

**OPINION**

# Up close look at state's new data security regulations

By Mark E. Schreiber, Theodore P. Augustinos and Socheth Sor



SCHREIBER



AUGUSTINOS



SOR

Massachusetts has adopted final data security regulations that are now fully effective Jan. 1, 2010, and will affect almost every business in the state (and others outside Massachusetts), large and small, including law firms.

These requirements are currently the most rigorous in the country, outstripping California and the new federal Red Flag rules for financial institutions and creditors. The regulations will require significant security and other policy changes, including encryption of laptops, PDAs and wireless communications, and, as many are rapidly realizing, will involve far more work than first anticipated.

The breadth of the regulations is impressive, and the impact is already being felt nationally. There are no industry, private sector or out-of-state exemptions and no de-minimus number of employees under the regulations.

Massachusetts is now, in important respects, driving aspects of the data security agenda across the country. Absent federal legislation, some major cor-

*Mark E. Schreiber is an employment litigation partner in the Boston office of Edwards Angell Palmer & Dodge. Theodore P. Augustinos is a partner, and Socheth Sor an associate, in the insurance reinsurance department at EAP&D's Hartford, Conn., office.*



**Massachusetts is now, in important respects, driving aspects of the data security agenda across the country.**

issue security regulations to safeguard the personal information of Massachusetts residents.

Many thought these regulations would address ambiguities and offer guidance on data breach notification steps and issues. Taking a broader stance, the OCABR created a comprehensive tool designed to prevent data breaches and instituted an expansive policy approach to accomplish that goal.

Regulation 201 CMR 17.00, Standards for the Protection of Personal Information of Residents of the Commonwealth (the regulation),

was finalized in September 2008, with additional changes in mid-February.

It establishes minimum standards for private businesses in safeguarding personal information contained in both paper and electronic records. (Only state and local governmental entities are not covered, but they have to implement their own security regulations.)

Under the regulation, every person (the definition of "person" includes business entities) that owns, licenses, stores or maintains personal information about a resident of Massachusetts is required to develop, implement, maintain and monitor a comprehensive, written information security program (WISP).

The effective date of the regulation was initially Jan. 1, 2009, but after industry opposition and extensive comments in late November 2008, the OCABR extended the date to May 1, 2009, and most recently to Jan. 1, 2010.

porations are already adopting the most severe state data security standard, in this case Massachusetts, as a compliance approach across their operations.

The new regulations have spurred extensive company scrutiny of existing policies and accelerated identification of the numerous definable tasks, upgrades and follow-up necessary to implement this new security regime.

Frequently, this involves first pulling together a dedicated team from legal, IT, compliance, human resources or other departments, as the strategic questions and resultant "to do" list cross several disciplines and units.

Some entities, including those that have yet to begin this exercise, will find major challenges and difficulties in meeting these obligations and the Jan. 1, 2010, date.

**Background**

Chapter 93H, An Act Relative to Security Freezes and Notification of Data Breaches, requires the Office of the Consumer Affairs and Business Regulation to

### What the regulations require

The regulations are divided into four sections: (1) purpose and scope, (2) definitions, (3) requirements of a WISP and (4) minimum computer security requirements a company must maintain. The full text of the regulation and other guidelines can be found on the OCABR website at

<http://www.mass.gov/?pageID=ocatopic&L=3&L0=Home&L1=Business&L2=Identity+Theft&sid=Eoca>.

OCABR also issued a set of FAQs, a compliance checklist and a model policy for small businesses (all available on the OCABR website). Hopefully, the OCABR will issue further explanatory FAQs, including on terms or areas of encryption like "other portable devices."

### The definition of personal information

The regulation protects the personal information of Massachusetts residents, which is defined to mean the first name and last name or first initial and last name in combination with any one or more of the following of a Massachusetts resident:

- (1) Social Security number;
- (2) Driver's license number or state-issued identification card number; or
- (3) Financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account.

Information that is publicly available or can be obtained from government records is not considered personal information.

### WISP

Under the regulation, every person or company that owns, licenses, stores or maintains personal information about a Massachusetts resident must develop, implement, maintain and monitor the WISP.

The WISP must be reasonably consistent with industry standards and is required to contain administrative, technical and physical safeguards to ensure the security and confidentiality of such records.

The WISP provisions are both quite broad and very granular and effectively demand an assessment of the company's personal data collection and protection practices, an entire systems review, and policy and other reconfigurations where necessary. The company's WISP must, inter alia, do the following:

- Identify documents, devices and other records that contain personal information;
- Limit the amount of personal information collected and the length of time it is stored;
- Limit access to personal information on a need-to-know basis;
- Identify and evaluate internal and external risks;
- Regularly monitor employees' access to personal information;
- Block terminated employees' access to documents, devices and other records that contain personal information;
- Take all reasonable steps to ensure third-party service providers' compliance with the regulation;

- Review security measures annually and update the WISP when there is a material change in the business operations;
- Develop and maintain a procedure for actions taken in response to any breach of security;
- Train employees about and discipline employees for violation of the policy; and
- Designate one or more employees to maintain, supervise and implement the WISP.

### Computer security requirements

The WISP must also address the establishment and maintenance of a detailed computer security program, which must include:

- Encryption of all transmitted records and files containing personal information that is stored on laptops and other portable devices and/or will travel across public networks or wirelessly;
- Secure user authentication protocols and access control measures, including control over user identifiers, passwords and access;
- A system for monitoring unauthorized use; and
- Up-to-date firewalls, anti-virus definitions and anti-malware programs.

A company must evaluate its computer systems to determine what must be done to bring the company into compliance. Fortunately, the definition of "encryption" is flexible and not limited to 128 bit, and permits other mechanisms equally secure; this would allow for masking, hashing and future developed security vehicles.

Whether, as a practical matter, these encryption requirements can be limited to systems that contain only Massachusetts personal data remains to be seen. Encryption on certain devices or communications will take some effort to achieve, even if a company has an adequate IT staff or resources to implement a compliant computer security program.

### Strategic and implementation choices

A number of strategic questions and issues have already surfaced and frequently must be addressed before implementation.

A company may need to decide between selective versus full-enterprise protection. That is, should protection extend to only records containing personal information of Massachusetts residents (or employees) or to all records with personal information, regardless of the state of residence?

Large employers with employees in various states, including Massachusetts, face a critical choice point in this respect as a matter of practicality, fairness and policy. For smaller employers, it may be possible to data-strip or redact Massachusetts personal information or set strict rules for laptop or PDA use and storage of personal data, thus reducing the scope of tasks required under the regulation.

Should encryption be at the laptop level, point-to-point or whole disk? The regulation only requires encryption of personal data "stored" on laptops or other portable devices, and data in motion. However, there are additional questions as to how far this extends, such as

to backup tapes, CDs and the like, and the vulnerability of or value of encrypting data at rest.

Another fundamental question involves identification of the data that must be protected. Although an OCABR-issued FAQ makes clear that an inventory of all papers and electronic records is not required, companies still must identify which records contain personal information.

This may be an easier task for smaller companies, but larger corporations may have to review prior data audits, begin a new data inventory or both. It is not uncommon to discover in this process previously unknown data storage locations or repositories, including data on a variety of unprotected or unencrypted servers or legacy systems.

Companies that already have a computer security policy in place must also decide whether to create a new WISP or build the regulation requirements into an existing policy or policies.

If there are several existing policies, including computer security incident response (CSIRP), crisis management, data breach escalation or a Red Flag policy (still due by May 1, 2009), one possibility is to have a master WISP, linking or integrating these other policies. Experience has begun to show that drafting the WISP is best left until after some of the above decisions have been made.

### Vendor compliance

The issue of third-party vendor compliance is an equally important one. As noted, companies must ensure by Jan. 1, 2010, that their third-party vendors with access to the personal information of Massachusetts residents are in compliance with the regulation.

The strategic questions here involve how to identify, capture and update the relevant contracts, service agreements and renewals, either regularly or on a rolling basis.

Fortunately, the final regulation eliminated the mandatory written certification from vendors that had been required by the regulation in its prior form. At minimum, companies should begin identifying their existing third-party vendors with access to the personal information of Massachusetts residents, and begin amending their service agreements. Amendments will undoubtedly include new versions of security representations and warranties, which are already beginning to appear.

### Enforcement

The regulation will be enforced by the Attorney General's Office. Compliance with the regulation will depend on the (1) the size, scope and type of business; (2) the amount of resources available to such person; (3) the amount of data stored; and (4) the need for security and confidentiality of both consumer and employee information.

Compliance is evaluated on a case-by-case basis, and, as such, a WISP must be customized for each business. Deficiencies in compliance after Jan. 1, 2010, especially after a data breach, are sure to draw attention by regulators and perhaps by civil litigants, although no enforcement guidelines have yet been issued and there is no private right of action under Chapter 93H itself. ■