



The Massachusetts Data Security Law and Regulations

Developments and Challenges

Rachel E. Muñoz
June 8, 2010

The Law

- “The Regulations” – 201 CMR 17.00
 - Standards for the Protection of Personal Information of Residents of the Commonwealth
 - Finalized November 4, 2009
 - Took effect March 1, 2010
- Chapter 93H of Massachusetts General Laws
 - Addresses Security Breaches
 - October 2007
- Chapter 93I of Massachusetts General Laws
 - Addresses disposal of personal information
 - February 2008

Why?

- TJX breach
- Reported data security breaches
 - Office of Consumer Affairs and Business Regulation (“OCABR”) 2009 Report
 - Breaches involving electronic information (criminal acts – e.g. hackers)
 - Breaches involving human error (e.g. poor employee handling)



Compliance

- No regulatory guidance – yet
- OCABR
 - Regulations apply to personal information stored out of state
 - Encrypt, encrypt, encrypt



Chapter 93H – Security Breaches

- Reporting and notification for (1) breach of security of (2) personal information
- (1) “Breach of Security”
 - Defined as unauthorized acquisition or use of unencrypted data or unauthorized acquisition or use of encrypted data along with the key used to decipher the encrypted data
 - Must create a “substantial risk of identity theft or fraud” against a Massachusetts resident
 - Examples
 - Loss of laptop with personal information
 - Hacking
 - Terminated employees stealing information



Chapter 93H – Personal Information

- (2) “Personal Information”
 - Last name and first name or last name and first initial
 - **AND** one of the following:
 - Social Security Number
 - Driver’s license number or state-issued ID number
 - Financial account information (including debit/credit card number)



Chapter 93H – When to Provide Notice

- Notice “as soon as practicable and without unreasonable delay” after you “know[] or [have] reason to know” of a 1) possible breach or 2) that an “authorized person” has acquired or used personal information for an “unauthorized purpose”
- Exception for pending criminal investigation



Chapter 93H – Where to Provide Notice

- If you own or license personal information (custody and control)
 - Individual notification
 - To the Attorney General and the OCABR
 - Different information in notice to individual vs. government



Chapter 93H – Where to Provide Notice

- If you maintain or store personal information (e.g. swipe credit cards, but otherwise lack custody and control)
 - “Cooperate with” owner or licensor of the data



Chapter 93H – Acceptable forms of notice

- Written
- Electronic
- “Substitute Notice” (instead of individual notification)
 - Permissible if:
 - Cost is more than \$250,000;
 - More than 500,000 affected residents; or
 - Cannot contact affected individuals



Chapter 93I – Disposal of Records

- Requires all companies disposing of personal information of Massachusetts residents to destroy records “so that personal information cannot be practicably read or reconstructed.”
 - Personal information includes name and one of four other pieces of information
 - New 4th piece is “biometric indicator” (e.g. fingerprint)
- Paper records must be redacted, burned, pulverized or shredded
- Electronic records must be destroyed or erased permanently
- Companies may outsource to third party



The Regulations

- Rule #1: Don't Shoot the Messenger



The Regulations

- 201 CMR 17.00
- Took effect March 1, 2010
- Applies to anyone and everything that owns, licenses, receives, stores, maintains, processes or otherwise has access to personal information
 - Location of business is irrelevant
- Personal Information
 - Name and (1) SSN; (2) Driver's license number or state-issued identification number; or (3) financial account number



Comprehensive Information Security Program (“CISP”)

- Mandatory
- Must be written
- Addresses administrative, technical, and physical safeguards
- Designed to ensure security and confidentiality of records with personal information
- Minimum requirements
- Appropriate to your business



Elements of CISP

- Must assess paper, electronic, and other records with personal information
- Must develop security policies
- Must designate person(s) in charge



Elements of CISP

- Must monitor and maintain program and update annually or when business practices change
- Must have protocol for and document actions taken in response to a security breach
- Must conduct trainings on policy



Elements of CISP

- Must limit the amount of PI collected, time retained, and access to PI to what is “reasonably necessary” to accomplish a legitimate purpose
- Must restrict access to records (and document who has access)
- Must discipline employees who violate the program
- Must prevent access by terminated employees



Elements of CISP

- Must take “reasonable steps” to select and retain third parties who can meet the regulatory requirements
 - Verify third party can comply
 - Reference compliance in contract (3/1/12)
 - Consider adding a “hold harmless” provision



Computer System Security Requirements (“CSSR”)

- Included in the CISP must be Computer System Security Requirements
- Applies to all computers and any wireless systems
- Minimum requirements
- To the “extent technically feasible”



Elements of CSSR

- Secure user authentication protocols
- Limit access to PI to those who need to know/use it to perform their job(s)
 - User IDs; passwords
 - E.g., automatic lock out for multiple failed log on attempts
- Encryption of all transmitted records containing PI
 - All data that travels over public networks
 - All wireless transmissions
- Encryption of all laptops and other portable devices



Elements of CSSR

- Monitor system for unauthorized use
- Up-to-date software protection, including firewalls and virus protection
- Education and training of employees on the proper use of the security system and importance of security of PI



Other Elements of CISP & CSSR

- Physical safeguards
 - Physically protect personal information stored in paper records
 - Physically protect personal information in electronic format on computers, servers
 - Control of visitors



Compliance and Penalties

- AG enforces 93H and 93I
 - Chapter 93H – civil penalties of up to \$5,000 for each violation; legal costs
 - Chapter 93I – fines up to \$100 per data subject, up to maximum of \$50,000
- Compliance with the regulations will be reviewed on a case-by-case basis
 - Will consider size, scope, and type of business
 - Will consider need for security and confidentiality of consumer and employee information



Challenges to Compliance

- Cost
- Proactive implementation
- Ambiguity in Law and Regulations
- To encrypt or not encrypt – applying the regulations to your business and practices



Enforcement

- Good news
 - Compliance audits not likely
 - Attorney General's office not likely pursue enforcement actions for failure to comply with reporting guidelines
- Cooperate fully and quickly



The End

Rachel E. Muñoz
June 8, 2010