

LABOR & EMPLOYMENT ALERT

**DATA SECURITY STANDARDS IMPLEMENTATION
BY JANUARY 1, 2010****OCABR Postpones New Regulations' Implementation**

On February 12, 2009, less than a month after a public hearing regarding implementation of controversial data security standards regulations, the Massachusetts Office of Consumer Affairs and Business Regulation (OCABR) issued an amendment postponing implementation until January 1, 2010.

At the January 16, 2009 public hearing, Stakeholders responsible for maintaining Massachusetts residents' personal information (generally speaking, a name combined with personal identification or account numbers) aired manifold compliance concerns regarding contractual vendor certifications, personal information inventory, data encryption specifications and cumbersome administrative requirements. While not addressing all of the stakeholders' issues, the OCABR provided (i) necessary relief from the aggressive implementation timetable and (ii) a less restrictive vendor compliance approach.

We recommend that businesses and employers holding Massachusetts residents' personal information take all necessary action to ensure compliance by January 1, 2010.

OCABR's Regulation and Statutory Predicates

Massachusetts has, like most states, recently enacted data breach notice legislation requiring businesses owning, licensing or storing residents' computerized data to notify those residents of unauthorized disclosures of such data. The Massachusetts statute, M.G.L. Ch. 93H, goes beyond most states' legislation by directing OCABR to develop minimum security requirements for businesses and individuals maintaining Massachusetts residents' personal information.

These regulations, entitled the "Standards for the Protection of Personal Information of Residents of the Commonwealth" (201 C.M.R. 17.00), require implementation of two primary safeguards for electronic and paper records containing Massachusetts residents' personal information, each no later than January 1, 2010:¹

- (i) a comprehensive written information security program and
- (ii) a list of minimum security requirements for computer systems electronically storing or transmitting personal information.

National Impact of Regulation

The OCABR regulations represent the most forceful lawmaking attempt to date to promote information privacy and data security. With the Obama administration's campaign commitment to privacy issues, the Massachusetts regulation is poised to become a proving ground for national legislation along similar lines. Indeed, simply by virtue of the nationwide prevalence and pervasiveness of Massachusetts residents' personal information, this regulation may already be the *de facto* national standard.

¹ The regulations were originally effective January 1, 2009; however, the deadline has been extended to January 1, 2010.

LABOR & EMPLOYMENT ALERT

Impact Upon You and Your Business

You should evaluate (i) the personal information you own, license, store or maintain, (ii) the state of your policies, procedures, and systems, (iii) whether the regulation applies to you or your business, and (iv) whether the regulation applies to your contracting relationships (requiring your compliance to maintain the relationship). Even if you believe the Massachusetts regulation does not apply to you, you should be aware of its national scope and the general trend toward more heavy-handed regulation in this area. OCABR's impact statement estimated small business compliance costs to equal (for every ten employees) \$3,000 initially and \$500 per month afterward.

OCABR's Definition of Personal Information

"Personal information," for the regulations' purposes, means a Massachusetts resident's first name (or first initial) and last name *combined* with such resident's Social Security number, driver's license number, or any financial account number, debit account number, or credit card number.² If such information is lawfully obtained from (i) publicly available information or (ii) federal, state, or local government records, it is excluded from the regulations' definition of "personal information."

Broad Reach of Regulations

All individuals and entities owning, licensing, storing or maintaining a Massachusetts resident's personal information are subject to the regulations.³ OCABR's regulation does not end at the Massachusetts state line; it reaches across state boundaries to cover out-of-state individuals and entities. Further, the regulations do not exempt industries regulated by the federal government, other state governments or foreign governments. Therefore, an organization is still subject to the regulations despite complying with its own applicable regulatory requirements for protecting records containing personal information.

Comprehensive Written Information Security Program

Individuals and entities owning, licensing, storing or maintaining a Massachusetts resident's personal information must develop, implement, maintain and monitor a comprehensive written information security program (WISP) to protect any such information. WISPs must be consistent with both industry standards and the various state and federal regulations by which such individuals and entities may be regulated.⁴ Further, WISPs must contain safeguards (administrative, technical and physical) ensuring personal information's security and confidentiality.

Minimum WISP Requirements

All written information security programs must address the following minimum requirements:⁵

² This information need not be accompanied by the resident's security/access code, personal identification number or password for inclusion as "personal information."

³ Massachusetts state government agencies, excluded from the definition of "person," are covered by the Massachusetts governor's Executive Order No. 504.

⁴ The regulation hedges in this manner at several critical points; such over-arching requirements could create compliance uncertainty. At the very least, such language imposes an ongoing obligation to adhere to the regulation's "best practices" intent.

⁵ See 201 C.M.R. 17.03(3)(1)-(12).

LABOR & EMPLOYMENT ALERT

A. *WISP Implementation, Oversight and Evaluation*

1. Designating one or more employees with responsibility for WISP maintenance and oversight.
2. Identification and assessment of reasonably foreseeable security risks (both internal and external) to electronic, paper, and other records containing personal information.
3. Establishing and maintaining a computer security system as further described in the section entitled “Computer Security System Requirements,” below.
4. Monitoring the WISP regularly to ensure operation “reasonably calculated to prevent unauthorized access to or use of personal information” and periodically upgrading security measures as necessary.
5. Reviewing security measures not less than annually – or more frequently if there are material changes in business practice impacting personal information security or record integrity.
6. Evaluating and undertaking necessary improvements to increase the WISP’s effectiveness by: (i) implementing employee training programs; (ii) monitoring employee compliance with WISP rules; and (iii) improving detection and prevention of security system failures.
7. Documenting security breaches, including post-incident reviews of events and actions taken, to review and enhance business practices and the WISP.

B. *Intake and Identification of Personal Identification*

1. Limiting the amount of personal information collected, and retention period for such information, to a level “reasonably necessary to accomplish the legitimate purpose for which it is collected.”
2. Identifying (i) paper, electronic and other records containing personal information and (ii) computer systems, laptops, portable devices and other media used to store personal information.⁶

C. *Personnel Access to Personal Information*

1. Restricting employee access to personal information to individuals “reasonably required to know” such information in order to (i) achieve the “legitimate purpose for which it is collected” and (ii) comply with state or federal record retention requirements.
2. Restricting physical access to records containing personal information pursuant to a written procedure by, among other things, storing secure records and data in locked facilities, storage areas or containers.
3. Minimizing employees’ access to, and maintenance, retention, and transport of, records containing personal information off business premises.
4. Imposing disciplinary measures for WISP rule violations.
5. Restricting terminated employees’ access to physical and electronic records immediately upon termination.⁷

D. *Third Party Service Provider Access to Personal Information*

1. Verifying that third party service providers having personal information access are capable of maintaining required WISP safeguards.
2. Verifying that third party service providers having personal information access apply security measures at least as stringent as those required under the regulations.⁸

⁶ This process identifies the personal information records or systems to which the regulations are primarily applicable; however, it may be appropriate to treat some or all of these records or systems more cautiously as if containing or storing personal information.

⁷ Password and user name deactivation is required.

⁸ The February 12, 2009 amendment eliminated the troublesome vendor certification requirement for third party service providers having personal information access requiring a written certification of a compliant WISP. Instead,

LABOR & EMPLOYMENT ALERT

Computer Security System Requirements

The regulations enumerate minimum requirements for computer systems electronically storing or transmitting personal information. All computers, laptops and other electronic devices storing or transmitting personal information, including transmissions via wireless systems, are addressed. Such devices and systems must be protected by a security system incorporating the following base elements:

1. Secure user authentication protocols, including: (i) control of user IDs and other identifiers; (ii) reasonably secure password assignment and selection methodology;⁹ (iii) control and secured storage and/or formatting of all data security passwords; (iv) restrictions on access to active users and active user accounts; and (v) denial of login access after multiple failed attempts.
2. Secure access control measures that: (i) restrict access to personal information records to employees requiring such information to perform job duties; (ii) “reasonably design” institutional IDs and passwords in a manner that is calculated to maintain the integrity of access control security; and (iii) assign a unique ID and password (not vendor-supplied default passwords) to each person with computer access.
3. Encryption of all personal information that will be transmitted across public networks or transmitted wirelessly to the extent technologically feasible.
4. Reasonable system monitoring for unauthorized use of, or unauthorized access to, personal information.
5. Encryption of all personal information stored on laptops or other portable devices. The deadline for ensuring encryption of data on laptops and other portable devices is January 1, 2010.
6. For records containing personal information on an Internet-linked system (physically or wirelessly), reasonably up-to-date firewall protection and operating system security patches reasonably designed to maintain the integrity of such personal information.
7. Reasonably up-to-date versions of system security agent software, with malware and virus protection, which are diligently maintained and upgraded.
8. Employee education and training on proper use of computer security system and importance of personal information security.

Evaluating Your Personal Information Security Program

The regulations provide little guidance on practical aspects of WISP implementation. In order to determine whether a particular WISP is compliant, however, the regulations specify that the following factors must be taken into account:

1. size, scope and type of business of the person obligated to safeguard the personal information under the program;
2. amount of resources available to such person;

under the current regulations, verification consists of “all reasonable steps,” leaving the parties to determine what is reasonable under the circumstances. In Section 9 of Executive Order No. 504, there had been an analogous provision with respect to contracts entered into by Massachusetts state agencies, which may be modified by the OCABR consistent with the February 12, 2009 amendments to the general regulations.

⁹ The regulations permit use of unique identifier technologies, such as biometrics or token devices, as an alternative to such methodology.

LABOR & EMPLOYMENT ALERT

3. amount of data stored; and
4. need for security and confidentiality of the stored information.

Failure to Comply

In addition to general OCABR oversight, the Massachusetts Attorney General has enforcement options available for use against non-compliant individuals and entities. The Massachusetts AG's intervention may take the form of an enforcement action under the Commonwealth's consumer protection statute, M.G.L. ch. 93A. Injunctive relief could be sought regarding continuing noncompliance and fines could be assessed for each method, act or practice violating the regulations (up to \$5,000 for each, plus attorneys' fees, and \$15,000 for willful violations). It remains unclear whether out-of-state companies holding Massachusetts residents' personal information will be targeted by enforcement actions.

M.G.L. ch. 93A permits private rights of action as well and, further, the failure to comply with the OCABR regulation may be used as evidence of negligence. Violating this regulatory framework (where none had previously existed) may render breaches of security and associated defense costs uninsurable under standard commercial general liability policies – or even many cyber risk policies – without special endorsements.¹⁰

Additional Government Guidance

Additional OCABR guidance is available on its website, www.mass.gov/ocabr. OCABR published informative materials on establishing information security programs: a model WISP for small businesses, a link to frequently asked questions and, most importantly, a compliance checklist. Notably, while OCABR's model program sets forth practical suggestions for implementation, it also includes numerous provisions that appear to exceed the scope of the regulations. The model program should be used as a guide and adapted to the particular circumstances of each company implementing a written information security program.

Conclusion

Each individual and entity owning, licensing, storing or maintaining personal information within the meaning of 201 C.M.R. 17.00 et seq. needs to work steadily towards eventual compliance in time for the OCABR's January 1, 2010 deadline.

For more information, contact **Michael C. Hackett** at mhackett@eckertseamans.com or 617-342-6835. Mr. Hackett is a corporate attorney at Eckert Seamans Cherin & Mellott, LLC's Boston office practicing in the Business Division. In addition, you may contact any other Eckert Seamans Cherin & Mellott, LLC attorney with whom you have been working.

NOTE: The information in this Labor & Employment Alert is for general, educational purposes. It is not intended to be, and should not be considered, legal advice with respect to any particular situation.

© Eckert Seamans Cherin & Mellott, LLC, 2009, all rights reserved.

¹⁰ Note that there is a burgeoning market for insurance covering a variety of cyber risks, most of which will require an initial security assessment. Companies considering insuring some of their risks in this area must review policy language carefully as coverages vary widely.