

The New Massachusetts Data Security Rules

January 28, 2009

David J. Goldstone



Agenda

- Introduction
- Scope of Rules
- Comprehensive Written Information Security Program
- Computer System Security Requirements
- What To Do Now
- Questions and Answers

Summary

- Rules issued on September 19, 2008, originally scheduled to take effect January 1, 2009
- May 1, 2009: bulk of rules effective
- January 1, 2010: deadlines for vendor certification and encryption of non-laptop portable devices
- Rules apply to all entities, wherever located, with “personal information” of Massachusetts residents

Summary

- **Businesses must have**
 - Comprehensive written information security program
 - Heightened security procedures (including encryption)
 - Vendor contract provisions and certifications
- **Consequences for non-compliance: increased risk of government enforcement or private litigation**

What Prompted the Rules?

- High-profile data breach cases
- Breach notification alone insufficient
- Reflection of states' interest in protecting personal information
- Regulators determined data in transit or on portable devices most at risk
- Massachusetts is the first, but is likely not the last

What's On Your Mind

- How do the rules affect regulated entities?
- What is a “financial account”?
- Do the rules increase risk of private litigation?
- How does the size of your business affect your compliance obligations?
- What must a vendor certification include?
- What constitutes a “portable device”?

Scope of Rules

- Covers any entity that owns, licenses, stores and/or maintains personal information about Massachusetts residents
- Need not have operations in Massachusetts
- Financial institutions, health care and other regulated entities not exempt

Scope of Rules

- “Personal information” is:
 - Resident’s first and last name or first initial and last name in combination with
 - Social Security, driver’s license or financial account number
- “Financial account” flexible as in statute

Two Requirements

- Develop, implement and maintain a comprehensive written information security program that meets very specific requirements
- Heightened information security: Entities must meet specific computer information security requirements

Evaluating Compliance

- Factors:
 - Entity's size, scope and type of business
 - Entity's resources
 - Amount of stored data
 - Need for security and confidentiality of both consumer and employee information

Enforcement

- Litigation and enforcement by the Massachusetts Attorney General
- Massachusetts law requires notice to Attorney General of any breach, in addition to affected consumers
- Attorney General likely to investigate based on breach reports
- No explicit private right of action or penalties

Information Security Program

- “Develop, implement, maintain and monitor” a “comprehensive, written information security program”
- Applicable to “any records” with personal information
 - “reasonably consistent with industry standards”
 - “administrative, technical, and physical safeguards”
 - Many specific items “shall” be included

Information Security Program – Comprehensive

- Identify all records used to store personal information
- Identify and assess risks
 - Internal and external
- Evaluate (and improve) safeguards
 - Employee training and compliance
 - Security system
- Limit collection and use
 - Tailored to purpose, time, and access

Information Security Program – Administrative

- Designate employee(s) responsible
- Develop security policies for employees
 - Including keeping, transporting and accessing records off-site
- Verify capacity of service providers to protect personal information
 - Selecting and retaining service providers “capable of maintaining safeguards” and contracting to do so
 - Certification of compliance with Massachusetts rules required by January 1, 2010

Information Security Program – Tech/Physical

- Establish and maintain a “security system” for its computers
- Restrict physical access (with locks)
- Prevent access to personal information by former employees
 - “immediate” termination of access
- In event of “a breach of security”
 - Document responsive actions taken

Information Security Program – Maintain/Monitor

- “Mandatory post-incident review” to make changes in business practices
- Disciplinary measures for violations
- Regular monitoring to ensure the program is operating
 - Upgrade as necessary
- Review security measures annually or whenever there is a material change in business

Computer System Security Requirements

- All computer systems (including any wireless system) must meet seven specific security requirements
- Encryption:
 - Encryption of stored information
 - Encryption of information in transit
 - Key Issues:
 - Costs; Recipient ability to access transmitted information; Information stored with third parties

Computer System Security Requirements

- Other security requirements
 - Secure user authentication protocols
 - Reasonable monitoring of systems
 - Firewall protection
 - Malware and virus protection
- Education and training

Compliance Deadlines

By May 1, 2009

- Implement internal policies and practices
- Encrypt company laptops
- Amend contracts with service providers to incorporate the data security requirements

By January 1, 2010

- Obtain written certification from service providers
- Encrypt other (non-laptop) portable devices

Action Plan

- **Form a team**
 - Include necessary IT, HR, Legal and Compliance personnel
- **Review existing policies**
 - Do your current data security policies and procedures create barriers to compliance by May 1, 2009?
- **Map data flows that include personal information**
 - Consider limiting collection of personal information and restrict access to those with a need to know

Action Plan

- Identify internal and external risks and effectiveness of current safeguards
- Draft comprehensive written information security program
- Negotiate amendments to vendor agreements and obtain vendor certifications
- Encrypt laptops, portable devices and data in transit

Action Plan

- Restrict access to personal information
- Train employees
- Institute monitoring and self-auditing procedures
- Update systems including firewall protection and malware and virus protection

Additional Questions

- What about back-up tapes in storage with a vendor?
- What are alternative methods “at least as secure” as encryption?
- What is a “public network”?
- How do you determine “to the extent technically feasible” to encrypt emails sent over a public network?

Resources

- Statute (M.G.L. c. 93H)
- Rules (201 CMR 17.00)
- OCABR Guidance
- Goodwin Procter's Privacy & Data Security Practice

GOODWIN | PROCTER

Thank You

David Goldstone,
Goodwin Procter LLP
Exchange Place
Boston, MA 02109
(617) 570-1707
dgoldstone@goodwinprocter.com