INFORMATION SECURITY PLAN

[This document is intended to help you create a written information security plan for your organization which complies with Massachusetts law and regulation. Instructions and/or comments are set off in brackets and are italicized and bolded. While this document addresses issues that are common to insurance organizations, there is no one-size-fits-all plan, and it is recommended that you tailor this document to the needs and practices of your business.]

OBJECTIVE

This Information Security Plan (the "Plan") is intended to create effective administrative, technical and physical safeguards for the protection of personal information of employees who are residents of the Commonwealth of Massachusetts. The Plan sets forth the Organization's procedure for evaluating electronic and physical methods of accessing, collecting, storing, using, transmitting and protecting personal information of residents of the Commonwealth of Massachusetts.

For purposes of this Plan, "personal information" means:

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 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;

The Organization recognizes that, in particular, it possesses the personal information of Massachusetts residents in the following places:

[Assess whether and where your organization may have personal information. Below are common examples of files and data which may exist in your organization. You should include those that apply to your organization and add any additional materials in your possession.]

- hard copy customer and prospective customer files located in ***[file cabinet, file room, desk drawer]***
- electronic customer files located on ***[organization server, computer hard drive, CD-ROM, USB drive, e-mail server or account]***
- electronic customer or driver database located on ***[organization server, computer hard drive]***

- personnel files and benefits information for organization employees located in ***[file cabinet, file room, desk drawer]***

- Form I-9s for organization employees located in a ***[file cabinet, file room, desk drawer]***

- Payroll information for organization employees, including direct deposit information located in ***[file cabinet, file room, desk drawer, hard drive]***

This Plan is intended to protect this information from unauthorized access and/or use.

SCOPE

In formulating and implementing the Plan, we have (1) identified reasonably foreseeable internal and external risks to the security, confidentiality and/or integrity of any electronic, paper or other records containing personal information; (2) assessed the likelihood and potential danger of these threats, taking into consideration the sensitivity of the personal information; (3) evaluated the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to minimize those risks,(4) designed and implemented a plan that puts safeguards in place to minimize those risks, consistent with the requirements of 201 C.M.R. § 17.00, and (5) plan to regularly monitor the effectiveness of those safeguards.

DATA SECURITY COORDINATOR

The Organization has designated _____. as the Data Security Coordinator to implement, supervise and maintain the Plan.

[The Organization needs to designate an individual who will be responsible for the plan. This person needs to have authority to ensure compliance. For larger organizations, the coordinator may need to work with other organization employees to ensure compliance with this plan. The following description should be used for larger organizations:]

The Data Security Coordinator will be responsible for:

1. Initial implementation of the Plan;

2. Training employees;

3. Regular testing of the Plan's safeguards;

4. Evaluating the ability of service providers to comply with the law;

5. Reviewing the scope of the security measures in the Plan at least annually, or whenever there is a material change in business practices affecting the Plan;

6. Conducting an annual training session for all organization employees with access to personal information.

INTERNAL RISKS TO PERSONAL INFORMATION

[For small organizations with few or no employees other than the owner, use the following:]

To combat internal risks to the security, confidentiality and/or integrity of records containing personal information, including any and all customer files, such information should be maintained under lock and key when not being used. If such files need to be transported outside of the Organization, reasonable steps should be taken to maintain the security of the information. Organization computer(s) shall require a user log-in and password, and passwords will be changed periodically. Any employee who terminates his or her employment with the Organization should return all customer records and files, and that individual's access to Organization computers, e-mail or voice mail must be terminated.

[For larger organizations with employees, use all that apply to your business:]

To combat internal risks to the security, confidentiality and/or integrity of records containing personal information, including any and all customer files, the following measures will be taken:

1. Organization employees should access customer files only for legitimate business purposes.

2. Only ***[organization employee responsible]*** shall have access to personnel files, payroll information and employees' benefit information.

3. Files containing personal information should be maintained under lock and key when not in use. If an employee needs to transport records containing personal information outside of the organization premises, reasonable steps should be taken to maintain the security of the information.

4. When it is appropriate to destroy organization records, paper and electronic records containing personal information must be destroyed in a manner in which personal information cannot be read or reconstructed.

5. Organization computers shall require a user ID and password. Current employees' computer user-IDs and passwords will be changed periodically. Electronic access to personal information shall be blocked after multiple unsuccessful attempts to log-in.

6. Terminated employees must: (1) return all records containing personal information, in any form (including all such information stored on laptops or other portable devices or media, and in files, records, work papers, etc.),

(2) return all keys, IDs, access codes and/or badges, (3) be prohibited from accessing personal information and (4) the terminated employee's access to e-mail, voicemail, organization intranet and passwords will be invalidated.

7. Electronic access to personal information shall be restricted to active users and active user accounts only.

8. Employees are encouraged to report any suspicious or unauthorized use of customer information.

9. All security measures contained in this Plan shall be reviewed and reevaluated annually, or whenever there is a material chance in the business.

10. Employees with access to personal information will be trained on this Plan.

11. Organization employees who violate this Plan may be subject to discipline up to and including termination.

[If the Organization provides personal information to a vendor such as a payroll organization, then use the following:]

The Organization should ensure that vendors who are provided personal information have their own compliant written security plan.

EXTERNAL RISKS TO PERSONAL INFORMATION

[For all Organizations]

To minimize external risks to the security, integrity of records containing personal information, including any and all customer files, the following measures will be taken:

1. Visitors to the organization shall not have access to records containing personal information.

[If the Organization maintains computers with access to the Internet or its employees use handheld devices or laptops containing personal information, the following items should be included as applicable to:]

1. The Organization maintains up-to-date firewall protection and operating system security patches.

2. The Organization maintains up-to-date versions of security software, which includes mal-ware protection with up-to-date patches and virus definitions.

3. To the extent technically feasible, personal information stored on laptops or other portable devices in encrypted.

4. To the extent technically feasible, personal information transmitted across public networks or wirelessly is encrypted.

5. Computer systems are monitored for unauthorized use.

6. Secure user protocols are in place, including: (1) protocols for control of user IDs and other identifiers, (2) a secure method of assigning and selecting passwords, and (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.

7. Employee log-ins and passwords are not vendor supplied default log-ins and passwords.

IN THE EVENT A BREACH OF PERSONAL INFORMATION OCCURS

A security breach occurs when there is an unauthorized acquisition or use of personal information of one or more Massachusetts residents. The following measures will be taken by the Organization in the event of a security breach which creates a risk of identity theft to Massachusetts residents:

1. The Organization will notify the Office of Consumer Affairs and Business Regulations (OCABR) and the Attorney General's Office. This notice shall include the nature of the breach, the number of Massachusetts residents affected by the breach and all the steps the organization has taken to rectify the incident and to prevent any further breaches form occurring.

2. The Organization shall also notify the employee(s) or customer(s) affected by the breach. That notice shall include information concerning each resident's right to obtain a police report and how to request a security freeze on their consumer report, but shall not include information regarding the nature of the breach and the number of Massachusetts residents affected.