Protecting The Personal Information of Commonwealth Residents

February 9, 2010

By:
Jamy Buchanan Madeja, Esq.
Erik Rexford
Buchanan & Associates
33 Mount Vernon Street
Boston, MA 02108

617-227-8410
www.buchananassociates.com
jmadeja@buchananassociates.com

Why do *I* need to deal with this?!?

- If you are engaged in commerce, the new statute requires it (M.G.L. Ch. 93H)
- Your customers & employees need it
- You or your company are liable under a variety of laws for information security breaches

Scope

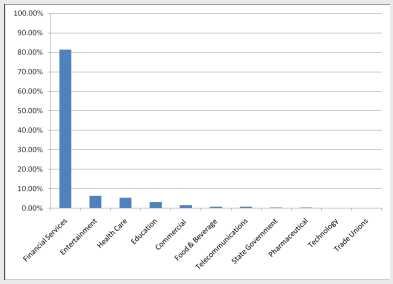
- This is a Massachusetts law that applies to protecting personal information of residents of the Commonwealth, not residents of other states or nations
- There are addition Federal requirements that may apply to the safeguarding of personal information (e.g. HIPA, Gramm-Leach-Bliley Act)

Who has to comply with this?

Any of the following, engaged in commerce:

- Individuals
- Corporations (for profit and non-profit)
- Associations (for profit and non-profit)
- Partnerships
- Sole-Proprietorships
- Pretty much any entity (other than the government)

Where are the common breaches?

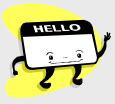


"Personal Information" =

- A Massachusetts resident's first name and last name *or* first initial and last name in combination with any one or more of the following:
  - Social Security number
  - Drivers license number or State issued ID number
  - Financial account number, credit card/debit card number

"Personal Information" ≠

- Information lawfully obtained from publically available information
- Information available from federal, state or local government records lawfully made available to the public



Purpose

"This regulation establishes minimum standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records…The objectives of this regulation are to insure that a customer's personal information is maintained in a manner that insures confidentiality and security" 201 CMR 17.00

NOTE: "In a manner fully consistent with industry standards" is an included official caveat in the regulations

QUESTION: What do you mean, "owns or licenses"?

…receives, stores, maintains, processes, or otherwise has access to personal information in connection with provision of goods or services or in connection with employment."

Question – Employee Info Only?

- **I have a small business with less than ten employees. Besides my employee data, such as direct deposit information, I do not store any other personal information. What are my obligations?**

The regulation adopts a risk-based approach to information security designed to be flexible that takes into account the particular business's size, scope of business, amount of resources and the need for security. If you only have employee data with a small number of employees, you should lock your files in a storage cabinet and lock the door to that room. You should permit access to only those who require it for official duties.

Conversely, if you have both employee and customer data containing personal information, then your security approach would be more stringent. If you have a large volume of customer data containing personal information, then your approach would be even *more* stringent.

When do I need to deal with this?

- The compliance deadline is March 1, 2010
- If you have existing contracts with 3rd party service providers your contracts must comply by March 1, 2012
- Any new contract with a 3rd party service provider must comply as of March 1, 2010

Question – Credit Cards Only?

- **Except for swiping credit cards, I do not retain or store any of the personal information of my customers. What is my obligation?**

If you use swipe technology only, and you do not have actual custody or control over the personal information, then you would not own or license personal information with respect to *that* data, as long as you batch out such data in accordance with the Payment Card Industry (PCI) standards. WATCH OUT – if you "write now and swipe later", that written record is "personal information" to protect

What do I need to do?

Your Duty to Protect Personal Information is two-fold:

- Written Information Security Program (WISP)
- Computer System Security Requirements

Written Information Security Program

"Every person that owns or licenses personal information about a resident of the Commonwealth shall develop, implement, and maintain a **comprehensive information security program that is written** in one or more readily accessible parts and contains administrative, technical, and physical safeguards…"

The Scope of your WISP

- Identify foreseeable internal and external risks to the security, confidentiality, and/or integrity of any records containing personal information
- assess the likelihood and potential damage of these threats
- evaluate your existing policies, procedures, and systems
- the WISP is intended to minimize risks consistent with 210 CMR 17.00
- regularly monitor the effectiveness of the safeguards you put in place

REMEMBER: "FULLY CONSISTENT WITH INDUSTRY STANDARDS" – **DO KEEP UP WITH THE JONESES!**

The WISP is specific to your organization, and should take into account:

- the size, scope and type of business
- amount of resources available to business
- the amount of stored data
- the need for for security and confidentiality of both consumer and employee information

The WISP shall include the following provisions:

- Designate one or more employees to maintain your information securitiy plan (Data Security Coordinator)
- Identify & assess foreseeable internal & external risks to security
- A method to evaluate and improve methods for:
  - ongoing employee training
  - employee compliance with policies and procedures
  - means for detecting & preventing security system failures

Buchanan & Associates

WISP Provisions (cont.)

- Develop security policies for employees relating to storage, access and transportation of personal infomation outside the office
- A disciplinary system for violations of the security program
- Prevent terminated employees from accessing records containing personal information

Buchanan & Associates

WISP Provisions (cont.)

- Develop reasonable restrictions to physical access of records containing personal data i.e locked offices, locked filing cabinets, etc
- Regular monitoring of the information security plan that assess the effectiveness of the plan; adjusting as needed
- Annual review of the plan or when regular business practices change that warrants changes to security protocol
- Documenting any responsive actions from a security breach and mandatory post-incident review

Buchanan & Associates

CAUTIONARY TIP

In the WISP (and any other written company policies), never include provisions you already know you can't comply with, or set operational standards you know your employees won't comply with. Violation of one's own policies is a liability red flag.

Buchanan & Associates

Question – Separate the Information?

- **What if Personal Information is stored in separate files?**
  i.e. Can I keep a name separate from a credit card number or an employee's name separate from a social security number?

  Yes, and DO THIS if it minimizes risk. For example, do you really need to keep the credit card number on the same record as a notation for other employees that an item or service has indeed been paid for?

  How you systematically deal with personal information must be outlined in your mandatory Written Information Security Program.

Computer System Requirements:

- Secure user authentication protocols
  - control of user IDs
  - secure method of assigning passwords
  - control of security passwords
  - restrict access to active users
  - block access after multiple unsuccessful attempts

Computer System Requirements:

- Secure access control measures that:
  - restrict access to necessary personnel only
  - unique IDs and passwords for each person with access
- Encryption of all transmitted records and files containing personal information that will travel across public networks and encryption of all data containing personal information to be transmitted wirelessly.
- Monitoring of systems for unauthorized use of or access to personal information

Computer System Requirements:

- Encryption of all personal information on laptops or other portable devices
- Firewalls on any computer the contains personal information and is connected to the internet
- Up to date versions of system security agent software i.e. virus, malware, spyware
- Education and training of employees on the proper use of the computer security system and importance of personal information security

Question – Employee Training?

- **How much employee training do I need to do?**

  There is no basic standard yet 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. This (especially) includes transient or seasonal employees.

What would make you comfortable if it was your personal information?

So, what's a 3rd Party Service Provider?

- A service provider is "any person that receives, stores, maintains, processes or otherwise is permitted access to personal information through its provision of services directly to a person that is subject to this regulation"
- E.g. PayPal, Iron Mountain, your local copy shop or data backup provider.

Third Party Vendor Requirements

- Oversight of service providers by:
  - Selecting third-party service providers that are capable of maintaining appropriate security measures that meet state and federal regulations
  - New contracts after March 1, 2010 must require third-party service providers to meet Massachusetts regulations for security measures for personal information
  - Existing contracts must meet the regulations by March 1, 2012

Estimating Your Security Needs

- Do you retain personal information of clients?
  - Do you really need to?
- Electronic or paper records, what type of info?
  - Who has access to these?
  - How and where are they stored?
  - Is access monitored?
  - How long do you retain these records?
  - Do you use a third party contractor who has access?

Estimating Your Security Needs (cont.)

- Technically feasible = reasonable means through technology to accomplish required result
- How are computers used at your facility
  - Do they store personal information?
  - Are they connected to the internet?
  - Who can access these computers?
  - Are they portable and can be lost or stolen? i.e. laptops and handhelds
- What security measures are already in place
  - Sufficient to meet the new standards?

Question – One Size Fits All? No!

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

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. CAUTION: Civil liability and bad publicity over any breach is reason to be over cautious, even if governmental fines wouldn't issue.

Security Breach Reporting

- If you know of a security breach or have reason to believe personal information of a Massachusetts resident was acquired or used by an unauthorized person for an unauthorized use

YOU SHOULD REPORT TO THE ATTORNEY GENERAL'S OFFICE AND THE GOVERNOR'S OFFICE OF CONSUMER AFFAIRS – See M.G.L. Ch. 93H: Section 3

Security Breach Reporting

- Access to unencrypted personal information *or* encrypted data along with the security key
- WARNING: Unauthorized access to personal information is both a violation of the new regulations AND a violation of violation of consumer protection statutes, so civil liability may ensue
- "No Harm Done" is irrelevant in the event of a breach of unencrypted personal information. Reporting is still required.

What Your Report Must Include:

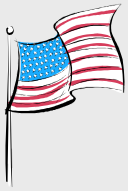
- A detailed description of the nature and circumstance of the breach
- The Number of Massachusetts residents affected
- The steps taken relative to the incident
- Any steps intended to be taken relative to the incident subsequent to notification
- Information regarding whether law enforcement is engaged in investigating the incident

Enforcement & Penalties

- It is unclear exactly how the State will proceed with enforcement actions with this evolving area of law. The Governor's Office of Consumer Affairs and the Attorney General's Office are "in discussions" at this time.
- According to the statute, the Attorney General may bring an action to remedy violations of this chapter and for other relief that may be appropriate. The statute is silent regarding fines.
- While small businesses or non-profits are unlikely to be the first targets, regulators can't help but look into the matter when breaches occur or a violation comes to their attention.

Civil Liability

This is America. Civil litigation may be your greatest exposure, not governmental liability



CHECK YOUR INSURANCE

- CHECK YOUR POLICIES – BE SURE YOU'RE COVERED FOR DATA SECURITY BREACHES, INCLUDING IF CRIMINAL ACTS ARE INVOLVED
- CHECK FOR COVERAGE FOR LEGAL DEFENSE COSTS AS WELL AS LIABILITY INSURANCE, AGAIN INCLUDING FOR CRIMINAL ACTS

Additional Information

- The Office of Consumer Affairs and Business Regulation "Identity Theft" website: www.mass.gov/ocabr
- Buchanan & Associates: www.buchananassociates.com (electronic copies of materials will be posted on this website)