

## 201 CMR 17.00 Massachusetts Privacy Law

I tried to explain with this document what I believe you should do in regard to the requirements of 201 CMR 17.00 Massachusetts Privacy Law. This is not a legal document; just what I perceive should be done to comply with these regulations. Please remember than I am not a lawyer, just a “technologist” and my expertise resides with the “logistics” associated with implementing these regulations, not with the reasoning or the “why” of these regulations.

Gerard Louise

**Technical Support International, Inc.**

**Tel: 508-543-6979**

**glouise@tsisupport.com**

Again, more details can be found at:

<http://www.mass.gov/?pageID=ocaterminal&L=4&L0=Home&L1=Consumer&L2=Privacy&L3=Identity+Theft&sid=Eoca&b=terminalcontent&f=reg201cmr17&csid=Eoca>

All items in black are excerpts from CMR 17.00, all items in red are my comments and recommendations.

## Does the law apply to my business?

This what the law says:

1. You electronically store a Massachusetts resident Last Name and First name on a computer

2. Plus one of the following (a,b,c or d)

- A. Social Security number
- B. Driver's License number
- C. Financial Account number (credit card, debit card)
- D. Access code that would allow you to access that person financial information

Then the law applies to your business..(See below VERBATIM, the section referring to whom it applies to"

"Personal information," a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account;

provided, however, that “Personal information” shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

## **What can you do on your own?**

a) Designating one or more employees to maintain the comprehensive information security program;

*The key here is to designate someone within the company (owner, CFO, office manager, IT staff, etc.) that would be responsible to maintain all documentations and is briefed by TSI or other professional firms on his/her responsibilities.*

(b) Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to: (i) ongoing employee (including temporary and contract employee) training; (ii) employee compliance with policies and procedures; and (iii) means for detecting and preventing security system failures.

*A basic security audit on your company practices, including electronic and paper disposal policy; access to documents, passwords policy would also be helpful. You can conduct that audit on your own or hire a professional firm to do this.*

(c) Developing security policies for employees that take into account whether and how employees should be allowed to keep access and transport records containing personal information outside of business premises.

*This policy makes a lot of sense and should be incorporated into your existing employee policies. All you need to do is draft a set of guidelines that define how your employees keep and transport data outside of the business. For instance, if you have employees that carry laptops and have access to sensitive personal information, your policy would clearly prohibit this unless the data is properly encrypted using a specialized encryption software. Another example is “backup tapes” transport. If you allow an employee to store backup tapes at their homes or at remote locations, these backup tapes must also be encrypted. Most backup software support encryption.*

(d) Imposing disciplinary measures for violations of the comprehensive information security program rules.

*Item c only stands if you find a way to monitor and enforce this. This should not be an “optional compliance” on the part of your employees but a requirement with very clear implications if they refuse or fail to comply. Again, in order to make sure that item c is respected, you need to MONITOR the process, not just assume that everyone is on board. There are many tools that allow you to monitor compliance and we can recommend a few.*

(e) Preventing terminated employees from accessing records containing personal information by immediately terminating their physical and electronic access to such records, including deactivating their passwords and user names.

*This also makes a lot of sense and most companies with basic security practices already implement this measure*

(f) Taking reasonable steps to verify that third-party service providers with access to personal information have the capacity to protect such personal information, including (i) selecting and retaining service providers that are capable of maintaining safeguards for personal information; and (ii) contractually requiring service providers to maintain such safeguards. Prior to permitting third-party service providers access to personal information, the person permitting such access shall obtain from the third-party service provider a written certification that such service provider has a written, comprehensive information security program that is in compliance with the provisions of these regulations.

*Now, this one is a good one. You have now deployed a good set of security practices for your firm, all your employees signed on it, you monitor the process and make sure that all data leaving the premises is secured and encrypted but what if you make some information available to a 3rd party contact such as your payroll company, your accounting firm, your outsourced HR company? Well, you have the right (and obligation) to demand that they provide you with a written document that certifies that they also in compliance with the regulations.*

*Keep in mind that this is not an optional request but a required step and you are responsible to obtain written documentation from them. (See article from Boston Globe, Sept 23, 2008)*

*“a covered business fails to comply with the regulations, the Massachusetts Attorney General may bring an action under Massachusetts' consumer protection statute for injunctive relief, to recover a fine payable to the commonwealth of up to \$5,000 for each “method, act or practice” that the business knew or should have known violated the regulations, and to recover the costs of such litigation, including reasonable attorneys' fees. See Mass. Gen. Laws Ch. 93H § 6 and 93A § 4 (2008). Such an action by the Massachusetts Attorney General may be more likely than attorney general enforcement actions generally because Massachusetts residents have recently been the victims of the highly publicized TJX and Hannaford data thefts. See Todd Wallack, “Tougher consumer data rule adopted,” The Boston Globe, Sept. 23, 2008”*

(g) Limiting the amount of personal information collected to that reasonably necessary to accomplish the legitimate purpose for which it is collected; limiting the time such information is retained to that reasonably necessary to accomplish such purpose; and limiting access to those persons who are reasonably required to know such information in order to accomplish such purpose or to comply with state or federal record retention requirements.

*I think most businesses already try to do this, by requiring specific ID's and passwords to access Payroll, HR or Accounting systems. The problem that I often see is due to the fact that many companies do not have a clear understanding of file access rights and inadvertently allow all users to access confidential data. Retention is also a big problem for many companies as sometimes people are afraid to delete old information. In my opinion, if you don't need it anymore, delete it or store it to external media (ENCRYPTED)*

(h) Identifying paper, electronic and other records, computing systems, and storage media, including laptops and portable devices used to store personal information, to determine which records contain personal information, except where the comprehensive information security program provides for the handling of all records as if they all contained personal information.

*Each company should conduct an internal audit and you, as a business should know where the data resides (electronic storage, paper, storage media, web site, etc.). Once you have a better understanding on how you are storing and keeping the information, TSI, can assist you in developing and implementing good electronic security measures.*

(i) Reasonable restrictions upon physical access to records containing personal information including a written procedure that sets forth the manner in which physical access to such records is restricted; and storage of such records and data in locked facilities, storage areas or containers.

*This is closely tied to item c. You need to have a written procedure that clearly defines how you handle access to personal records. In addition, your written procedure should include how you are protecting this information and where you are storing it*

(j) Regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information; and upgrading information safeguards as necessary to limit risks.

*You can monitor access to secure information by using many of the audit log built-in the Operating Systems of many computers (Windows, MAC's, Linux). In most cases, these audit tools need to be activated and configured by professional staff. In some other situations, these tools may not be sufficient and 3<sup>rd</sup> party tools need to be installed and configured. Monitoring also may include "manual" inspection on your side to make sure that people are complying with your security policies.*

(k) Reviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information.

*This makes perfect sense and I also would recommend an annual review of your business practices to determine if anything needs to be changed or updated in regard to data security at your place of business.*

(l) Documenting responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

*This "incident response plan" already exists within many of our customers and basically, it is a set of guidelines that clearly state "WHAT IF". For instance, you discover by reading one of the audit logs that one of your employees has tried 17 times in a row to access a secured location on your server, what do you do? Or you find out that one of your HR person has lost a USB Flash Drive that contains personal data of all your employees (Over 85.000 were lost last year!), what do you do? Keep in mind that the state of Massachusetts will not go after you if something happens but will if something happens and you do nothing about it.*

# How this law does relate to your computers and networks?

*The law is not very clear if this applies to all computers, wired, non wired (wireless), mobile computers, Servers, etc. My understanding is that it applies to all but some would argue that only mobile computers should be affected. Regardless, the security practices that are recommended are GOOD security practices and it would not make sense to just implement on mobile computers but on all computers.*

This is what item 17.04 says and you will find below each paragraph a quick explanation and recommendations from a “technologist” point of view.

## 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;

*You need to make sure that ALL user ID's and Passwords are “unique”*

(ii) a secure method of assigning and selecting passwords consisting of at least seven Letters and numbers;

*Use more complex passwords, example “tsifoxboro!2008” [word + Special Character + Number]*

(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;

*Do not store passwords on the same application that passwords are needed for. For instance, if you have a database called HR, do use a field in the HR database to store the passwords of the people who have access to the HR Database.*

(iv) Restricting access to active users and active user accounts only; and

*If that person is no longer in the company or doesn't use the application, REMOVE IT!*

(v) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;

*Most Operating systems (Server based mostly) provide a mechanism to BLOCK a user after so many unsuccessful attempts to access an application. I recommend this to everyone because we see a lot of this going on, mostly with people trying to gain access from the Internet.*

(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

*Make sure that people who have access to specific application containing personal information are the ONLY people with credentials to the applications. Review your application credentials and make sure that ONLY people who need access to certain modules are defined. For instance if you run an accounting system that includes a HR module, make sure that the HR module is not available for staff members who only need access to AR and payables.*

- (ii) assign a unique identification plus a password, which is not vendor supplied, to each person with computer access;

*All vendor supplied passwords should be replaced with your OWN passwords. Assign each person with computer access with their own User ID and their own password (Do not share ID's and passwords)*

(3) Encryption of all transmitted records and files containing personal information, including those in wireless environments that will travel across public networks.

*Two things here: First, if you are using wireless networks, make sure that the Access Points or Wireless routers are properly encrypted. This is normally done on the device itself and it requires some technical understanding. Second, the data that you are transmitting over the wireless network needs ALSO to be encrypted. There are many ways to encrypt data and I can suggest a few.*

(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;

*Monitoring of the security of your network can be accomplished by using comprehensive management tools and also tapping into the existing audit tools that are built-in most operating systems. I can provide you with more information if you have any questions.*

(5) Periodic review of audit trails restricted to those with job-related need to view audit trails;

*Some of the periodic reviews can be automated (regular email reports) or manually processed by a human being physically reviewing the system logs. Access to the logs should ONLY be permitted to specific individuals and defined in the Security policy of your firm.*

(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.

*Most businesses know by now that Internet Security requires a dedicated Firewall. Smaller organizations still use basic routers with NAT (network Address translation) and this is not good enough. If your business is*

*connected to the Internet and if you keep personal information that is subject to 201 CMR 17.00, you MUST use a certified firewall (Sonicwall, Cisco, Juniper, etc.). In addition, all up-to-date security patches for the Operating System MUST be installed. Many organizations use TSI to manage their Firewall and Patch Management but if you have the internal resources to perform these tasks, it can also be done internally.*

(7) The most current version of system security agent software which must include antispyware 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.

*Anti-virus and Anti-Spyware must be installed on ALL computers that are connected to the Internet. Many of these applications allow automatic updating of the various updates and patches. If your organization uses a File Server, the chances are that you are probably already doing this but if you are not sure, let us know and we can check this for you.*

(8) Education and training of employees on the proper use of the computer security system and the importance of personal information security.

*I strongly recommend spending an hour or two with your employees and explaining why security matter and what they can do to contribute and to make sure that your organization meets all compliance requirements*

(9) Restricted physical access to computerized records containing personal information, including a written procedure that sets forth the manner in which physical access to personal information is restricted. When notified of any unauthorized entry into a secure area by either an employee or any other unauthorized person, the integrity of the computerized records must be reviewed.

*This is probably one of the most difficult guidelines to implement because many companies do not have a "secure area". I would recommend incorporating your implementations for the guidelines (i) on page 4 of this document*

*In conclusion, the ramifications for non-compliance go beyond the potential fines from the law. If a business fails to comply with CMR 17.00, that company can be found professionally negligent. Since it is easy to prove or disprove due care and due diligence by the fact there are quantifiable standards, a law as this makes it easy to hold a company accountable. Unfortunately for the company, if they are not compliant and a verdict is awarded, insurance will not cover the loss. This is unfamiliar to most business owners, since they do not equate non-compliance with their computer security with negligent behavior. This can easily put a business into bankruptcy.*