

Massachusetts 201 CMR 17.00

Massachusetts 201 CMR 17.00 requires organizations to implement administrative, technical, and physical safeguards to protect residents' personal information.



What it is

U.S. Massachusetts 201 CMR 17.00 — Standards for the Protection of Personal Information is a state regulation that requires organizations to safeguard personal information of Massachusetts residents by implementing comprehensive data protection and cybersecurity measures. Its primary purpose is to reduce the risk of unauthorized access to, or disclosure of, personal information and to strengthen consumer privacy.

Issued and enforced by the Massachusetts Office of Consumer Affairs and Business Regulation (OCABR), 201 CMR 17.00 applies to any entity, regardless of location, that owns, licenses, stores, or maintains personal information about Massachusetts residents. The regulation mandates administrative, technical, and physical safeguards, covering areas such as risk assessment, access controls, encryption, incident response procedures, and ongoing workforce training.

At a glance

PUBLISHER Commonwealth of Massachusetts, Office of Consumer Affairs and Business Regulation	TYPE Regulation	VERSION 2010
EFFECTIVE March 1, 2010	DOMAIN Privacy	FAMILY Global Privacy Regulations
REGION Massachusetts	ADOPTION MODEL Regulatory Compliance	IMPLEMENTATION COMPLEXITY Moderate

Source: <https://www.mass.gov/regulations/201-CMR-1700-standards-for-the-protection-of-personal-information-of-ma-residents>

Why it matters

- **Strengthen data protection practices** Ensure consistent, organization-wide measures to prevent unauthorized access and disclosure of sensitive personal information.
- **Enhance regulatory alignment** Demonstrate compliance with state mandates, reducing legal risk and increasing organizational accountability for personal data handling.
- **Improve incident response readiness** Support the implementation of proactive processes to detect, report, and respond effectively to breaches or potential data compromise.
- **Increase audit preparedness** Facilitate easier documentation and verification of security controls, simplifying audit processes and regulatory inspections.

How SmartSuite supports MA 201 CMR 17

Personal Information Safeguards Library

Structure safeguards for protecting personal information, including encryption, access control, and secure data handling practices.

Illinois PIPA Data Inventory and Classification

Track personal data types, storage locations, and systems subject to Illinois PIPA requirements.

Risk Assessment and Safeguard Implementation

Manage risk assessments and track implementation of administrative, technical, and physical safeguards.

Access and Personal Information Management

Manage user access, permissions, and secure handling of personal information across systems.

Breach Detection and Notification Workflows

Track security incidents and manage notification timelines, communications, and regulatory obligations.

Illinois Personal Information Protection Compliance Reporting

Provide dashboards showing data protection posture, breach readiness, and compliance with Illinois personal information protection requirements.

Common framework mappings

CIS Controls v8.1

COBIT 2019

GDPR

ISO 27001:2022

ISO 27701

NIST CSF 2.0

NIST 800-53 Rev.5

PCI DSS 4.0.1

SOC 2

HIPAA

Official resources

Massachusetts 201 CMR 17.00 Regulation

Describes requirements for the protection of personal information in Massachusetts.

mass.gov/doc/201-cmr-1700-standards-for-the-protection-of-personal-information-of-residents-of-the-commonwealth

Massachusetts Data Protection Regulation Compliance Guidance

Provides guidance on complying with the Massachusetts data protection standards.

mass.gov/guides/compliance-with-201-cmr-1700-standards-for-the-protection-of-personal-information

Massachusetts Office of Consumer Affairs and Business Regulation

Offers resources and updates related to personal data protection laws.

mass.gov/orgs/office-of-consumer-affairs-and-business-regulation

Massachusetts General Law Chapter 93H

Defines regulations concerning data breaches and personal information security.

malegislature.gov/Laws/GeneralLaws/PartI/TitleXV/Chapter93H

Frequently asked questions

What is 201 CMR 17.00 used for?

201 CMR 17.00 establishes minimum standards to protect personal information of Massachusetts residents. Its primary purpose is to safeguard data against unauthorized access or use, especially in electronic and paper records held by businesses.

Is compliance with 201 CMR 17.00 mandatory?

Yes, compliance is mandatory for all businesses and organizations that own or license personal information about Massachusetts residents. Non-compliance can lead to regulatory enforcement actions and potential penalties.

Who does 201 CMR 17.00 apply to?

201 CMR 17.00 applies to any entity, regardless of location, that stores, processes, or transmits personal information of Massachusetts residents. This includes both for-profit and non-profit organizations.

What are the key requirements of 201 CMR 17.00?

Key requirements include implementing a comprehensive written information security program (WISP), encryption of personal information transmitted over public networks, strong access control measures, regular monitoring, and employee training on data protection.

How should organizations implement 201 CMR 17.00 controls?

Organizations should conduct risk assessments to identify vulnerabilities in how they handle personal information, develop and maintain a WISP, deploy technical controls like encryption and secure authentication, and establish administrative safeguards including user training and incident response procedures.

How does 201 CMR 17.00 relate to other data privacy laws?

201 CMR 17.00 complements broader federal and state data security regulations by focusing specifically on the personal information of Massachusetts residents. While similar in intent to laws like GLBA or HIPAA, it imposes distinct, local obligations.

What ongoing actions are necessary to maintain 201 CMR 17.00 compliance?

Maintaining compliance requires periodic review and updating of the WISP, continued employee awareness training, conducting regular audits of technical and organizational safeguards, and monitoring for emerging threats to personal data.

How would SmartSuite support U.S. Massachusetts 201 CMR 17.00?

SmartSuite can help organizations manage 201 CMR 17.00 by supporting risk tracking, control management, and evidence collection for security practices. It enables documentation and monitoring of policies, streamlines audit preparation, and provides reporting tools to demonstrate ongoing compliance with state requirements.

License included / downloadable: Yes Massachusetts 201 CMR 17.00 is publicly available free from Mass.gov and official state publications.
License included with platform

Full framework page and mappings: smartsuite.com/frameworks/us-massachusetts-201-cmr-17-00-standards-for-the-protection-of-personal-inform