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
www.mass.gov/consumer

GREGORY BIALECKI
SECRETARY OF HOUSING AND ECONOMIC DEVELOPMENT

BARBARA ANTHONY
UNDERSECRETARY OF CONSUMER AFFAIRS AND BUSINESS REGULATION

Frequently Asked Question Regarding 201 CMR 17.00

What are the differences between this version of 201 CMR 17.00 and the version issued in February of 2009?

There are some important differences in the two versions. First, the most recent regulation issued in August of 2009 makes clear that the rule adopts a risk-based approach to information security, consistent with both the enabling legislation and applicable federal law, especially the FTC's Safeguards Rule. A risk-based approach is one that directs a business to establish a written security program that takes into account the particular business' size, scope of business, amount of resources, nature and quantity of data collected or stored, and the need for security. It differs from an approach that mandates every component of a program and requires its adoption regardless of size and the nature of the business and the amount of information that requires security. This clarification of the risk based approach is especially important to those small businesses that do not handle or store large amounts of personal information. Second, a number of specific provisions required to be included in a business's written information security program have been removed from the regulation and will be used as a form of guidance only. Third, the encryption requirement has been tailored to be technology neutral and technical feasibility has been applied to all computer security requirements. Fourth, the third party vendor requirements have been changed to be consistent with Federal law.

To whom does this regulation apply?

The regulation applies to those engaged in commerce. More specifically, the regulation applies to those who collect and retain personal information in connection with the provision of goods and services or for the purposes of employment. The regulation does not apply, however, to natural persons who are not in commerce.

Does 201 CMR 17.00 apply to municipalities?

No. 201 CMR 17.01 specifically excludes from the definition of "person" any "agency, executive office, department, board, commission, bureau, division or authority of the Commonwealth, or any of its branches, or any political subdivision thereof." Consequently, the regulation does not apply to municipalities.

Must my information 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 owns or licenses personal information must have a written plan detailing the measures adopted to safeguard such information.

What about the computer security requirements of 201 CMR 17.00?

All of the computer security provisions apply to a business if they are technically feasible. The standard of technical feasibility takes reasonableness into account. (See definition of "technically feasible" below.) The computer security provisions in 17.04 should be construed in accordance with the risk-based approach of the regulation.

Does the regulation require encryption of portable devices?

Yes. The regulation requires encryption of portable devices where it is reasonable and technically feasible. The definition of encryption has been amended to make it technology neutral so that as encryption technology evolves and new standards are developed, this regulation will not impede the adoption of such new technologies.

Do all portable devices have to be encrypted?

No. Only those portable devices that contain personal information of customers or employees and only where technically feasible The "technical feasibility" language of the regulation is intended to recognize that at this period in the development of encryption technology, there is little, if any, generally accepted encryption technology for most portable devices, such as cell phones, blackberries, net books, iphones and similar devices. While it may not be possible to encrypt such portable devices, personal information should not be placed at risk in the use of such devices. There is, however, technology available to encrypt laptops.

Must I encrypt my backup tapes?

You must encrypt backup tapes on a prospective basis. However, if you are going to transport a backup tape from current storage, and it is technically feasible to encrypt (i.e. the tape allows it) then you must do so prior to the transfer. If it is not technically feasible, then you should consider the sensitivity of the information, the amount of personal information and the distance to be traveled and take appropriate steps to secure and safeguard the personal information. For example, if you are transporting a large volume of sensitive personal information, you may want to consider using an armored vehicle with an appropriate number of guards.

What does "technically feasible" mean?

"Technically feasible" means that if there is a reasonable means through technology to accomplish a required result, then that reasonable means must be used.

Must I encrypt my email if it contains personal information?
If it is not technically feasible to do so, then no. However, you should implement best practices by not sending unencrypted personal information in an email. There are alternative methods to communicate personal information other through email, such as establishing a secure website that requires safeguards such as a username and password to conduct transactions involving personal information.

Are there any steps that I am required to take in selecting a third party to store and maintain personal information that I own or license?
You are responsible for the selection and retention of a third-party service provider who is capable of properly safeguarding personal information. The third party service provider provision in 201 CMR 17.00 is modeled after the third party vendor provision in the FTC's Safeguards Rule.

I have a small business with ten employees. Besides my employee data, I do not store any other personal information. What are my obligations?
The regulation adopts a risk-based approach to information security. A risk-based approach is one that is designed to be flexible while directing businesses to establish a written security program that takes into account the particular business's size, scope of business, amount of resources and the need for security. For example, if you only have employee data with a small number of employees, you should lock your files in a storage cabinet and lock the door to that room. You should permit access to only those who require it for official duties. Conversely, if you have both employee and customer data containing personal information, then your security approach would be more stringent. If you have a large volume of customer data containing personal information, then your approach would be even *more* stringent.

Except for swiping credit cards, I do not retain or store any of the personal information of my customers. What is my obligation with respect to 201 CMR 17.00?
If you use swipe technology only, and you do not have actual custody or control over the personal information, then you would not own or license personal information with respect to *that* data, as long as you batch out such data in accordance with the Payment Card Industry (PCI) standards. However, if you have employees, see the previous question.

Does 201 CMR 17.00 set a maximum period of time in which I can hold onto/retain documents containing personal information?
No. That is a business decision you must make. However, as a good business practice, you should limit the amount of personal information collected to that reasonably necessary to accomplish the legitimate purpose for which it is collected and limit the time such information

is retained to that reasonably necessary to accomplish such purpose. You should also limit access to those persons who are reasonably required to know such information.

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 should perform a risk assessment and identify which of your records contain personal information so that you can handle and protect that information.

How much employee training do I need to do?
There is no basic standard here. You will need to do enough training to ensure that the employees who will have access to personal information know what their obligations are regarding the protection of that information, as set forth in the regulation.

What is a financial account?
A financial account is an account that if access is gained by an unauthorized person to such account, an increase of financial burden, or a misappropriation of monies, credit or other assets could result. Examples of a financial account are: checking account, savings account, mutual fund account, annuity account, any kind of investment account, credit account or debit account.

Does an insurance policy number qualify as a financial account number?
An insurance policy number qualifies as a financial account number if it grants access to a person's finances, or results in an increase of financial burden, or a misappropriation of monies, credit or other assets.

I am an attorney. Do communications with clients already covered by the attorney-client privilege immunize me from complying with 201 CMR 17.00?
If you own or license personal information, you must comply with 201 CMR 17.00 regardless of privileged or confidential communications. You must take steps outlined in 201 CMR 17.00 to protect the personal information taking into account your size, scope, resources, and need for security.

I already comply with HIPAA. Must I comply with 201 CMR 17.00 as well?
Yes. If you own or license personal information about a resident of the Commonwealth, you must comply with 201 CMR 17.00, even if you already comply with HIPAA.

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 own or license. 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.

Is everyone's level of compliance going to be judged by the same standard?
Both the statute and the regulations specify that security programs should take 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.