SmartSuite

Framework / Privacy / Global Privacy Regulations

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

Massachusetts 201 CMR 17.00 requires anyone that owns or licenses a resident's personal information to keep a written information security program with the 17.03 and 17.04 safeguards.



What it is

201 CMR 17.00, Standards for the Protection of Personal Information of Residents of the Commonwealth, is the Massachusetts regulation that requires every person that owns or licenses personal information about a Massachusetts resident to develop, implement and maintain a written comprehensive information security program (WISP) with administrative, technical and physical safeguards; full compliance has been required since March 1, 2010 (201 CMR 17.05). The Office of Consumer Affairs and Business Regulation (OCABR) issued it under M.G.L. c. 93H, section 2(a), and the Attorney General enforces chapter 93H through M.G.L. c. 93A, section 4 (c. 93H, section 6).

At a glance

PUBLISHER
Massachusetts Office of Consumer Affairs and Business Regulation (regulation under M.G.L. c. 93H, enacted by the Massachusetts General Court); enforced by the Attorney General

TYPE
Regulation

VERSION
201 CMR 17.00 (compliance required from March 1, 2010; service-provider contract transition to March 1, 2012)

EFFECTIVE
March 1, 2010

DOMAIN
Privacy

FAMILY
Global Privacy Regulations

REGION
Massachusetts

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
Medium

Source: mass.gov/regulations/201-CMR-1700-standards-for-the-protection-of-personal-information-of-residents-of-the-commonwealth

Why it matters

- **A written program with a named owner** Section 17.03(1) requires a comprehensive information security program written in one or more readily accessible parts, and 17.03(2)(a) requires one or more employees designated to maintain it, so accountability is documented before an incident.
- **Risk-scaled safeguards** The safeguards must be appropriate to the size, scope and type of business, the resources available, the amount of stored data and the need for security and confidentiality of consumer and employee information (17.03(1)(a) to (d)).
- **Named technical controls** Section 17.04 lists secure user authentication, access control, encryption in transit and on portable devices, monitoring, firewalls and patches, malware protection and training, each applied to the extent technically feasible.
- **Service providers under contract** Section 17.03(2)(f) requires reasonable steps to select providers capable of appropriate security measures and a contract that requires them to implement and maintain those measures.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports MA 201 CMR 17

WISP Requirement Library

Load 17.03(2)(a) to (j) and 17.04(1) to (8) as requirements with a designated program owner, implementation status, linked policies and the evidence that shows each is operating.

Risk Assessment Record

Run the 17.03(2)(b) assessment of reasonably foreseeable internal and external risks as a record with the safeguards evaluated, training status and the means for detecting security system failures.

Personal Information Inventory

Track in Privacy Management where resident personal information is received, stored, processed and transmitted, on paper and electronically, including laptops and portable devices subject to 17.04(5).

Service Provider Oversight

Track each provider's selection due diligence and the contract clause required by 17.03(2)(f) in Third Party Risk Management, with review dates and the safeguards the provider has confirmed.

Technical Control Monitoring

Record authentication, access control, encryption, firewall, patch and malware controls in Cyber & IT Risk, with the technical-feasibility rationale 17.04 allows and the monitoring 17.04(4) requires.

Breach Response and Annual Review

Run the 17.03(2)(j) incident record with responsive actions, the c. 93H section 3 notices to the Attorney General, OCABR and residents, the section 3A credit monitoring offer and the post-incident review; schedule the 17.03(2)(i) annual review.

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

Who must comply with 201 CMR 17.00?

Every person that owns or licenses personal information about a resident of the Commonwealth (17.01(2)). Owns or licenses means receiving, storing, maintaining, processing or otherwise having access to personal information in connection with goods, services or employment, so employers, retailers, professional firms and nonprofits are covered wherever they are located (17.02). The definition of Person excludes Commonwealth agencies and political subdivisions, which follow separate rules under M.G.L. c. 93H, section 2(b) and (c).

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

What counts as personal information under 201 CMR 17.02?

A Massachusetts resident's first name and last name, or first initial and last name, in combination with a Social Security number, a driver's license or state-issued identification card number, or a financial account number or credit or debit card number, with or without any security code, access code, PIN or password that would permit access to the account. Information lawfully obtained from publicly available sources or public government records is excluded (17.02).

What must a written information security program (WISP) contain?

Section 17.03(1) requires a comprehensive program, written in one or more readily accessible parts, with administrative, technical and physical safeguards appropriate to the business's size, resources, data volume and need for confidentiality. Section 17.03(2) lists ten elements: designated employees to maintain the program, risk identification and assessment, policies for records taken off premises, disciplinary measures, cutting off terminated employees, service provider selection and contracts, physical access restrictions, regular monitoring, a review at least annually or on a material business change, and documented responsive actions with a post-incident review after any breach.

What computer security controls does 201 CMR 17.04 require?

For anyone that stores or transmits personal information electronically, section 17.04 requires, to the extent technically feasible: secure user authentication protocols with controlled user IDs, secure passwords or unique identifier technologies, protected password storage, access limited to active users and lockout after multiple failed attempts; access controls restricting records to those who need them, with unique IDs and non-default passwords; encryption of personal information sent across public networks or wirelessly; reasonable monitoring for unauthorized access; encryption on laptops and portable devices; up-to-date firewalls and operating system patches; current malware protection; and employee training.

What must a Massachusetts business do after a breach of security?

M.G.L. c. 93H, section 3(b) requires notice to the Attorney General, the Director of Consumer Affairs and Business Regulation and the affected residents as soon as practicable and without unreasonable delay. The regulator notice states the nature of the breach, the number of residents affected, the type of information compromised, whether the business maintains a written information security program and the steps taken; the resident notice explains the right to a police report and a free security freeze but may not describe the nature of the breach. Section 3A adds at least 18 months of free credit monitoring when Social Security numbers are involved, and 17.03(2)(j) requires a documented post-incident review.

License included / downloadable: Yes 201 CMR 17.00 is a Massachusetts state regulation published free on Mass.gov by the Office of Consumer Affairs and Business Regulation, and M.G.L. c. 93H is published free by the General Court; the Legal Information Institute mirrors the regulation text. The platform links to the official text.

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