201 CMR 17.00

Massachusetts WISP Checklist

[Business name] | Completed by [Name] | [Month DD, YYYY]

Before You Start

Massachusetts requires every business that owns or licenses personal information about a Massachusetts resident to have a written information security program, called a WISP (201 CMR 17.03(1)). This checklist walks through what the regulation says the WISP must include, plus the state's disposal and breach notice rules. Each item names the paragraph it comes from.

For each item, mark Yes, Partial or No, and write down where the proof is kept. A Yes with nothing in the evidence column should be treated as a No.

Who it covers	Anyone who owns or licenses personal information about a Massachusetts resident (201 CMR 17.01(2)). That includes data you receive, store or can access to provide goods or services, or as an employer (17.02). Payroll records for Massachusetts employees usually count.
Personal information	A resident's first name or initial and last name, with a Social Security number, a driver's license or state ID number, or a financial account or credit or debit card number (17.02). Paper and electronic records both count.
HIPAA and Regulation S-P	If you follow HIPAA or Regulation S-P, the WISP's safeguards must be consistent with those rules too (17.03(1)). One program can meet 201 CMR 17.00 and those rules.
Rule text	mass.gov/regulations/201-CMR-1700-standards-for-the-protection-of-personal-information-of-residents-of-the-commonwealth

1. The Written Program

Item	Rule	Evidence on file	Result
A written program, in one or more parts that staff can find, covering administrative, technical and physical safeguards for personal information	17.03(1)	[WISP name, version, date]	☐ Yes ☐ Partial ☐ No
The safeguards fit the business: its size, scope and type, its resources, how much data it stores, and the need to protect both customer and employee information	17.03(1)(a)-(d)	[WISP section]	☐ Yes ☐ Partial ☐ No
The safeguards are consistent with any state or federal rules the business also follows, such as HIPAA or Regulation S-P	17.03(1)	[WISP section]	☐ Yes ☐ Partial ☐ No
One or more named employees maintain the program	17.03(2)(a)	[Name, appointment memo]	☐ Yes ☐ Partial ☐ No
A current list of the paper records, systems, laptops, phones and storage media that hold personal information	Supports 17.03(2)(b)	[Inventory, date]	☐ Yes ☐ Partial ☐ No

2. Risk Assessment and Review

Item	Rule	Evidence on file	Result
Reasonably foreseeable internal and external risks to electronic, paper and other records are identified and assessed	17.03(2)(b)	[Risk assessment, date]	☐ Yes ☐ Partial ☐ No
Current safeguards are evaluated and improved where needed, including staff training, staff compliance with policies, and ways to detect and prevent security failures	17.03(2)(b)1.-3.	[Assessment section]	☐ Yes ☐ Partial ☐ No
The program is monitored regularly to make sure it is working, and safeguards are upgraded as needed	17.03(2)(h)	[Monitoring records]	☐ Yes ☐ Partial ☐ No
The scope of the security measures is reviewed at least once a year, and whenever a material change in business practices may affect how records are protected	17.03(2)(i)	[Review memo, date]	☐ Yes ☐ Partial ☐ No

3. Employees

Item	Rule	Evidence on file	Result
Ongoing training for every employee, including temporary and contract staff	17.03(2)(b)1.	[Training records]	☐ Yes ☐ Partial ☐ No
Training covers how to use the computer security system and why protecting personal information matters	17.04(8)	[Training content]	☐ Yes ☐ Partial ☐ No
Policies for keeping, accessing and carrying records with personal information outside the office	17.03(2)(c)	[Policy section]	☐ Yes ☐ Partial ☐ No
Disciplinary measures for breaking the program's rules	17.03(2)(d)	[Policy section]	☐ Yes ☐ Partial ☐ No
People who leave can no longer reach records with personal information, both physical and electronic	17.03(2)(e)	[Offboarding checklist]	☐ Yes ☐ Partial ☐ No

4. Service Providers

Item	Rule	Evidence on file	Result
Reasonable steps to choose and keep service providers that can protect personal information. Service providers generally include your IT provider and cloud software vendors	17.03(2)(f)1.	[Vendor reviews]	☐ Yes ☐ Partial ☐ No
Contracts require each service provider to put in place and maintain appropriate security measures	17.03(2)(f)2.	[Contract clauses]	☐ Yes ☐ Partial ☐ No

5. Physical Security

Item	Rule	Evidence on file	Result
Reasonable limits on who can physically reach records with personal information, and storage in locked rooms, cabinets or containers	17.03(2)(g)	[Policy, key log]	☐ Yes ☐ Partial ☐ No

6. Computer System Security

Skip this section only if the business never stores or sends personal information electronically. Each item applies "to the extent technically feasible" (17.04).

Item	Rule	Evidence on file	Result
User IDs and other sign-in identifiers are controlled	17.04(1)(a)	[User list]	☐ Yes ☐ Partial ☐ No
Passwords are assigned and chosen in a reasonably secure way, or the business uses unique identifier technology such as biometrics or token devices	17.04(1)(b)	[Password or MFA settings]	☐ Yes ☐ Partial ☐ No
Passwords are stored in a place or format that does not put the data at risk	17.04(1)(c)	[Password manager or policy]	☐ Yes ☐ Partial ☐ No
Only active users and active accounts have access	17.04(1)(d)	[Account review, date]	☐ Yes ☐ Partial ☐ No
Access is blocked after multiple failed sign-in attempts	17.04(1)(e)	[Lockout setting]	☐ Yes ☐ Partial ☐ No
Access to files with personal information is limited to people who need it for their jobs	17.04(2)(a)	[Access list, review date]	☐ Yes ☐ Partial ☐ No
Each person has a unique ID and password. No vendor default passwords	17.04(2)(b)	[User list, setup checklist]	☐ Yes ☐ Partial ☐ No
Records and files with personal information are encrypted when they travel across public networks, and all wireless transmissions of personal information are encrypted	17.04(3)	[Email, Wi-Fi, portal settings]	☐ Yes ☐ Partial ☐ No
Systems are reasonably monitored for unauthorized use of or access to personal information	17.04(4)	[Log settings, alerts]	☐ Yes ☐ Partial ☐ No
Personal information on laptops and other portable devices is encrypted	17.04(5)	[Encryption report]	☐ Yes ☐ Partial ☐ No

Item	Rule	Evidence on file	Result
Systems with personal information that connect to the internet have reasonably up-to-date firewall protection and operating system security patches	17.04(6)	[Firewall and patch report]	☐ Yes ☐ Partial ☐ No
Security software with malware protection is installed, kept current, and set to receive updates regularly	17.04(7)	[Device report]	☐ Yes ☐ Partial ☐ No

7. Disposal

The state's disposal law, M.G.L. c. 93I, also counts biometric data as personal information (c. 93I, section 1).

Item	Rule	Evidence on file	Result
Paper with personal information is redacted, burned, pulverized or shredded so it cannot practicably be read or rebuilt	c. 93I, s. 2(a)	[Shredding log or certificates]	☐ Yes ☐ Partial ☐ No
Computers, drives, phones and other media are destroyed or erased so personal information cannot practicably be read or rebuilt	c. 93I, s. 2(b)	[Wipe records, certificates]	☐ Yes ☐ Partial ☐ No

8. Incidents and Breach Notice

Item	Rule	Evidence on file	Result
Every incident involving a breach of security is documented, with the actions taken in response	17.03(2)(j)	[Incident log]	☐ Yes ☐ Partial ☐ No
A post-incident review is done after each one, and business practices are changed where needed	17.03(2)(j)	[Review notes]	☐ Yes ☐ Partial ☐ No
A written procedure to notify the Attorney General, the director of the Office of Consumer Affairs and Business Regulation, and affected residents as soon as practicable and without unreasonable delay	Supports c. 93H, s. 3(b)	[Procedure section]	☐ Yes ☐ Partial ☐ No
The procedure covers offering at least 18 months of free credit monitoring through a third party when Social Security numbers are involved	Supports c. 93H, s. 3A(a)	[Procedure section]	☐ Yes ☐ Partial ☐ No

Breach notices must mention the WISP. When a business reports a breach under section 3, the notice to the Attorney General and OCABR must say whether it maintains a WISP, and what steps it is taking, including updating the WISP (c. 93H, section 3(b)(viii) and (ix)).

Results by Section

Section	Items	Yes	Partial	No
1. The written program	5			
2. Risk assessment and review	4			
3. Employees	5			
4. Service providers	2			
5. Physical security	1			
6. Computer system security	12			
7. Disposal	2			
8. Incidents and breach notice	4			
Total	35			

What to fix first. Every No or Partial needs an owner and a date. Start with section 1: without a written program, nothing else on this list can be shown. Then move to encryption of laptops and portable devices (17.04(5)) and service provider contracts (17.03(2)(f)2.).

Completed by	[Name, title]
Program owner	[Name]
Date	[Month DD, YYYY]

ABOUT

About This Checklist

A checklist for any business that holds personal information about Massachusetts residents, built from the text of 201 CMR 17.00 and the state's disposal and breach notice laws. Each item names the paragraph it comes from. Items marked "Supports" help show a requirement is met but are not named in the rule.

How to use it

- Work through it with whoever runs IT for the business. Section 6 needs that person's answers.
- Fill in the evidence column for every Yes. If you cannot point to a document or a setting, mark it No.
- If you already have a HIPAA risk analysis or a Regulation S-P program, check whether it covers each item.
- The Office of Consumer Affairs and Business Regulation also publishes a short compliance checklist on mass.gov.
- Run it again each year (17.03(2)(i)), and after any incident, new vendor or system change.

Before you rely on it

This checklist reflects 201 CMR 17.00 and M.G.L. c. 93H and c. 93I as published in November 2026. It is not legal advice and it does not certify compliance. A checklist is not a WISP: the program itself has to be written for your business.

Free to use

Use it, change it and share it inside your business. If you would rather have the WISP written for you, it is included with every SaberGuard HIPAA risk analysis. Contact SaberGuard.

Jonathan DeLeon, CISM, CCSP

SaberGuard, LLC | jonathan.deleon@saberguard.tech | saberguard.tech