



201 CMR 17.00: Standards for The Protection of Personal Information of Residents of the Commonwealth

[17.01: Purpose and Scope](#)

[17.02: Definitions](#)

[17.03: Duty to Protect and Standards for Protecting Personal Information](#)

[17.04: Computer System Security Requirements](#)

17.01 **Purpose and Scope**

(a) Purpose

This regulation implements the provisions of M.G.L. c. 93H relative to the standards to be met by persons who own, license, store or maintain personal information about a resident of the Commonwealth of Massachusetts. This regulation establishes minimum standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records. Further purposes are to (i) ensure the security and confidentiality of such information in a manner consistent with industry standards, (ii) protect against anticipated threats or hazards to the security or integrity of such information, and (iii) protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft or fraud against such residents.

(b) Scope

The provisions of this regulation apply to all persons that own, license, store or maintain personal information about a resident of the Commonwealth.

17.02: **Definitions**

The following words as used herein shall, unless the context requires otherwise, have the following meanings:

"Breach of security", the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth. A good faith but unauthorized acquisition of personal information by a person or agency, or employee or agent thereof, for the lawful purposes of such person or agency, is not a breach of security unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure.

"Electronic," relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities.

"Encrypted," transformation of data through the use of a 128-bit or higher algorithmic process, or other means or process approved by the office of consumer affairs and business regulation that is at least as secure as such algorithmic process, into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

"Person," a natural person, corporation, association, partnership or other legal entity, other than an agency, executive office, department, board, commission, bureau, division or authority of the Commonwealth, or any of its branches, or any political subdivision thereof.

"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 data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

"Record" or "Records," any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics.

17.03: **Duty to Protect and Standards for Protecting Personal Information**

Every person that owns, licenses, stores or maintains personal information about a resident of the Commonwealth shall develop, implement, maintain and monitor a comprehensive, written information security program applicable to any records containing such personal information. Such comprehensive information security program shall be reasonably consistent with industry standards, and shall contain administrative, technical, and physical safeguards to ensure the security and confidentiality of such records. Moreover, the safeguards contained in such program must be consistent with the safeguards for protection of personal information and information of a similar character set forth in any state or federal regulations by which the person who owns, licenses, stores or maintains such information may be regulated.

Whether the comprehensive information security program is in compliance with these regulations for the protection of personal information, shall be evaluated taking into account (i) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program, (ii) the amount of resources available to such person, (iii) the amount of stored data, and (iv) the need for security and confidentiality of both consumer and employee information. Without limiting the generality of the foregoing, every comprehensive information security program shall include, but shall not be limited to:

- (a) Designating one or more employees to design, implement and coordinate the maintenance of the comprehensive information security program;
- (b) Identifying and assessing internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information in each relevant area of the person's operation, and evaluating and improving, where necessary, the effectiveness of the current safeguards for minimizing such risks, including but not limited to: (i) ongoing employee (including temporary and contract employee) training; (ii) monitoring employee compliance with policies and procedures; (iii) upgrading information systems, including network, system and software design, as well as information processing, storage, and transmission, as necessary; (iv) storage of records and data in locked facilities, storage areas or containers; and (v) improving, as necessary, means for detecting, preventing and responding to security, including but not limited to security systems, failures.
- (c) Developing security policies for employees who telecommute that take into account whether and how such employees should be allowed to keep, access and transport data containing personal information.
- (d) Imposing disciplinary measures for violations of the comprehensive information security program rules.

- (e) Preventing terminated employees from accessing records containing personal information by immediately terminating their physical and electronic access to such records, including deactivating their passwords and user names.
- (f) Taking reasonable steps to verify that third-party service providers with access to personal information have the capacity to protect such personal information, including (i) selecting and retaining service providers that are capable of maintaining safeguards for personal information; and (ii) contractually requiring service providers to maintain such safeguards. Prior to permitting third-party service providers access to personal information, the person permitting such access shall obtain from the third-party service provider a written certification that such service provider has a written, comprehensive information security program that is in compliance with the provisions of these regulations.
- (g) Collecting the minimum amount of personal information necessary to accomplish the legitimate purpose for which it was collected; retaining such information for the minimum time necessary to accomplish such purpose; and permitting access to the smallest number of persons who are reasonably required to know such information in order to accomplish such purpose.
- (h) Inventorying paper, electronic and other records, computing systems, and storage media, including laptops and portable devices used to store personal information, to identify those records containing personal information.
- (i) Regularly monitoring and auditing employee access to personal information in order to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information.
- (j) Reviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information.
- (k) Documenting responsive actions taken in connection with any incident involving a breach of security or the potential therefor, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

17.04: **Computer System Security Requirements**

Every person that owns, licenses, stores or maintains personal information about a resident of the Commonwealth and electronically stores or transmits such information shall include in its written, comprehensive information security program the establishment and maintenance of a security system covering its computers, including any wireless system, that, at a minimum, shall have the following elements:

- (1) Secure user authentication protocols including:
 - (i) control of user IDs and other identifiers;
 - (ii) a secure method of assigning and selecting passwords consisting of at least seven letters and numbers;
 - (iii) control of data security passwords to ensure that such passwords are kept at a location separate from that of the data to which such passwords permit access;
 - (iv) restricting access to active users and active user accounts only; and
 - (v) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;
- (2) Secure access control measures that:

- (i) restrict access to records and files containing personal information to those who need such information to perform their job duties; and
- (ii) assign a unique identification plus a password, which is not vendor supplied, to each person with computer access;
- (3) Encryption of all transmitted records and files containing personal information, including those in wireless environments, that will travel across public networks.
- (4) Periodic monitoring of networks and systems, for unauthorized use of or access to personal information, and recording the audit trails for users, events, dates, times and success or failure of login;
- (5) Periodic review of audit trails restricted to those with job-related need to view audit trails;
- (6) For files containing personal information on a system that is connected to the Internet, there must be firewall protection with up-to-date patches, including operating system security patches. A firewall must, at a minimum, protect devices containing personal information from access by or connections from unauthorized users.
- (7) The most current version of system security agent software which must include antispysware and antivirus software, including up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and which includes security software that is set to receive the most current security updates on a regular basis.
- (8) Education and training of employees on the proper use of the computer security system and the importance of personal information security.
- (9) Restricted physical access to computerized records containing personal information, including a written procedure that sets forth the manner in which physical access to personal information is restricted. When notified of any unauthorized entry into a secure area by either an employee or any other unauthorized person, the integrity of the computerized records must be reviewed.

REGULATORY AUTHORITY:

201 CMR 17.00: M.G.L. c. 93H