcannon@eapdlaw.com  
jgeoghegan@eapdlaw.com  
ssor@eapdlaw.com  
stacey@eapdlaw.com

This article is published by Edwards Angell Palmer & Dodge for the benefit of clients, friends and fellow professionals on matters of interest. The information contained herein is not to be construed as legal advice or opinion. We provide such advice or opinion only after being engaged to do so with respect to particular facts and circumstances. The firm is not authorized under the U.K. Financial Services and Markets Act 2000 to offer U.K. investment services to clients. In certain circumstances, as members of the Law Society of England and Wales, we are able to provide these investment services if they are an incidental part of the professional services we have been engaged to provide.

Please note that your contact details, which may have been used to provide this bulletin to you, will be used for communications with you only. If you would prefer to discontinue receiving information from the firm, or wish that we not contact you for any purpose other than to receive future issues of this bulletin, please email [UKMarketing@eapdlaw.com](mailto:UKMarketing@eapdlaw.com).

© 2009 Edwards Angell Palmer & Dodge LLP a Delaware limited liability partnership including professional corporations and Edwards Angell Palmer & Dodge UK LLP a limited liability partnership registered in England (registered number OC333092) and regulated by the Solicitors Regulation Authority.

Disclosure required under U.S. Circular 230: Edwards Angell Palmer & Dodge LLP informs you that any tax advice contained in this communication, including any attachments, was not intended or written to be used, and cannot be used, for the purpose of avoiding federal tax related penalties, or promoting, marketing or recommending to another party any transaction or matter addressed herein.

ATTORNEY ADVERTISING: This publication may be considered “advertising material” under the rules of professional conduct governing attorneys in some states. The hiring of an attorney is an important decision that should not be based solely on advertisements. Prior results do not guarantee similar outcomes.

EDWARDS  
ANGELL  
PALMER &  
DODGE

111 Huntington Avenue  
Boston, MA 02199  
Tel 617.239.0100  
Fax 617.227.4420  
[eapdlaw.com](http://eapdlaw.com)