

International Association of Privacy Professionals
Practical Privacy Series
New York City




**MASSACHUSETTS OFFICE OF
CONSUMER AFFAIRS AND
BUSINESS REGULATION
AND
DATA SECURITY LAW**

Barbara Anthony
Undersecretary of Consumer Affairs and Business Regulation
Commonwealth of Massachusetts

October 29, 2012

Helpful businesses. Smarter consumers.

1



This Presentation Covers:

- The Notification Requirement
- Defining "Personal Information"
- The Regulation: An Overview
- Required Safeguards
- How to Safeguard
- Recent Actions
- Top 10 Issues in Data Security Law

Helpful businesses. Smarter consumers.


2



Massachusetts Data Security Law
Data Breach Notifications Law
Data Security Regulations


Helpful businesses. Smarter consumers.

3




The Massachusetts Notification Law

- M.G.L. c. 93H § 3
- A person who owns or licenses a resident's personal information (PI) must notify:
 - The resident affected
 - The Attorney General
 - OCABR
- When the person knows or has reason to know of:
 - A security breach or
 - An unauthorized use



Buffer businesses, empower consumers.

4




The Massachusetts Notification Law

- The notice to the MA state offices must include
 - nature of the breach
 - number of residents affected
 - steps taken or to be taken in response
- The notice to the MA resident must include
 - information about the right to obtain a police report
 - how to request a security freeze
 - fees to be paid to a consumer reporting agency
 - *NO* information about the nature of the breach
 - *NO* information about the number of residents impacted.

Buffer businesses, empower consumers.

5



Defining "Personal Information"


Last Name, First Name or Initial
PLUS

1. Social Security Number	OR	2. Driver's license (or state-issued ID)	OR	3. Financial account or credit/debit card number (with or without pin)
-------------------------------------	-----------	--	-----------	--

Note: PI Includes Employee Information


Buffer businesses, empower consumers.

6




The Regulation: An Overview

- The regulation applies to
 - Entities that own or license PI
- What is covered
 - A MA resident's PI
- It requires encryption of PI that is
 - Transmitted over public networks
 - Transmitted wirelessly
 - On laptops & portable devices



Buffer backrooms. Smarter consumers.

7




Required Safeguards

All organizations must have a Written Information Security Program (WISP)


The WISP must contain

- Evaluation of reasonably foreseeable risks to PI
- Evaluation of current safeguards
- Employee training and compliance
- Policies/procedures for storage, access, and transport
- Documentation of responses to a security breach



Buffer backrooms. Smarter consumers.

8



Third-Party Service Providers

- Due Diligence
 - Select a service provider capable of protecting PI
- Contract Requirements
 - Require, by contract, that the service provider implement and maintain data security protections
 - Grace period for contracts signed before Mar. 1, 2010 expired Mar. 1, 2012

Buffer backrooms. Smarter consumers.

9



How to Safeguard PI

System Security Methods


- Control Access
- Encrypt
- Monitor






Helpful businesses. Smarter consumers.

10



Data Security Enforcement in Mass. The Attorney General

- Applicable Authority
 - M.G.L. c. 93H § 6
 - M.G.L. c. 93A § 4
- MGL Ch. 93A § 4 allows for
 - Injunctive relief
 - Restitution
 - Civil penalties up to \$5,000 for each violation
 - Investigation costs and attorneys' fees



Helpful businesses. Smarter consumers.

11




Data Security Enforcement in Mass. Private Right of Action

- Data privacy law is silent as to private action
- 93A is broad and allows private action
 - Broad language – unfair and deceptive acts
 - Potential double or treble damages
 - Equitable relief
 - Attorneys' fees and costs



Helpful businesses. Smarter consumers.

12




MA Actions Under Data Security Law

- Briar Group LLC – 125,000 credit card #s
 - \$110K penalty
- Belmont Savings Bank – 13,000 bank account #s
 - \$7,500 penalty
- Maloney Properties – 600 customer SS #s
 - \$15,000 penalty
- South Shore Hospital – 800,000 patients' data
 - \$750,000 penalty

Helpful businesses. Smarter consumers.


13



Data Breach Notifications


(Nov. '07 – Nov. '11)

- Total data breach notifications
 - 1,833
- Residents in Massachusetts affected
 - 3,166,031
- Residents protected by encryption
 - 11,367
- Residents protected *if* portable devices were encrypted
 - 1,490,308



Helpful businesses. Smarter consumers.

14




Recent Steps Taken by OCABR

- Designated Ombudsman
- Data Security Brochure for IT Professionals
- Sent out letters to companies that reported breaches that affected over 5,000 residents

Helpful businesses. Smarter consumers.

15



Industry Response from Letters

- Encryption
 - Encrypting data not previously encrypted
 - Even data "at rest" (not required) – South Shore Hospital
- Training
 - Instituting or strengthening existing training programs
 - Many are instituting "reminder" trainings
 - Videos, newsletters, continuing education courses
- Limit accessibility
 - Many companies are changing passwords and restricting access to personal information to employees that need it

Helpful businesses. Smarter consumers.


16



Top 10 Issues With the Massachusetts Data Security Law

Helpful businesses. Smarter consumers.


17



- 1: Must my information security program be in writing?
- 2: How much employee training do I need to do?
- 3: What about the computer security requirements of 201 CMR 17.00?
- 4: Does the regulation require encryption of portable devices?
- 5: Must I encrypt my backup tapes?
- 6: Must I encrypt my email if it contains personal information?

Helpful businesses. Smarter consumers.

18



7: Are there any steps that I am required to take in selecting a third party to store and maintain personal information that I own or license?


8: I am an attorney. Do communications with clients already covered by the attorney-client privilege immunize me from complying with 201 CMR 17.00?

9: I already comply with HIPAA. Must I comply with 201 CMR 17.00 as well?

10: Is everyone's level of compliance going to be judged by the same standard?

Helpful background. Smarter consumers.

19



Q: Must my information security program be in writing?


A: Yes, your information security program must be in writing. The scope and complexity of the document will vary depending on your resources, and the type of personal information you are storing or maintaining. But, everyone who owns or licenses personal information must have a written plan detailing the measures adopted to safeguard such information.

Q: How much employee training do I need to do?

A: There is no basic standard here. You will need to do enough training to ensure that the employees who will have access to personal information know what their obligations are regarding the protection of that information, as set forth in the regulation.

Helpful background. Smarter consumers.

20



Q: What about the computer security requirements of 201 CMR 17.00?


A: All of the computer security provisions apply to a business if they are technically feasible. The standard of technical feasibility takes reasonableness into account. The computer security provisions in 17.04 should be construed in accordance with the risk-based approach of the regulation.

Q: Does the regulation require encryption of portable devices?

A: Yes. The regulation requires encryption of all portable devices that contain PI of customers or employees where it is reasonable and technically feasible. The "technical feasibility" language of the regulation is intended to recognize that at this period in the development of encryption technology, there is little generally accepted encryption technology for most portable devices, such as cell phones, blackberries, net books, iphones and similar devices. The definition of encryption has been amended to make it technology neutral so that as encryption technology evolves and new standards are developed, this regulation will not impede the adoption of such new technologies.

Helpful background. Smarter consumers.

21



Q: Must I encrypt my backup tapes?


A: You must encrypt backup tapes on a prospective basis. However, if you are going to transport a backup tape from current storage, and it is technically feasible to encrypt (i.e. the tape allows it) then you must do so prior to the transfer. If it is not technically feasible, then you should consider the sensitivity of the information, the amount of personal information and the distance to be traveled and take appropriate steps to secure and safeguard the personal information. For example, if you are transporting a large volume of sensitive personal information, you may want to consider using an armored vehicle with an appropriate number of guards.

Q: Must I encrypt my email if it contains personal information?

A: If it is not technically feasible to do so, then no. However, you should implement best practices by not sending unencrypted personal information in an email. There are alternative methods to communicate personal information other through email, such as establishing a secure website that requires safeguards such as a username and password to conduct transactions involving personal information.

Buffer backrooms. Smaller consumers.

22



Q: Are there any steps that I am required to take in selecting a third party to store and maintain personal information that I own or license?


A: You are responsible for the selection and retention of a third-party service provider who is capable of properly safeguarding personal information. The third party service provider provision in 201 CMR 17.00 is modeled after the third party vendor provision in the FTC's Safeguards Rule.

Q: I am an attorney. Do communications with clients already covered by the attorney-client privilege immunize me from complying with 201 CMR 17.00?

A: If you own or license personal information, you must comply with 201 CMR 17.00 regardless of privileged or confidential communications. You must take steps outlined in 201 CMR 17.00 to protect the personal information taking into account your size, scope, resources, and need for security.

Buffer backrooms. Smaller consumers.

23



Q: I already comply with HIPAA. Must I comply with 201 CMR 17.00 as well?

A: Yes. If you own or license personal information about a resident of the Commonwealth, you must comply with 201 CMR 17.00, even if you already comply with HIPAA.

Q: Is everyone's level of compliance going to be judged by the same standard?

A: Both the statute and the regulations specify that security programs should take into account the size and scope of your business, the resources that you have available to you, the amount of data you store, and the need for confidentiality. This will be judged on a case by case basis.

Buffer backrooms. Smaller consumers.

24

