



DEVAL L. PATRICK
GOVERNOR

TIMOTHY P. MURRAY
LIEUTENANT GOVERNOR

**COMMONWEALTH OF MASSACHUSETTS
OFFICE OF CONSUMER AFFAIRS & BUSINESS REGULATION**

10 Park Plaza, Suite 5170 Boston, MA 02116
(617) 973-8700 FAX (617) 973-8799 TTY/TDD (617) 973-8790
www.mass.gov/consumer

DANIEL O'CONNELL
SECRETARY OF HOUSING AND
ECONOMIC DEVELOPMENT

DANIEL C. CRANE
UNDERSECRETARY OF
CONSUMER AFFAIRS AND
BUSINESS REGULATION

Frequently Asked Question Regarding 201 CMR 17.00

Must my data security program be in writing?

Yes, your information security program must be in writing. The scope and complexity of the document will vary depending on your resources, and the type of personal information you are storing or maintaining. But, everyone who stores or maintains personal information must have a written plan detailing the measures adopted to safeguard such information.

If I have independent contractors working for me, am I responsible for them?

You have the duty to take all reasonable steps (1) to verify that any third-party service provider with access to personal information has the capacity to protect such personal information in the manner provided for in 201 CMR 17.00; and (2) to ensure that such third party service provider is applying to such personal information protective security measures at least as stringent as those required to be applied to personal information under 201 CMR 17.00.

Do I have to do an inventory of all my paper and electronic records?

No, you do not have to inventory your records. However, you do need to identify which of your records contain personal information so that you can handle and protect that information in a manner that complies with the regulations. Most small companies already know which files contain this kind of information, and can quickly determine where in the company's paper and electronic systems this information exists.

How do I know if my current computer system complies with the encryption requirements?

You are probably going to need outside help in figuring this out, unless you have in-house IT staff or already retain the services of a consultant to help with IT matters. Although the definition of encryption is technology neutral, you do need to make sure that the encryption process you are using is transforming the data so that it cannot be understood without the use of a confidential key or process. Free encryption software is available, but unless you are computer savvy, you are going to need an outside IT consultant to help with setup (unless, of course, you have your own IT staff).

Is everyone's level of compliance going to be judged by the same standard?

Both the statute and the regulations specify that compliance is to be judged taking into account the size and scope of your business, the resources that you have available to you, the amount of data you store, and the need for confidentiality. This will be judged on a case by case basis.

How much employee training do I need to do?

There is no magic formula here. You will need to do enough training to ensure that the employees that will have access to personal information know what their obligations are regarding the protection of that information, as set forth in the regulations.



Better businesses. Smarter consumers.



How do I decide who can have access to records containing personal information?

The regulations require you to limit access to personal information only to those persons who are reasonably required to have access in order to accomplish a legitimate business purpose, or to comply with other state or federal regulations. Whatever is needed for compliance with state or federal laws/regulations is automatically authorized. Otherwise, you should identify your business needs, determine what tasks are reasonably necessary to satisfy those business needs, and identify who must have access to carry out those tasks.

How do I know if I'm limiting in the right way the amount of personal information collected?

Like the previous question the correct approach here involves determining your legitimate business needs, identifying the kind of personal information reasonably needed to perform the tasks required to satisfy those business needs. Here again collection of personal information needed for compliance with state or federal laws/regulations is always permitted.

Will I need to buy new computer equipment or new software?

Your need for new computer equipment will depend on whether your current equipment meets the minimum requirements for running the software that will secure any electronic records containing personal information. The versions of the security and operating system that you currently have must be supported to receive security updates, and your computer equipment must meet the minimum requirements for running the needed software. If not, you will need new software, new hardware, or both.

What is the extent of my "monitoring" obligation?

The level of monitoring necessary to ensure your information security program is providing protection from unauthorized access to, or use of, personal information, and effectively limiting risks will depend largely on the nature of your business, your business practices, and the amount of personal information you are maintaining or storing. It will also depend on the form in which the information is kept and stored. Obviously, information stored as a paper record will demand different monitoring techniques from those applicable to electronically stored records. In the end, the monitoring that you put in place must be such that it is reasonably likely to reveal unauthorized access or use.

Do I need to hire a computer consultant to set up user identification protocols, secure access control measures, and firewalls?

Businesses that store or maintain electronic records, and do not have in-house IT resources or regular access to providers of IT services, will probably need to hire someone to provide these services/resources, even if only on a one-time or part-time basis.

