A PRACTICAL GUIDE TO UNDERSTANDING AND COMPLYING WITH MASSACHUSETTS DATA SECURITY REGULATIONS

February 2010

www.morganlewis.com

A PRACTICAL GUIDE TO UNDERSTANDING AND COMPLYING WITH MASSACHUSETTS DATA SECURITY REGULATIONS

Background

On October 30, 2009, the Massachusetts Office of Consumer Affairs and Business Regulation ("OCABR") filed its final amended regulations for 201 CMR 17.00 (the "Regulations") with the Secretary of the Commonwealth requiring that persons who "own or license personal information about a resident of the Commonwealth" comply with strict requirements to safeguard such personal information.

The Regulations set forth the minimum standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records. The objectives of the Regulations are (1) to ensure the security and confidentiality of personal information consistent with industry standards, (2) to protect against anticipated threats or hazards to the security or integrity of such information, and (3) to protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any resident of the Commonwealth.

The deadline for compliance with the Regulations is March 1, 2010. This Guide is intended to assist you in understanding and complying with the Regulations.

Are You Required to Comply?

The Regulations are applicable to ANY business (including an out-of-state entity) that "receives, stores, maintains, processes, or otherwise has access to personal information in connection with the provision of goods or services or in connection with employment" about a resident of Massachusetts.

ANY business, *no matter where located*, with customers or employees who are residents of Massachusetts must comply with the Regulations.

Personal information is defined as:

- A Massachusetts resident's first name and last name or first initial and last name, in combination with any one of the following data elements that relate to such resident:
  (a) Social Security number;
  (b) Drivers license or state-issued identification 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.
- Personal information does *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.
- If you are a business that only uses credit card swiping technology and batches out such data in accordance with the Payment Card Industry standards and does not otherwise have

actual custody or control over personal information, then you are not considered to "own or license" personal information with respect to that data within the meaning of the Regulations.

- While the Regulations suggest that only information about *natural* persons is protected, better practice is to treat confidential information about all "persons" (including a corporation, trust, partnership or other legal entity) with the same duty of care as natural persons.

What You Need to Do

- **Read the Regulations.** Compliance with the requirements of the Regulations begins with an understanding of the Regulations. Familiarize yourself with the Regulations, which are attached to this Guide as Exhibit A and can be found online at: http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf. The requirements stem directly from the language of the Regulations, which include a requirement to develop a written comprehensive information security program.

  The OCABR has published answers to frequently asked questions regarding the Regulations, which are attached to this Guide as Exhibit B and can be found online at: http://www.mass.gov/ocabr/docs/idtheft/201cmr17faqs.pdf.

- **Assemble a team.** Determine who in your organization should be the point person to lead and coordinate your compliance efforts. You may want to designate a team to be responsible for ongoing compliance with the Regulations. Your team for developing the information security plan may need to include representatives from your IT, HR, Legal, Corporate Communications, and Audit Departments and key business lines. It is important to educate everyone in your organization about the Regulations and that non-compliance may result in disciplinary measures being taken.

- **Identify personal information.** Determine where personal information resides in your organization both in paper and electronic format. Utilize your point person and/or team to coordinate and assess among departments what information is collected and maintained by your organization. While the Regulations do not specifically require a written inventory of such data (although your organization must assess the amount of personal information it maintains as stored data), it would be helpful to your organization to do so. Depending on the structure of your organization, you may require assistance from many employees – including potentially as part of your training – to determine where such data resides. Sample survey questions are included as part of the sample acknowledgement form referenced in "*Provide ongoing training and monitoring*" below.

- **Develop, implement and maintain a comprehensive information security program.** Organizations are required to implement a written program that includes specific requirements applicable to any records containing personal information. These requirements include:

  (a) **Designating** person(s) responsible for maintaining the program;

  (b) **Identifying and assessing** "reasonably foreseeable" internal and external risks of personal information;

  (c) **Developing** security policies for employees relating to the storage, access and transportation of records containing personal information outside of business premises;

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

(e) **Preventing** terminated employees from accessing personal information;

(f) **Overseeing** third-party service providers by:

(i) **Taking reasonable steps** to select and retain third-party service providers that are capable of maintaining appropriate security measures; and

(ii) **Requiring third-party service providers** *by contract* to implement and maintain such appropriate security measures for personal information;[1]

(g) **Imposing reasonable restrictions** on how employees may keep, access, and transport personal information, including off premises;

(h) **Monitoring and ensuring** that the program is "operating in a manner reasonably calculated to prevent unauthorized access," including minimum annual review; and

(i) **Documenting** responsive actions taken in connection with a breach.

It is important that you discuss with your IT department and/or computer consultants the specifics of your organization's computer systems and to assess and develop a plan accordingly. While the OCABR has published a guide for *small businesses* in formulating a written program, which can be found online at: http://www.mass.gov/ocabr/docs/idtheft/sec-plan-smallbiz-guide.pdf; you must assess and determine your organization's structure and appropriate needs for a comprehensive written information security program. We have also included a listing to some resources on information security plans that you may find helpful.

- **Implement necessary computer security requirements**. You are required to have minimum security requirements for your computer systems and to encrypt data to the extent it is technically feasible. The standard of technical feasibility takes reasonableness into account: if there is a "reasonable means through technology" to accomplish a required result, then that reasonable means must be used. The minimum computer security and data encryption requirements include, but are not limited to the following:

(a) "reasonably up-to-date" firewall protection and operating system security patches;

(b) "reasonably up-to-date" versions of system security agent software, which must include malware protection and reasonably up-to-date patches and virus definitions;

(c) secure user authentication protocols including (i) control of user IDs, (ii) reasonably secure methods of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices, (iii) control of data security passwords, (iv) restricting access to active user and user accounts, and (v) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system; and

[1] Third-party contracts entered into prior to March 1, 2010 will be deemed compliant with the Regulations - even if the contract does not include a requirement that the third-party service provider maintain such appropriate safeguards - until March 1, 2012. Notwithstanding this exception, organizations are still required to take reasonable steps to select third-party service providers that are capable of maintaining appropriate security measures to protect such personal information consistent with the Regulations and any federal regulations.

(d) encryption of all transmitted records and files containing personal information that will travel across public networks and encryption of all data containing personal information to be transmitted wirelessly.

- **Encrypt data in transit, data stored on portable devices.** Any personal information that is travelling across "public networks" or that is transmitted wirelessly, or is stored on laptops or other portable devices must be encrypted, to the extent technically feasible. Many organizations will have questions regarding the encryption requirement. Some common questions and answers follow:

Q: What does "encrypted" mean?

A: The Regulations define "encrypted" as the transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key. Basic file/folder encryption allows the user to determine if a file should be encrypted or not, and can be used on an individual basis for encrypting personal files. Encryption is designed to make files only accessible to the one who had them encrypted. Full disk encryption and intelligent file/folder encryption take the encryption decision entirely out of the user's hands. Full disk is more comprehensive and encrypts the entire disk, including operating systems and files.

Q: What if it isn't possible for us to encrypt portable devices such as my cell phone or iPhone?

A: If it is not possible for you to encrypt such portable devices, then personal information should not be transmitted through such device. Encryption of data on devices such as blackberries and other PDAs is becoming more technically feasible. Check with your IT department to see whether your organization is utilizing such technology.

Q: We use email frequently for business, which includes sending and receiving personal information. Do we need to encrypt all of our email?

A: While the OCABR states that you need only encrypt your emails "to the extent technically feasible," it also indicates that you must find alternative means of transmitting personal information if email encryption is not feasible. These alternative means may include, for example, (1) a secure website or datasite where data is uploaded and that requires safeguards (such as a username and password); (2) use of password-protected zip files within your emails (caveat: this method only protects the data contained as an attachment, not within the text/body of the email so consider utilizing this method if the personal information is only contained in the attached document); (3) a mandatory transport layer security (TLS) link, which provides security for email communication; or (4) a virtual private network (VPN) link, which can be used to encrypt all types of Internet communication between organizations (not just email).

Q: If you are the recipient of an email that contains personal information but such email is not encrypted, what is your responsibility?

A: The Regulations apply to all businesses that "receive" personal information, but suggest that the data must be encrypted only if it "will" be transmitted across public networks or stored on a portable device. Better practice is to set up an alternative means of transmission, such as those outlined in the previous Q&A.

Q: Our organization has retained backup tapes. Are we required to encrypt these tapes?

A: Backup tapes must be encrypted as they are being created, but tapes existing prior to March 1, 2010 need not be pulled up from storage and encrypted unless they are transported from your current storage elsewhere. In that event, backup tapes should be encrypted prior to transfer if technically feasible (i.e. the tape allows it); if not, you must take appropriate steps to safeguard the tapes, such as using an armored vehicle with guards, etc.

- **Oversee third-party service providers**. You must take all reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect personal information consistent with state and federal law.

  As you enter into new contracts, you must include language in the contract by which your third-party provider warrants to you its obligations to implement and maintain such appropriate security measures for personal information. You may also wish to include remedies in the event of the third-party provider's breach of its security obligations, such as liquidated damages and indemnification obligations. You may wish to include other protective provisions in the contract, including requirements that your third-party provider maintain adequate levels of insurance and that the third-party provider provide you with prompt notice in the event of a suspected or known security breach.

  If you have ongoing relationships and/or contracts with third-party service providers, the Regulations provide a "grandfathering" exemption for any third-party service provider contracts entered into prior to March 1, 2012. Those contracts will be deemed to be in compliance with the Regulations even without a clause that requires the third-party service provider to maintain appropriate security measures, so long as the contact was entered into *prior to March 1, 2010*. This eliminates any need, as may have been the case under the prior regulations that would have caused companies to retroactively modify existing third-party service provider contracts. Notwithstanding this provision, you are still required and responsible for selecting third-party service providers that are capable of maintaining appropriate security measures to protect personal information consistent with state and federal law.

- **Provide ongoing training and monitoring**. All of your employees should be educated on the Regulations. Require employees to sign a compliance/acknowledgment certificate with your policy/plan upon hiring (and in adopting your written policy). A sample acknowledgment form is attached to this Guide as **Exhibit C**. Design and document a training program to familiarize the employees with your data protection policy. Include required annual training sessions to address the security practices and procedures, reporting procedures and any updates to your organization's policies. Require employees to sign a certificate of attendance/completion upon completion of training programs. A sample certificate of attendance/training completion is attached to this Guide as **Exhibit D**.

- **Comply with other data security regimes**. Compliance with the Regulations should be viewed in the broad context of the many other state and federal regimes concerning data security. Other data privacy regimes may include federal, state and international laws and regulations. In addition to the Gramm-Leach-Bliley Act's "Safeguards Rule," HIPAA's "Security Rule," and the FTC's "Red Flag Rule," many states now require, or have pending legislation that would require, companies to take data security measures. Organizations should be sure to engage in data security "best practices" and to comply with all state and federal regimes to which they are subject. Special rules also may apply with respect to information transmitted across international lines. For instance, the European Union has stringent data protection requirements that only a handful of non-European Union countries (but *not* the United States) currently meet, such as Argentina, Canada, Switzerland and Hungary. Personal data sent from the European Union to the United States must comply with cross-border transfer restrictions. Your organization

must assess where your personal information resides, whether you will be transmitting or receiving information from other states or other countries, and whether you are in compliance with those regimes.

- **Discuss any questions with your lawyer.** If you do not know whether you are in legal compliance with the Regulations, contact your lawyer at Morgan Lewis.

Contacts

If you have any questions or would like more information on the issues discussed in this White Paper, please contact the author:

Washington, DC
Ronald Del Sesto, Jr. +1.202.373.6023 ronald.delsesto@morganlewis.com

About Morgan, Lewis & Bockius LLP

Founded in 1873, Morgan Lewis offers more than 2,200 lawyers, patent agents, benefits advisers, regulatory scientists, and other specialists in 30 offices* across North America, Asia, Europe, and the Middle East. The firm provides comprehensive litigation, corporate, transactional, regulatory, intellectual property, and labor and employment legal services to clients of all sizes—from globally established industry leaders to just-conceived startups. For more information about Morgan Lewis or its practices, please visit us online at www.morganlewis.com.

*Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan Lewis operates through Morgan, Lewis & Bockius, which is a separate Hong Kong general partnership registered with The Law Society of Hong Kong as a registered foreign law firm operating in Association with Luk & Partners.

Reference Materials

Exhibit A 201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth

Exhibit B FAQs Regarding 201 CMR 17.00

Exhibit C Sample Acknowledgment Form

Exhibit D Sample Certificate of Attendance/Training Completion

EXHIBIT A

201 CMR 17.00: STANDARDS FOR THE PROTECTION OF PERSONAL INFORMATION OF RESIDENTS OF THE COMMONWEALTH

Sections:

17.1 Purpose and Scope

Purpose

This regulation implements the provisions of M.G.L. c. 93H relative to the standards to be met by persons who own or license personal information about a resident of the Commonwealth of Massachusetts. This regulation establishes minimum standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records. The objectives of this regulation are to insure the security and confidentiality of customer information in a manner fully consistent with industry standards; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer.

Scope

The provisions of this regulation apply to all persons that own or license personal information about a resident of the Commonwealth.

17.2 Definitions

The following words as used herein shall, unless the context requires otherwise, have the following meanings:

Breach of security, the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth. A good faith but unauthorized acquisition of personal information by a person or agency, or employee or agent thereof, for the lawful purposes of such person or agency, is not a breach of security unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure.

Electronic, relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities.

Encrypted, the transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key.

Owns or licenses, receives, stores, maintains, processes, or otherwise has access to personal information in connection with the provision of goods or services or in connection with employment.

Person, a natural person, corporation, association, partnership or other legal entity, other than an agency, executive office, department, board, commission, bureau, division or authority of the Commonwealth, or any of its branches, or any political subdivision thereof.

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.

Record or Records, any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics.

Service provider, any person that receives, stores, maintains, processes, or otherwise is permitted access to personal information through its provision of services directly to a person that is subject to this regulation.

17.3 Duty to Protect and Standards for Protecting Personal Information

- Every person that owns or licenses personal information about a resident of the Commonwealth shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to (a) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program; (b) the amount of resources available to such person; (c) the amount of stored data; and (d) the need for security and confidentiality of both consumer and employee information. The safeguards contained in such program must be consistent with the safeguards for protection of personal information and information of a similar character set forth in any state or federal regulations by which the person who owns or licenses such information may be regulated.
- Without limiting the generality of the foregoing, every comprehensive information security program shall include, but shall not be limited to:

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

  (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:

    - ongoing employee (including temporary and contract employee) training;
    - employee compliance with policies and procedures; and

- means for detecting and preventing security system failures.

(c) Developing security policies for employees relating to the storage, access and transportation of records containing personal information outside of business premises.

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

(e) Preventing terminated employees from accessing records containing personal information.

(f) Oversee service providers, by:

- Taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such personal information consistent with these regulations and any applicable federal regulations; and

- Requiring such third-party service providers by contract to implement and maintain such appropriate security measures for personal information; provided, however, that until March 1, 2012, a contract a person has entered into with a third party service provider to perform services for said person or functions on said person's behalf satisfies the provisions of 17.03(2)(f)(2) even if the contract does not include a requirement that the third party service provider maintain such appropriate safeguards, as long as said person entered into the contract no later than March 1, 2010.

(g) Reasonable restrictions upon physical access to records containing personal information,, and storage of such records and data in locked facilities, storage areas or containers.

(h) 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.

(i) 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.

(j) 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.

17.4 Computer System Security Requirements

Every person that owns or licenses 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, and to the extent technically feasible, shall have the following elements:

(a) Secure user authentication protocols including:

- control of user IDs and other identifiers;

- a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;
- control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;
- restricting access to active users and active user accounts only; and
- blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;

(b) Secure access control measures that:

- restrict access to records and files containing personal information to those who need such information to perform their job duties; and
- assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls;

(c) Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly.

(d) Reasonable monitoring of systems, for unauthorized use of or access to personal information;

(e) Encryption of all personal information stored on laptops or other portable devices;

(f) For files containing personal information on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information.

(g) Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably 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 is set to receive the most current security updates on a regular basis.

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

17.5 Compliance Deadline

Every person who owns or licenses personal information about a resident of the Commonwealth shall be in full compliance with 201 CMR 17.00 on or before March 1, 2010.

REGULATORY AUTHORITY

201 CMR 17.00: M.G.L. c. 93H

EXHIBIT B

COMMONWEALTH OF MASSACHUSETTS
OFFICE OF CONSUMER AFFAIRS AND BUSINESS REGULATION
10 Park Plaza – Suite 5170, Boston MA 02116
(617) 973-8700 FAX (617) 973-8799
www.mass.gov/consumer

DEVAL L. PATRICK
GOVERNOR

TIMOTHY P. MURRAY
LIEUTENANT GOVERNOR

GREGORY BIALECKI
SECRETARY OF HOUSING AND ECONOMIC DEVELOPMENT

BARBARA ANTHONY
UNDERSECRETARY

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.

I password protect data when storing it on my laptop and when transmitting it wirelessly. Is that enough to satisfy the encryption requirement?

No. 201 CMR 17.00 makes clear that encryption must bring about a "*transformation* of data into a form in which meaning cannot be assigned" (emphasis added). This is to say that the data must be *altered* into an unreadable form. Password protection does not *alter* the condition of the data as required, and therefore would not satisfy the encryption standard.

I am required by law to contract with a specific third party service provider, not necessarily of my choosing. Must I still perform due diligence in the selection and retention of that specific third party service provider?

Where state or federal law or regulation requires the use of a specific third party service provider, then the obligation to select and retain would effectively be met.

November 3, 2009

EXHIBIT C

[YOUR ORGANIZATION]

[Information Security Policy]
CONFIDENTIAL
SAMPLE Acknowledgment

After you have reviewed the Policy, please fill in your name, title and signature in the spaces indicated below and return this Acknowledgement to _____.

I acknowledge that I have received a copy of [Organization's] Information Security Policy effective_____, 20__. I have reviewed the Policy and have familiarized myself with the policies and procedures described therein.

I understand that the Policy supersedes and replaces any prior materials addressing [Organization's] policies and procedures regarding the protection of personal information and that the Policy may be updated from time to time.

I agree to abide by the Policy, as may be updated from time to time. In addition, I attach hereto as Annex A a true and complete list of all locations where [Organization's] personal information is maintained by me or on my behalf as of the date hereof.

Name:_____

Signature: _____

Title: _____

Date: _____

****

RECEIVED BY ORGANIZATION:

Name: _____

Signature: _____

Title: _____

Date: _____

Annex A

CONFIDENTIAL

The following is a true and accurate list of locations where personal information of [Organization] is currently maintained by me or on my behalf:

Hard Copy or Tangible Forms of Information

- Office file cabinets
- Home office file cabinets
- Other location file cabinets

Describe: _____

- Other type of hard copy or tangible forms

Describe: _____

Electronic Forms of Information

- Office "desktop" computer
- Office email
- Organization-owned PDA or other device
- Home office, non-"Organization-owned" "desktop" computer
- Personal email
- Personal, non-"Organization-owned" PDA or other device
- Other electronic forms of information

Describe: _____

Travel/Transport

- I travel outside of the organization's premises with either hard copy or electronic data that may contain personal information.

Describe: _____

EXHIBIT D

[YOUR ORGANIZATION]

SAMPLE CERTIFICATE OF ATTENDANCE/TRAINING COMPLETION

INFORMATION SECURITY TRAINING PROGRAM

Training Provider (if different than ORGANIZATION): _____

Date and Time of Training: _____

Location: _____

Length of Training: _____

Training Modules Covered: [describe or attach] _____

To be completed by Employee:

By signing below, I certify that I participated in the training described above.

Name: _____

Signature: _____

Title: _____

Date: _____

****

Acknowledged by ORGANIZATION:

Name: _____

Signature: _____

Title: _____

Date: _____