



Q. What is Mass 201 CMR 17.00, and when does it take effect?

A. It's a new Massachusetts State law entitled, "Standards for The Protection of Personal Information of Residents of the Commonwealth" and the deadline for each company to comply is March 1st 2010.

Q. How do I know whether the new law applies to my business?

A. The law applies to all organizations, "who own, license, store or maintain personal information about a resident of the Commonwealth of Massachusetts." This includes Human Resources data on your employees in addition to your customer records, transaction records and other sensitive data.

Q. What is required in order to be compliant with CMR 17?

A. In order to be compliant with the new law, you must:

- Create and maintain a Written Information Security Plan (WISP) that details all of your potential security vulnerabilities and the remedies you have taken to address them.
- Enact a Data Privacy Awareness Policy which applies to all employees who have access to private data.
- Employ data security monitoring, antivirus, firewall and encryption on all your servers, PCs, laptops, mobile devices and databases.
- Review the policies of all third-parties with whom you share information to ensure that they are also compliant.

Q. What are the consequences of non-compliance?

A. If there is a data breach at your business and you are found to have been non-compliant, the Attorney General of Massachusetts can investigate and levy fines against you. Currently, your financial liability appears to be:

- Up to \$50,000 per incident of improper record disposal.
- A maximum of \$5,000 per violation of compliance standards.
- The Attorney General may file suit, and order a Forensic Data Discovery performed by a third party. You would be liable to pay for this audit – typically around \$150,000.
- Massachusetts citizens whose data were compromised may file suit individually, or through class action.
- Courts can order punitive damages if it is determined that a company's security was poor enough to be considered willful negligence.

Q. How can Internet & Telephone help me become compliant?

A. Our IT Managed Services (ITMS) customers receive dedicated support, 24/7 monitoring, anti-virus, firewall and CIO level consulting for IT Planning. We will help guide you so you can bring all of your systems in to compliance, and provide you with the WISP and Data Privacy Awareness Policies you need to protect your business.



Overview of Mass Privacy requirements

Conduct Internal Audit

- Identify and evaluate the effectiveness of current safeguards.
- Identify reasonably foreseeable internal and external risks.
- Review contracts with third party vendors to ensure they require that they be compliant.
- Review password policies, security access levels and unique identification processes.
- Identify training methodology for employees on proper privacy security.



Written Information Security Plan

Safeguards

The WISP should identify policy and technical safeguards to protect Personal Information. This includes electronic security (Firewall, Anti-Virus, Security Configurations, etc) as well as details on specific administrative and policy protocols that your employees will follow when dealing with Personal Information.



Custodians

Your WISP must specifically identify which employee(s) are responsible for the implementation and performance for the plan, and who is responsible for each area of security. Specific responsibilities should be delegated to those individuals most capable of managing them.



Risk Assessment

The WISP must list all of the physical and digital mediums which contain or grant access to Personal Information, and specify which specific steps are to be taken to secure them. This includes both electronic and physical record-keeping, as well as any transaction-based process that could potentially expose Personal Information to risk. Each potential threat must be listed, rated and described.



Training

The WISP should outline employee training and monitoring policies to ensure that all employees are aware of proper protocol and security procedures. It should also specify what consequences are anticipated in the event an employee violates the policy.



Access

The WISP needs to include policies and procedures for determining which employees have access, and it should also include a provision to immediately terminate access (passwords, logins) of any employee who leaves your company. It also must detail when and how records containing Personal Information are allowed to be stored or transported off-site.



Maintenance

The WISP must include a policy for regular review and maintenance of the Written Information Security Plan, including a policy for upgrading the WISP as necessary. It must also detail a procedure for documenting details in the event of a security breach, and outline the policy for a post-incident review following any such event.





Security procedures

Intrusion Prevention and Detection

- Install Firewalls
- Install Anti-Virus and Intrusion Monitoring
- Require Encryption of all Personal Information
- Create a locked-door policy for all areas which grant access to PI.
- Conduct periodic intrusion detection of your networks and computers.



Record Management

- Adopt a document shredding policy and retain a service that provides Certifications of Destruction.
- Physically secure the location of all computerized and physical records.
- Restrict access to Personal Information records to “need to know” employees.



Audit

- Hire a third party to conduct a Compliance Audit to ensure that your efforts have been thorough and that you have adequately prepared all documentation.

