



MASSACHUSETTS DATA SECURITY REQUIREMENTS

Mark J. Ventola
Sheehan Phinney Bass + Green, PA
255 State Street, 5th Floor
Boston, MA 02109
617-897-5600
mventola@sheehan.com

Joel Buckman
President/CEO
YourTechnologySolutions, Inc.
10 Congress St., #1
Stoneham, MA 02180
781-929-0124
joel.yts@comcast.net



MASSACHUSETTS DATA SECURITY LAW

- Protecting Personal Information
 - Chapter 93H
 - Security Breaches – personal information
 - Notice/reporting of breach
 - Regulations to safeguard personal information for Massachusetts residents
 - Department of Consumer Affairs & Business Regulation
 - **March 1, 2010 Deadline**
 - Chapter 93I
 - Standards for disposing of personal information



MASSACHUSETTS DATA SECURITY LAW

- Regulations – the current news.
 - Designated to provide minimum standards to safeguard personal information
- Who is covered?
 - All individuals, for and not for profits, businesses, sole proprietors who maintain or store personal information about a Massachusetts resident



PI PROTECTIONS

- Identify and Assess risks to security of PI
- Develop and Adopt Protections
- Prevent Data Breaches
- Verify protection by 3rd Party Providers
- Report Data Breaches



MASSACHUSETTS DATA SECURITY LAW

- What is “Personal Information”?
 - Combination of first name (or first initial) and last name with one or more of:
 - social security #
 - drivers license #
 - state ID Card #
 - credit card #
 - debit card #
 - financial account #
 - If you have PI, you must adopt a WISP – Written Information Security Program
 - **Personnel Files?**



MASSACHUSETTS DATA SECURITY LAW

- Written Information Security Program
 - Must contain administrative, technical and physical safeguards that are appropriate to:
 - the size, scope and type of business
 - the resources of the business
 - the amount of data involved
 - the need for security and confidentiality of consumer and employee information
 - A “risk-based”, balancing approach



MASSACHUSETTS DATA SECURITY LAW

- Written Information Security Program
 - designating an employee to maintain the program
 - identifying and assessing risks to security of electronic, paper and other records
 - developing policies for employees to protect PI
 - discipline for violations
 - preventing former employees from accessing PI



MASSACHUSETTS DATA SECURITY LAW

- Written Information Security Program
 - verifying protection by outside service providers - **contracts with 3rd parties**
 - reasonable physical restrictions (hard files, passwords)
 - regular monitoring, review annually
 - report data breaches and document actions



MASSACHUSETTS DATA SECURITY LAW

- Computer System Security Requirements
 - If you electronically store or transmit PI, the WISP must include a security system covering computers, including wireless systems



MASSACHUSETTS DATA SECURITY LAW

- Computer System Security Requirements
 - Must include the following elements, **to the extent technically feasible**:
 - (1) Secure user authentication
 - control of user ID
 - secure methods to assign and select passwords
 - protect passwords
 - restrict access to active users and active accounts
 - block access after numerous unsuccessful attempts



MASSACHUSETTS DATA SECURITY LAW

- Computer System Security Requirements
 - (2) Secure access control measures
 - restrict access to PI to those with a need
 - assign unique passwords
 - (3) Encryption
 - of data and files traveling across public networks
 - of PI on laptops and other portable devices
 - (4) Monitoring of systems for unauthorized use



MASSACHUSETTS DATA SECURITY LAW

- Computer System Security Requirements
 - (5) If connected to internet, must have reasonably up-to-date firewall protection and operating systems security patches
 - (6) Must have reasonably up-to-date system security software, with malware protection, with virus protection and regular updates
 - (7) Training – proper use and importance of PI



DATA BREACHES

- Trigger -> Known or reason to know of a “breach of security” that PI was used by an unauthorized person or for an unauthorized purpose
- Breach of security = unauthorized acquisition or use of unencrypted data or encrypted data with key capable of compromising the security which creates a substantial risk of identity theft or fraud against a Mass. resident.



WHO TO NOTIFY AND WHEN

- As soon as practicable and without unreasonable delay

Notify:

- 1) Attorney General;
- 2) Dir. Of Consumer Affairs and Business Regulation;
- 3) Affected Mass. Resident(s)



THANK YOU

Mark J. Ventola
Sheehan Phinney Bass + Green, PA
255 State Street, 5th Floor
Boston, MA 02109
617-897-5600
mventola@sheehan.com

Joel Buckman
President/CEO
YourTechnologySolutions, Inc.
10 Congress St., #1
Stoneham, MA 02180
781-929-0124
joel.yts@comcast.net