ITPMG

Responding to Data Privacy Regulations

Preparing for Recent State Laws

Mike Corby

June 2009

Agenda

- Background
- Definitions and Scope
- Key Elements of the new Regulations
- Twelve General Privacy Provisions
- Eight Electronic Data Privacy Provisions
- Breach Reporting and Enforcement
- What You Need to Do Next

Statistics

- Dell Ponemon Institute Study:
  - Up to 12,000 laptops are lost in United States airports each week
  - Between 65 and 70 percent of lost laptops are never reclaimed
  - Most laptops are lost at security checkpoints
  - 53 percent of business travelers surveyed carry sensitive corporate information on their laptop
  - 65 percent of those who carry confidential information have not taken steps to protect it while traveling
  - 42 percent of respondents say they do not back up their data
- 75% of all data privacy breaches involve unencrypted data
  - In Massachusetts alone, over 750,000 resident data items have been compromised
  - 60% of the data items compromised will be used against the residents

The Massachusetts Law

- M.G.L. c.93 H
  - Signed into Law August 4, 2007
  - Requires actions to be taken to protect personal information
  - Requires notification of breaches
  - Mandates that regulations governing how to comply be promulgated
- Reg. 201 CMR 17.00
  - Promulgated September 2008
  - Sponsored by Office of Consumer Affairs and Business regulations (OCABR)
  - Originally effective January 1, 2009, postponed to May 1, 2009 and finally January 1, 2010

Common Purpose of New Data Security Regulations

- Implement the privacy provisions of state law
- Establish minimum standards for safeguarding personal information contained both in paper and electronic records
- Ensure the security and confidentiality in a manner consistent with industry standards
- Protect against anticipated threats or hazards to the security or integrity of such information
- Protect against unauthorized access to or use of personal information that creates a substantial risk of identity theft or fraud against residents.

Definitions in state laws

- "Person" is
  - Natural Person
  - Corporation
  - Association
  - Partnership
  - Other Legal Entity

  Particularly employees, customers, bank customers, investors, credit card customers
- **Does not apply** to any Government Agency

- "Personal Information"
  - First Name and Last name or First Initial and Last Name
  - Associated with:
    - Social Security Number
    - Driver's License Number
    - State-issued Identification Number
    - Financial Account Number
    - Credit Card Number with or without Access Code
  - Excluding – Data Available in Public Records

Definitions in state laws

- "Breach of Security" covers Acts and Targets
  - The Acts:
    - Unauthorized acquisition or
    - Unauthorized use
  - The Targets:
    - Unencrypted data or encrypted electronic data
    - Paper documents containing private information
- "Electronic" includes
  - Electrical Impulse
  - Wireless transmitted
  - Digital
  - Magnetic
  - Optical
  - Electromagnetic
- "Encryption"

  Transformation of data by use of a mathematical process, or an alternative method that renders the information unreadable without a special code to re-translates the information into its original form

Scope of Data Privacy Laws

- Applies to "persons" that
  - Own
  - License
  - Store or maintain
  - "Personal Information" about a resident
- Applies to non-governmental entities
  - For Profit (businesses, corporations, etc.)
  - Not-for-profit (charities, churches, elderly centers, etc.)
  - Other legal entity (excluding government)
- Form of Information
  - Paper documents
  - Electronic Records
  - Any other storage methods
    - Magnetic
    - Optical
    - Electronic Devices (phones, PDA's, iPods, etc.)

What is different about the Massachusetts Law?

- 44 Other states have a privacy law starting with California SB 1386
- MA is a prevention not a notification law
- Designed for resident protection not company behavior, therefore not for MA companies
- Narrow definition of what is PII
- Includes archived data in storage

Watch laws pending in MI & WA
(criminal penalties)

Key Elements of This Regulation

- Duty to Protect
  - Develop and implement a Written information Security Program (WISP) to maintain and monitor all records containing personal information
  - Conduct a Risk Assessment taking into consideration
    - Size scope and type of business
    - Amount of resources available
    - Amount of stored data
    - The need for security and confidentiality
- Activities that Constitute Excessive Risk
  - Data stored in the clear accessible to too many people
  - Employees who are unaware of their responsibilities for data security
  - Former employees who retain access to computer system resources
  - Laptop computers and portable data storage devices that have unencrypted private information

The jury is still out on…

- Third Party Compliance
- Standard of Reasonable-ness
  - In Writing
  - Certification
  - Business Partner's Plans
  - Technology Available
- Other than reporting violations how will the government determine compliance?
  - Periodic Audits
  - "Official" Credentialing
  - Random Samples

Twelve General Privacy Provisions

1. Designate one or more employees to maintain the comprehensive information security program.
2. Minimize risks to the confidentiality, integrity and availability of an personal information whether stored or recorded electronically or on paper.
3. Create security policies to determine whether and how employees should be allowed to keep, access and transport records containing personal information off business premises.
4. Imposes disciplinary measures for violations of the comprehensive information security program rules.
5. Prevent terminated employees from accessing records containing personal information.

Twelve General Privacy Provisions

6. Third Party Service Providers must maintain appropriate protection measures.
7. Limited physical access to personal information to that required to accomplish the necessary task.
8. Create a method of identifying records and devices used to store personal information.
9. Require written approval prior to being given physical access to any protected personal information.
10. Regularly monitor and review all aspects of the comprehensive security program.
11. Annually review the information security program.
12. Document actions taken in response to a breach of security.

Eight Electronic Data Privacy Provisions

1. Secure user authentication process.
2. Secure access control measures.
3. Encrypt records transmitted over networks both wired and wirelessly.
4. Monitor the system.
5. All laptops and storage devices must have private data encrypted.
6. All systems must contain firewalls and have up-to-date operating system security patches applied according to industry standards.
7. Activated and up-to-date anti-virus and anti-spam applications.
8. Employees should be trained to recognize the presence of potential security problems and a clear procedure to notify the appropriate support people.

Breach Reporting

- Breach of Personal Information
  - What constitutes a Breach?
  - Acquiring vs. actually using
- Do you own the Information?
- Notification
  - Notify the Government
  - Notify the Individual - Must Include
    - How to request a freeze
    - What information is needed
    - Cost of the security freeze

Enforcement in Massachusetts (and elsewhere)

- Prior laws encouraged reporting over prevention.
- Failure to comply
  - Lawsuit by the Attorney General
- Violations
  - $5,000 per violation
    - Per person?
    - Per event?
  - $50,000 fine for failure to dispose of PII properly
- NV Law allows companies in compliance to enjoy a $1,000 maximum per person liability

Summary

- You are Responsible
  - Develop an enterprise data protection policy
  - Appoint someone to take the lead
  - Recognize what is covered by
    - HIPAA
    - GLBA
    - Fair Trade Credit Transaction Act - 2003 (Red Flag Rule)
    - Patriot Act
    - Other Federal Laws
    - Credit Card Processor
- Special Precautions
  - Laptop computers
  - Remote Access
  - International Travel
  - Documentation Volume
  - Former Employees

Three Phase Action Plan

Phase I - Assessment

- Designate a Coordinator
  - Define job and establish responsibility/authority
- Issue a W.I.S.P.
- Inventory protected data (in use, at rest, in motion)
  - Company versus personal protected data
  - On-site, off-site, processed by third party
  - Paper and electronic (location, protection, retention, destruction)
- Review data security policies
  - General business practices
  - Employee behavior policies
- "Turn on" data encryption and protection in standard software
- Create Employee Training Plan

Three Phase Action Plan

Phase II –Technology and Exercises

- Direct the Coordinator to assemble a team
  - Large organizations – representatives from HR, Finance, IS, Legal
  - Small organizations – “reasonable” representation
  - Reduce the “Attack Surface” – places where PII is vulnerable
- Develop a plan to review and exercise the incident response plan
  - Review and respond the significant risks indicated during Phase I
  - Develop detailed procedures to respond to the most likely events
  - Create a library of documents to be used during possible compliance audit
- Obtain technology required to facilitate data protection
  - Laptop disk encryption
  - Remote access Virtual Private Network
  - “Tokenization” to translate PII (ssn, credit card # etc.) to neutral data
- Establish budget for resolving any outstanding issues
- Designate a technology representative to monitor data protection advancements

Three Phase Action Plan

Phase III –Develop an Incident Management Plan

- Review firewall technology & consider advanced incident handling
  - Consider outsourced response and/or forensics teams
- Regularly test and improve employee awareness and response
  - Build data protection expectations into performance plans
  - Create skills development plan, succession plan, certification guidelines
- Pursue independent certification
  - Coordinate with credit card PCI standards
  - Integrate industry specific plans
  - Establish a team to conduct third party certification exercises
- Integrate data protection into marketing and public image

To receive additional materials on
Responding to Data Privacy Regulations**,**
contact ITPMG at:

by email:
information@itpmg.com

or phone:
+1 843.377.8228