



Mass Law 201 CMR 17.00 Standards for The Protection of Personal Information of Residents of the Commonwealth of Massachusetts

Massachusetts law 201 CMR 17 will go into effect in March 2010. Compliance is mandatory for ALL corporations housing Massachusetts resident's personal data.

The law requires that businesses inventory all PII (personal individual information) records throughout the corporation, use secure authentication protocols, block and restrict access to records and files, and ensure ALL computer assets include most current version of system security software, patches and agents.

201 CMR 17.00: STANDARDS FOR THE PROTECTION OF PERSONAL INFORMATION OF RESIDENTS OF THE COMMONWEALTH
Section
17.01: Purpose and Scope
17.02: Definitions
17.03: **Duty to Protect and Standards for Protecting Personal Information**

...every comprehensive information security program shall include, but shall not be limited to:

(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.

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.

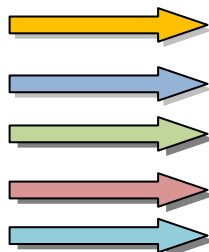
(7) **The most current version of system security agent software**

which must include antispayware 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.

Compliance Requirement

- 17.03(h)
- 17.04(1)
- 17.04(1)(v)
- 17.04(2)(i)
- 17.04(7h)

- PII Discovery
- Web App Security
- Database Security
- Data Control/PCI
- Agent / Patching



-
-
-
-
-

Solutions

- [StoredIQ](#)
- [Breach](#)
- [Secerno](#)
- [Varonis](#)
- [BigFix](#)



NuTech and our **partners** can guide you through the compliance and provide the expertise to **Comply with 201 CMR 17.00.**