ANNA MARIA COLLEGE
INFORMATION SECURITY PLAN

I. OBJECTIVE:

This information security plan ("ISP Plan") creates effective administrative, technical and physical safeguards for the protection of personal information ("PI") of our employees and students, and complies with our obligations under 201 CMR 17.00. The ISP Plan sets forth our procedures for evaluating our electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting personal information of employees and students. "Personal Information" means an employee's, student's or parent'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 him/her: (a) Social Security Number; (b) driver's license number or state-issued identification card number; (c) financial account number, or credit/debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to an employee's or student's financial account. However, PI does not include publicly available information, or from federal, state or local government records lawfully made available to the general public.

II. PURPOSES:

The purpose of the ISP Plan is to:

a. Ensure the security and confidentiality of PI;
b. Protect against any anticipated threats or hazards to the security or integrity of such information; and
c. Protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft or fraud.

III. SCOPE:

In formulating and implementing the ISP Plan, we will (1) identify reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing PI; (2) assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the PI; (3) evaluate the sufficiency of existing policies, procedures, customer information systems, student information systems, and other safeguards in place to control risks; (4) design and implement a plan that puts safeguards in place to minimize those risks, consistent with the requirements of 201 CMR 17.00 (Appendix A); and (5) regularly monitor the effectiveness of those safeguards.

IV. DATA SECURITY COORDINATOR:

The College has designated Michael Miers, Chief Information Officer, to implement, supervise, and maintain the ISP Plan. That designated employee (the "Data Security Coordinator") will be responsible for:

a. Initial implementation of the ISP Plan;

b. Training employees (Training Quick Reference – Appendix F);
c. Regular testing of the ISP Plan's safeguards;
d. Evaluating the ability of service providers to comply with 201 CMR 17.00 in the handling of PI to which we are responsible, ensuring that there are included in our contracts with those service providers provisions obligating them to comply with 201 CMR 17.00 in providing the contracted for services, and obtaining from such service providers written certification that such service provider has a written, comprehensive information security program that is in compliance with the provisions of 201 CMR 17.00.
e. Reviewing the scope of the security measures in the ISP Plan at least annually, or whenever there is a material change in our business practices that affects the security of records containing PI.
f. Conducting an annual training session for all managers, employees and independent contractors, including temporary and contract employees who have access to PI on the elements of the ISP Plan. All attendees at such training sessions are required to certify their attendance at the training, and their familiarity with the college's requirements for ensuring the protection of PI.

V. INTERNAL RISKS:

To combat internal risks to the security, confidentiality, and/or integrity of any electronic, paper, or other records containing PI, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures are mandatory and are effective immediately.

The amount of PI collected must be limited to that amount reasonably necessary to accomplish our legitimate business purposes, or necessary to us to comply with other state or federal regulations.

- Access to records containing PI shall be limited to those persons who are reasonably required to know such information in order to accomplish their legitimate business purpose or to enable us to comply with other state or federal regulations (Department/Vendor Data Access Survey – Appendix D).
- Electronic access to user identification after multiple unsuccessful attempts to gain access must be blocked.
- All security measures shall be reviewed at least annually, or whenever there is a material change in our business practices that implicates the security of records containing PI. The Data Security Coordinator is responsible for this review and shall fully apprise management of the results of that review and any recommendations for improved security arising out of that review.
- Terminated employees must return all records containing PI, in any form, in their possession (including all such information stored on laptops or other portable devices or media and in files, records, work papers, etc.).
- A terminated employee's physical and electronic access to PI must be immediately blocked. Such terminated employee shall be required to surrender all keys, ID's or access codes or badges, business cards, and the like, that permit access to the college's premises or information. Moreover, such terminated employee's remote electronic access to PI must be disabled; his/her voicemail access, e-mail access, internet access, and passwords must be invalidated. The Data Security Coordinator shall maintain a highly secured master list of all lock combinations, passwords and keys (See Procedure for Exiting Employees – Appendix E).

- Current employees' user-IDs and passwords must be changed periodically.
- Access to PI is restricted to active users and active user accounts only.
- Employees should report any suspicious or unauthorized use of PI to the Data Security Coordinator who will follow-up with the appropriate procedures.
- Whenever there is an incident that requires notification (See Sample Letters – Appendix G) under M.G.L. c. 93H, §3 (Appendix B), there shall be an immediate mandatory post-incident review of events and actions taken, if any, with a view to determining whether any changes in our security practices are required to improve the security of PI for which we are responsible.
- Employees are prohibited from keeping open files containing PI on their desks when they are not at their desks.
- At the end of the work day, all files and other records containing PI must be secured in a manner that is consistent with the ISP Plan's rules for protecting the security of PI.
- Each department shall develop rules (bearing in mind the business needs of that department) that ensure that reasonable restrictions upon physical access to records containing PI are in place, including a written procedure that sets forth the manner in which physical access to such records in that department is to be restricted; and each department must store such records and data in locked facilities, secure storage areas or locked containers.
- Access to electronically stored PI shall be electronically limited to those employees having a unique log-in ID; and a re-log-in shall be required when a computer has been inactive for more than a few minutes.
- Paper or electronic records (including records stored on hard drives or other electronic media) containing PI shall be disposed of only in a manner that complies with M.G.L. c. 93I, §2 (Appendix C).

VI. EXTERNAL RISKS

To combat external risks to the security and confidentiality of electronic, paper, or other records containing PI, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures are mandatory and are effective immediately.

- There must be a reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the PI, installed on all systems processing PI.
- There must be reasonably up-to-date versions of system security agent software, which must include malware protection and reasonably up-to-date patches and virus definitions, installed on all systems processing PI.
- To the extent technically feasible, all PI stored on laptops or other portable devices must be encrypted, as must all records and files transmitted across public networks or wirelessly, to the extent technically feasible. Encryption here means the transformation of data through the use of an algorithmic process, or an alternative method at least as secure, into a form in which meaning cannot be assigned without the use of a confidential process or key, unless further defined by regulation by the Office of Consumer Affairs and Business Regulation.
- All computer systems must be monitored for unauthorized use of or access to PI.
- There must be secure user authentication protocols in place, including: (1) protocols for control of user IDs and other identifiers; (2) a reasonably secure method of assigning and selecting passwords; (3) 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; (4)

restriction of access to active users and active user accounts only; and (5) blocking of access to user identification after multiple unsuccessful attempts.

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

Section:

17.1 Purpose and Scope

(1) 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.

(2) 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

(1) 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.

(2) 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:
1. ongoing employee (including temporary and contract employee) training;
2. employee compliance with policies and procedures; and
3. 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:
1. 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
2. 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:
(1) Secure user authentication protocols including:
(a) control of user IDs and other identifiers;
(b) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;
(c) 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;
(d) restricting access to active users and active user accounts only; and
(e) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;
(2) Secure access control measures that:
(a) restrict access to records and files containing personal information to those who need such information to perform their job duties; and
(b) 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;
(3))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.
(4) Reasonable monitoring of systems, for unauthorized use of or access to personal information;
(5) Encryption of all personal information stored on laptops or other portable devices;
(6) 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.
(7) 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.
(8) 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

(1)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

M.G.L. 93H: §3.
DUTY TO REPORT KNOWN SECURITY BREACHES
OR UNAUTHORIZED USE OF PERSONAL INFORMATION

[Text of section added by 2007, 82, Sec. 16 effective October 31, 2007.]

Section 3. (a) A person or agency that maintains or stores, but does not own or license data that includes personal information about a resident of the commonwealth, shall provide notice, as soon as practicable and without unreasonable delay, when such person or agency (1) knows or has reason to know of a breach of security or (2) when the person or agency knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose, to the owner or licensor in accordance with this chapter. In addition to providing notice as provided herein, such person or agency shall cooperate with the owner or licensor of such information. Such cooperation shall include, but not be limited to, informing the owner or licensor of the breach of security or unauthorized acquisition or use, the date or approximate date of such incident and the nature thereof, and any steps the person or agency has taken or plans to take relating to the incident, except that such cooperation shall not be deemed to require the disclosure of confidential business information or trade secrets, or to provide notice to a resident that may have been affected by the breach of security or unauthorized acquisition or use. (b) A person or agency that owns or licenses data that includes personal information about a resident of the commonwealth, shall provide notice, as soon as practicable and without unreasonable delay, when such person or agency (1) knows or has reason to know of a breach of security or (2) when the person or agency knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose, to the attorney general, the director of consumer affairs and business regulation and to such resident, in accordance with this chapter. The notice to be provided to the attorney general and said director, and consumer reporting agencies or state agencies if any, shall include, but not be limited to, the nature of the breach of security or unauthorized acquisition or use, the number of residents of the commonwealth affected by such incident at the time of notification, and any steps the person or agency has taken or plans to take relating to the incident.

Upon receipt of this notice, the director of consumer affairs and business regulation shall identify any relevant consumer reporting agency or state agency, as deemed appropriate by said director, and forward the names of the identified consumer reporting agencies and state agencies to the notifying person or agency. Such person or agency shall, as soon as practicable and without unreasonable delay, also provide notice, in accordance with this chapter, to the consumer reporting agencies and state agencies identified by the director of consumer affairs and business regulation.

The notice to be provided to the resident shall include, but not be limited to, the consumer's right to obtain a police report, how a consumer requests a security freeze and the necessary information to be provided when requesting the security freeze, and any fees required to be paid to any of the consumer reporting agencies, provided however, that said notification shall not include the nature of the breach or unauthorized acquisition or use or the number of residents of the commonwealth affected by said breach or unauthorized access or use.

(c) If an agency is within the executive department, it shall provide written notification of the nature and circumstances of the breach or unauthorized acquisition or use to the information technology division and the division of public records as soon as practicable and without unreasonable delay following the discovery of a breach of security or unauthorized acquisition or use, and shall comply with

all policies and procedures adopted by that division pertaining to the reporting and investigation of such an incident.

M.G.L. 93I: §2.
STANDARDS FOR DISPOSAL OF RECORDS CONTAINING
PERSONAL INFORMATION; DISPOSAL BY THIRD PARTY; ENFORCEMENT

[Text of section added by 2007, 82, Sec. 17 effective February 3, 2008. See 2007, 82, Sec. 19.]

Section 2. When disposing of records, each agency or person shall meet the following minimum standards for proper disposal of records containing personal information:

(a) paper documents containing personal information shall be either redacted, burned, pulverized or shredded so that personal data cannot practicably be read or reconstructed;

(b) electronic media and other non-paper media containing personal information shall be destroyed or erased so that personal information cannot practicably be read or reconstructed.

Any agency or person disposing of personal information may contract with a third party to dispose of personal information in accordance with this chapter. Any third party hired to dispose of material containing personal information shall implement and monitor compliance with policies and procedures that prohibit unauthorized access to or acquisition of or use of personal information during the collection, transportation and disposal of personal information.

Any agency or person who violates the provisions of this chapter shall be subject to a civil fine of not more than $100 per data subject affected, provided said fine shall not exceed $50,000 for each instance of improper disposal. The attorney general may file a civil action in the superior or district court in the name of the commonwealth to recover such penalties.

Anna Maria College
Department Data Access Survey

Document Name	Document Content	Users w/ Access	Can Info Be Eliminated?	Paper	Electronic	How Is Data Secured?

Anna Maria College
Vendor Data Access Survey

Vendor Name	Vendor Access Level	Vendor Contract?	Can Access Be Eliminated?	Paper	Electronic	How Is Data Secured?

Prepared by: Michael Miers
Approved by: Stephen Neun
Date: April, 7, 2009
Revised Date: April 7, 2009

IT Procedure For Exiting Employees

I. PURPOSE:

The purpose of this procedure is to:

a. Provide information on the steps taken when an employee leaves the College.
b. Ensure the security and confidentiality of the employee's data.
c. Protect against any unauthorized access to college resources.
d. Maintain compliance with Federal, State and College regulations and guidelines.

II. SCOPE:

In formulating this procedure we will be providing the steps taken by the Information Technology Department when an employee leaves the College to ensure the protection of that employee's information, as well as maintain compliance with existing Federal, State and College policies.

III. PROCEDURES:

The procedures to be followed are:

a. A representative from Human Resources informs IT that an employee will be leaving/has left the College.
b. The user's passwords to all systems (login, email, web and Empower) will be changed.
c. An auto-responder for that user's email account will be set up.
d. The user's accounts will be disabled.
e. All external access to college systems will be terminated (where applicable)
f. Shared department passwords will be changed to maintain security and reliability of data (where applicable).
g. A backup of the user's data to be accessed only by the department head until mission critical data is recovered and placed on a shared resource for other members of the department (at the discretion of the department head) will be created.
h. Voicemail will be cleared out and reset to 1111.
i. All phone calls will be forwarded to another individual in the department (chosen by the department head).
j. The physical computer will be collected and stored by a member of ITS, if necessary.

Anna Maria College
Training Quick Reference

I. PURPOSE:

The purpose of this document is to:

a) Define variables that are being used in the Massachusetts Data Security Regulations, as well as those variables adapted by the College for this purpose.
b) Develop a simple FAQ for the representatives from each Department that will be charged with completing the Data/Vendor surveys.

II. SCOPE:

This document will serve as a quick reference for variable definitions, as well as a place for frequently asked questions (FAQ's) based off of the Massachusetts Data Security Regulations (201 CMR 17.00) as well the Duty to Report Known Security Breaches or Unauthorized Use of Personal Information (M.G.L. 93H: §3).

III. REFERENCES:

Variables:

"Breach of security" – As defined by the State of Massachusetts, a 'security breach' is 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.

"Data Security Coordinator" – This person, assigned by the College, is responsible for the initial implementation of the ISP Plan, training employees, regular testing of safeguards, evaluating the ability of service providers to comply with the ISP Plan and reviewing the scope of the ISP Plan at least annually.

"Electronic" – Consists of anything relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities.

"Encrypted" – Means the transformation of data through the use of a 128-bit or higher algorithmic process, or other means or process approved by the office of consumer affairs and business regulation that is at least as secure as such algorithmic process, into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

"ISP Plan" or "The Plan" – This refers to the Information Security Plan. The ISP Plan is an extensive document that contains all the information regarding the Massachusetts Data Security Regulations as well as the Duty to Report Known Security Breaches or Unauthorized Use of Personal Information.

"Person" – Is 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" – As defined by the State of Massachusetts, 'personal information' is to be defined as an employee's, student's, or parent'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 him/her: (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 an employee's or student's financial account; However, "personal information" does not include publicly available information, or from federal, state or local government records lawfully made available to the general public (of a Massachusetts resident only).

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

FAQ:

Does this law trump Federal laws such as FERPA or HIPPA?

No. These are State law which all business must be in compliance with. The College still needs to abide by all regulations set forth by the Federal Government (such as FERPA, HIPPA, or FACTA).

How long do I need to keep documents containing "personal information"?

This varies among departments. Please contact your department/division head who will let you know how long documents need to be kept (based off of State/Federal laws).

I am hiring a new vendor, what do I need to do?

You will need to contact the Data Security Coordinator, Human Resources, or your Department Head to have the vendor agree and sign the *Vendor Compliance Form*.

I no longer need a document that contains personal information, what do I do?

You need to dispose of that document in the appropriate manner (i.e. shredding). Before shredding any document, you must make sure that that document is not required for record-keeping purposes. If you have any questions regarding whether or not you should dispose of a document, please contact your department head.

What do I do if I witness a breach?

Contact the Data Security Coordinator immediately; he/she will then follow the appropriate protocols as laid out by the State of Massachusetts.

What type of document is covered under this law?

All documents whether paper or electronic are covered under 201 CMR 17.00. Even a post-it note with personal information written on it, is covered.

Who is the Data Security Coordinator?

The Data Security Coordinator for Anna Maria College is Michael Miers, Director of Information Technology.

Date:

Attorney General Martha Coakley
Office of the Attorney General
One Ashburton Place
Boston, MA 02108

Dear Attorney General Coakley:

Pursuant to M.G.L. c. 93H, we are writing to notify you of [a breach of security/an unauthorized access or use of personal information] involving [number] Massachusetts resident[s].

NATURE OF THE SECURITY BREACH OR UNAUTHORIZED USE OR ACCESS

[This paragraph should provide the date of the incident, a summary of the nature of the incident, a description of the categories of personal information involved in the incident, and whether the personal information that was the subject of the incident was in electronic or paper form].

NUMBER OF MASSACHUSETTS RESIDENTS AFFECTED

[This paragraph should specify the number of affected individuals residing in Massachusetts whose personal information was the subject of the incident. This paragraph should also indicate that these Massachusetts residents have received or will shortly receive notice pursuant to M.G.L. c.93H, s. 3(b) and should specify the manner in which Massachusetts residents have or will receive such notice. You should also include a copy of the notice to affected Massachusetts residents in your notification to the Attorney General].

STEPS YOU HAVE TAKEN OR PLAN TO TAKE RELATING TO THE INCIDENT

[This paragraph should outline all the steps you have taken or plan to take relating to the incident including, without limitation, what you did when you discovered the incident; whether you have reported the incident to law enforcement; whether you have any evidence that the personal information has been used for fraudulent purposes; whether you intend to offer credit monitoring services to consumers; and what measures you have taken to ensure that similar incidents do not occur in the future].

OTHER NOTIFICATION AND CONTACT INFORMATION

[Finally, you letter should indicate whether you have provided similar notification to the Director of Consumer Affairs and Business Regulation. You should also include the name and contact information for the person whom the Office of the Attorney General may contact if they have any questions or need further information].

Date:

Person's Name
Address
City, MA Zip

Dear _____:

We are writing to notify you that a [breach of security/unauthorized acquisition or use] of your personal information occurred on [date(s)].

THE NOTICE MUST INCLUDE THE FOLLOWING INFORMATION

Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Massachusetts law also allows consumers to place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services.

If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $5.00 each to place, temporarily lift, or permanently remove a security freeze.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com) by regular, certified or overnight mail at the addresses below:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013

Trans Union Security Freeze
Fraud Victim Assistance Department
P.O. Box 6790
Fullerton, CA 92834

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc);

2. Social Security Number;
3. Date of birth
4. If you have moved in the past five (5) years, provide the address where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issues identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entry or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report of the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each other the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

If you should have any further questions, please contact [provide contact information for the College].

Sincerely,

CONTACT

CHARLES D. BAKER
GOVERNOR

KARYN E. POLITO
LIEUTENANT GOVERNOR

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

JAY ASH
SECRETARY OF HOUSING AND ECONOMIC DEVELOPMENT

JOHN C. CHAPMAN
UNDERSECRETARY

201 CMR 17.00 COMPLIANCE CHECKLIST

The Office of Consumer Affairs and Business Regulation has compiled this checklist to help small businesses in their effort to comply with 201 CMR 17.00. **This Checklist is not a substitute for compliance with 201 CMR 17.00**. Rather, it is designed as a useful tool to aid in the development of a written information security program for a small business or individual that handles "personal information." Each item, presented in question form, highlights a feature of 201 CMR 17.00 that will require proactive attention in order for a plan to be compliant.

The Comprehensive Written Information Security Program (WISP)

- ⌋ Do you have a comprehensive, written information security program ("WISP") applicable to all records containing personal information about a resident of the Commonwealth of Massachusetts ("PI")?
- ⌋ Does the WISP include administrative, technical, and physical safeguards for PI protection?
- ⌋ Have you designated one or more employees to maintain and supervise WISP implementation and performance?
- ⌋ Have you identified the paper, electronic and other records, computing systems, and storage media, including laptops and portable devices that contain personal information?
- ⌋ Have you chosen, as an alternative, to treat all your records as if they all contained PI?
- ⌋ Have you identified and evaluated reasonably foreseeable internal and external risks to paper and electronic records containing PI?
- ⌋ Have you evaluated the effectiveness of current safeguards?
- ⌋ Does the WISP include regular ongoing employee training, and procedures for monitoring employee compliance?

- ⎦ Does the WISP include disciplinary measures for violators?

- ⎦ Does the WISP include policies and procedures for when and how records containing PI should be kept, accessed or transported off your business premises?

- ⎦ Does the WISP provide for immediately blocking terminated employees, physical and electronic access to PI records (including deactivating their passwords and user names)?

- ⎦ Have you taken reasonable steps to select and retain a third-party service provider that is capable of maintaining appropriate security measures consistent with 201 CMR 17.00?

- ⎦ Have you required such third-party service provider by contract to implement and maintain such appropriate security measures?

- ⎦ Is the amount of PI that you have collected limited to the amount reasonably necessary to accomplish your legitimate business purposes, or to comply with state or federal regulations?

- ⎦ Is the length of time that you are storing records containing PI limited to the time reasonably necessary to accomplish your legitimate business purpose or to comply with state or federal regulations?

- ⎦ Is access to PI records limited to those persons who have a need to know in connection with your legitimate business purpose, or in order to comply with state or federal regulations?

- ⎦ In your WISP, have you specified the manner in which physical access to PI records is to be restricted?

- ⎦ Have you stored your records and data containing PI in locked facilities, storage areas or containers?

- ⎦ Have you instituted a procedure for regularly monitoring to ensure that the WISP is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of PI; and for upgrading it as necessary?

- ⎦ Are your security measures reviewed at least annually, or whenever there is a material change in business practices that may affect the security or integrity of PI records?

- ⎦ Do you have in place a procedure for documenting any actions taken in connection with any breach of security; and does that procedure require post-incident review of events and actions taken to improve security?

Additional Requirements for Electronic Records

- ⎦ Do you have in place secure authentication protocols that provide for:

- Control of user IDs and other identifiers?
- A reasonably secure method of assigning/selecting passwords, or for use of unique identifier technologies (such as biometrics or token devices)?
- Control of data security passwords such that passwords are kept in a location and/or format that does not compromise the security of the data they protect?
- Restricting access to PI to active users and active user accounts?
- Blocking access after multiple unsuccessful attempts to gain access?

⎦ Do you have secure access control measures that restrict access, on a need-to-know basis, to PI records and files?

⎦ Do you assign unique identifications plus passwords (which are not vendor supplied default passwords) to each person with computer access; and are those IDs and passwords reasonably designed to maintain the security of those access controls?

⎦ Do you, to the extent technically feasible, encrypt all PI records and files that are transmitted across public networks, and that are to be transmitted wirelessly?

⎦ Do you, to the extent technically feasible, encrypt all PI stored on laptops or other portable devices?

⎦ Do you have monitoring in place to alert you to the occurrence of unauthorized use of or access to PI?

⎦ On any system that is connected to the Internet, do you have reasonably up-to-date firewall protection for files containing PI; and operating system security patches to maintain the integrity of the PI?

⎦ Do you have reasonably up-to-date versions of system security agent software (including malware protection) and reasonably up-to-date security patches and virus definitions?

⎦ Do you have in place training for employees on the proper use of your computer security system, and the importance of PI security?

CHARLES D. BAKER
GOVERNOR

KARYN E. POLITO
LIEUTENANT GOVERNOR

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

JAY ASH
SECRETARY OF HOUSING AND ECONOMIC DEVELOPMENT

JOHN C. CHAPMAN
UNDERSECRETARY

Frequently Asked Questions 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 riskbased 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." 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.