MA201 CMR 17.00

John Hally
January 2012
GIAC GSEC, GCIA, GCIH, GCFA, GCWN, GPEN

17.01 - Purpose and Scope

- Effective Date: March 2010
- Purpose
  - Implementation of provisions set forth in Massachusetts General Law (MGL) 93H
  - Establish minimum standard to safeguard personal information contained in paper and electronic records
  - Ensure security and confidentiality of information consistent with industry standards
- Scope
    - Applies to any and all persons that own or license personal information of a Massachusettes resident

17.02 - Key Definitions

- Personal Information: Resident's first name/initial and last name in combination with:
    - Social Security Number.
    - Driver's License/State Identification Number.
    - Financial account/Credit card number with or without PIN/Security/Access Code.
- Record: Any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics.
- Owner/licenser: Receives, maintains, processes, or otherwise has access to personal information in connection with the provision of goods or services or in connection with employment.

17.04 - Computer System Security Requirements

- Secure User Authentication Protocols.
- Secure Access Control Measures.
- Encryption of all transmitted records/files containing Personal Information.
- "Reasonable" monitoring of systems.
- Encryption of all stored personal information on laptops/portable devices.
- "Reasonably up to date" firewall protection, security patches for any Internet-connected system that stores/transmits personal data.
- "Reasonably up to date" system security anti-malware agent software.
- Education/training of employees on proper use and security of personal data.

Massachusetts Data Privacy Law Summary

- MA 201 CMR 17.00 Requires:
  - Any and all personal information as outlined in the law be protected
  - The owner of the data is ultimately responsible for the security of personal information and meeting compliance.
  - 17.03 Duty to Protect sets the requirement of having a comprehensive, written security program containing administrative, technical, and physical safeguards
  - 17.04 Computer System Security Requirements addresses system security by requiring the implementation of 8 technical controls for any system that stores or transmits personal data
  - The lastest revision of the law allows for a risk-based approach to compliance and enforcement efforts.
  - Law in effect as of March 2010.