

Frequently Asked Questions about the new Massachusetts Data Privacy Law (201 CMR 17.00).

Contents

What do I have to do?.....	1
When do I have to do this?	1
Who does it cover?	1
What information does it cover?	1
What are some examples things that must be encrypted?	1
Does encryption only affect my computer?	2
What are the penalties?.....	2
Do I need some kind of policy?	2
Who, in my company does this job?	2
What can I use to encrypt and erase files on my computer?	2
TrueCrypt containers to secure computer files	2
Tolvanen's Eraser	2
Thawte Personal E-mail Certificate	2

What do I have to do?

Get the "201 CMR 17.00 COMPLIANCE CHECKLIST" published by the state. It lists the requirements in an easy to understand format.

When do I have to do this?

The law goes into effect on January 1st 2010. I recommend starting changes now, if you wait till the last minute it will become a rushed project and that increases the probability of running into problems. Take your time and pace yourself.

Who does it cover?

Every person and company that owns, licenses, stores or maintains personal information about a resident of Massachusetts.

What information does it cover?

It covers "Personal Information". That is a combination of a resident's first and last name connected to one of the following: A driver's license number, state-issued identification card number, a credit card number, financial account number or a Social Security number.

What are some examples things that must be encrypted?

- Quickbooks or Pro Series files and backups
- Letters to the IRS that contain SSNs
- Letters to banks that contain account numbers
- Email storage (in case a customer or employee sends you the SSN).
- Email you send that contains personal information.

Note: Password Protection is NOT the Same as Encryption

Does encryption only affect my computer?

No, it applies to any electronic data. Some examples are:

- Computer, it most likely contains some personal information in tax or accounting applications or letters.
- Flash, jump or keychain drives, they may have letters or backups that contains some personal.
- PDAs or cell phones, if you store client or employee personal information on them in things like contact list. Or if it synchronizes with your email.
- Backup tapes may contain some personal information.

What are the penalties?

According to MA General Law 93I, there's a \$100 fine per record lost, with a maximum of \$50K per "incident". MA General Law 93H states that there will be a \$5,000 fine per "violation." It's unclear what the correlation is between an individual record lost and an "incident or violation".

Do I need some kind of policy?

You need to have a Written Information Security Policies (WISP). It is a security policy in writing that describes how you will discipline violators, prevent terminated employees from accessing data, destroy hard copies of personal information, prevent third parties that have access to your data, lock up all hard copies that contain personal data, report and record violations of the policy, and regularly monitor and review the scope and effectiveness of the policy.

ISO 27001 is an internationally accepted best practices framework for the development and management of information security programs. I recommend looking at it also when developing your WISP.

DO NOT assume a "computer guy" is qualified to write a WISP or the policies, procedures and controls that are necessary for compliance. They can help with application and remediation but there's a big difference between technology and compliance.

Who, in my company does this job?

You need to designate someone who will design, maintain, report and enforce the security policy. If you're a small business owner, sorry, that's probably you.

What can I use to encrypt and erase files on my computer?

TrueCrypt containers to secure computer files

TrueCrypt is a versatile, well-respected, free program that allows you to create a new drive on your computer-- you pick the letter-- which you can use like any other drive. Copy files to it, delete files, create folders and subfolders, copy whole folder trees from you data.

Tolvanen's Eraser

Tolvanen's Eraser (<http://www.tolvanen.com/eraser/>) is a free, widely-used program that lets you securely delete electronic files from your computer so that no one, including an IT professional with fancy recovery tools, can recover the files.

Thawte Personal E-mail Certificate

A Thawte Personal E-mail Certificate in conjunction with the Thawte Web of Trust allows you to secure and guarantee authorship of your e-mail communications by digitally signing and encrypting your e-mails.