SAMPLE

HIPAA/HITECH POLICIES AND PROCEDURES
MANUAL FOR THE SECURITY OF ELECTRONIC
PROTECTED HEALTH INFORMATION

Please Note:

1. THIS IS NOT A ONE-SIZE-FITS-ALL OR A FILL-IN-THE BLANK COMPLIANCE PROGRAM. The only purpose of this Sample Manual is to serve as an informational example of a HIPAA/HITECH Security Rule compliance program. It is not intended – and should not be used -- as a “one size fits all” compliance program. The Security Rule is specifically designed to permit some flexibility in compliance so that you can adopt the security measures that are best suited to your particular situation and needs - as long as you meet the Standards specified in the Security Rule. There is no “one-size-fits-all” compliance program. Rather, what you do to come into compliance will depend on the size, complexity, and capabilities of your particular practice.

2. THIS IS NOT LEGAL ADVICE. This Manual is not legal advice, nor should it substitute for legal advice. You should always seek the advice of an attorney before using this sample Manual to develop a compliance program that fits your particular situation and needs.

3. USE THIS IN CONJUNCTION WITH THE GUIDE TO COMPLYING WITH THE HIPAA/HITECH SECURITY RULE. For guidance about the particulars of the HIPAA/HITCH Security Rule and a more detailed explanation of the policies and procedures in this Manual, please refer to a companion document entitled “Physicians’ Guide to Complying with the HIPAA/HITECH Security Rule.”

4. THIS MATERIAL IS THE PROPERTY OF SVMIC AND IS RESTRICTED TO THE USE OF OUR POLICYHOLDERS. Anyone else desiring to use this material may do so only with the express written permission of SVMIC. Any other copying and any distribution, retransmission, linking, or modification of the material, including modification of copyright, trademark, or other proprietary notices, whether such material or information is in electronic or hard copy form, without the express written permission of SVMIC is prohibited.

Copyright © 2011 by SVMIC
SAMPLE HIPAA/HITECH POLICIES AND PROCEDURES
MANUAL FOR THE SECURITY OF ELECTRONIC
PROTECTED HEALTH INFORMATION

As a “covered entity” under HIPAA, [insert name of practice] is required to comply with the provisions of the HIPAA Security Rule, 45 CFR §§164.308 -164.318 (as amended by the HITECH Act), that are applicable to it.

In general, the Security Rule requires us to protect the confidentiality, integrity, and availability of all electronic protected health information (“e-PHI”) that we create, receive, maintain, or transmit by establishing and implementing (1) Administrative Safeguards to protect e-PHI, (2) Physical Safeguards to limit physical access to e-PHI, and (3) Technical Safeguards for electronic information systems that control access to e-PHI. We must also properly document all the policies and procedures that we establish to comply with the Standards, Implementation Specifications, and other requirements of the Security Rule.

To meet our obligations under the Security Rule we have established and implemented the policies and procedures set out in this Manual. All our personnel are required to comply fully with these policies and procedures.

**HIPAA SECURITY OFFICER**

We have designated a HIPAA Security Officer who is primarily responsible for developing and implementing our security policies and procedures and for making sure that we comply with the requirements of the Security Rule.

Any questions or concerns that you have regarding these policies and procedures, their proper implementation, or how to comply with them should be addressed to the Security Officer. If you know of, or suspect that there may be a problem with, or breach of, security, you should report the problem or breach immediately to the Security Officer.

**Security Officer Contact Information:**

Name of Security Officer:__________________________________________________

Office location:____________________________________________________________

Telephone:_______________________________________________________________

E-mail address:____________________________________________________________

Mobile phone:____________________________________________________________

Fax:______________________________________________________________

Address:________________________________________________________________

Copyright © 2011 by SVMIC
I. RISK ANALYSIS

A. Initial Risk Analysis

We have conducted an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of our e-PHI.

1. **When.** Our initial risk analysis was conducted from __________ to __________ 2011.

2. **Who.** The following persons participated in the initial risk analysis, performing the following functions:

<table>
<thead>
<tr>
<th>Name</th>
<th>Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3. **Glossary of Terms.** In conducting our risk analysis, we have used the following definitions of key terms, which are the definitions in the Security Rule or definitions in NIST Special Publication (SP) 800-30.

- **Availability** means that data or information are accessible and useable on demand by an authorized person.

- **Confidentiality** means that data or information are not made available or disclosed to unauthorized persons or processes.

- **E-PHI** is “protected health information” (PHI) that is transmitted or maintained in electronic media. Paper PHI is not covered by the Security Rule. Electronic transmission includes the Internet, extranets, dial-up lines, computer-generated faxes (but not traditional paper-to-paper faxes), private networks, and e-PHI that is physically moved from one location to another using magnetic tape, disk, or compact disc media.

- **Integrity** means that data or information have not been altered or destroyed in an unauthorized manner.
• **Risk** is a function of (1) the likelihood of a given threat triggering or exploiting a particular vulnerability, and (2) the resulting impact on the organization. More technically, risk is the net mission impact considering (1) the probability that a particular threat will exercise (accidentally trigger or intentionally exploit) a particular vulnerability and (2) the resulting impact if this should occur. Risks arise from legal liability or mission loss due to (1) unauthorized (malicious or accidental) disclosure, modification, or destruction of information, (2) unintentional errors and omissions, (3) IT disruptions due to natural or man-made disasters, or (4) failure to exercise due care and diligence in the implementation and operation of the IT system.

• **Threat** is the potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability. Threats may be natural (*e.g.*, floods, earthquakes, tornadoes, landslides), human (*e.g.*, network- and computer-based attacks, malicious software upload, unauthorized access to e-PHI, inadvertent data entry or deletion, inaccurate data entry actions), or environmental (*e.g.*, power failures, pollution, chemicals).

• **Vulnerability** means a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system’s security policy. Vulnerabilities may be technical (*e.g.*, flaw in the development of an information system, an incorrectly configured information system), or nontechnical (*e.g.*, ineffective or non-existent policies, procedures, standards or guidelines).

4. **Data Gathering Methods.** To conduct the initial risk analysis, we have used the following methods of gathering data:

   a. reviewing past and existing projects
   b. conducting interviews
   c. reviewing documents and records
   d. making an inventory of our computer system
   e. ____________________________

   We will use the same or similar methods of gathering data whenever we update our risk analysis.
5. **E-PHI.** We have identified the following e-PHI that we create, receive, maintain or transmit:

a. medical records 

b. __________

c. __________

d. __________

e. __________

6. **Electronic Media.** We have identified the following forms of electronic media on which we create, receive, maintain, or transmit e-PHI at the locations indicated:

<table>
<thead>
<tr>
<th>Medium</th>
<th>Locations</th>
</tr>
</thead>
<tbody>
<tr>
<td>hard drives</td>
<td></td>
</tr>
<tr>
<td>floppy disks</td>
<td></td>
</tr>
<tr>
<td>CDs</td>
<td></td>
</tr>
<tr>
<td>DVDs</td>
<td></td>
</tr>
<tr>
<td>smart cards</td>
<td></td>
</tr>
<tr>
<td>personal digital assistants</td>
<td></td>
</tr>
<tr>
<td>transmission media</td>
<td></td>
</tr>
<tr>
<td>portable electronic media (laptops)</td>
<td></td>
</tr>
<tr>
<td>thumb drives</td>
<td></td>
</tr>
<tr>
<td>networks</td>
<td></td>
</tr>
<tr>
<td>telephones (voicemail)</td>
<td></td>
</tr>
</tbody>
</table>
7. **External Sources of e-PHI.** We have the following external sources of e-PHI, including our vendors or consultants who create, receive, maintain, or transmit e-PHI for us:

____________________________________________________________

____________________________________________________________

8. **E-PHI Locations.** We have the following locations (e.g., offices, workstations) where e-PHI is created, received, maintained, or used:

____________________________________________________________

____________________________________________________________

9. **Threats.** We have identified the following potential, reasonably anticipated natural, environmental, and human threats to our e-PHI:

   a. **Natural Threats** [list all that apply]

      ____________________________________________________________

      ____________________________________________________________

   b. **Environmental Threats** [list all that apply]

      ____________________________________________________________

      ____________________________________________________________

   c. **Human Threats** [list all that apply]

      ____________________________________________________________

      ____________________________________________________________

10. **Vulnerabilities.** We have identified the following vulnerabilities, which, if triggered or exploited by a threat, would create a risk security breach involving e-PHI:

      ____________________________________________________________

      ____________________________________________________________
   a. We have identified the following security measures that we currently use to safeguard e-PHI:

   ______________________________________________________
   ______________________________________________________
   ______________________________________________________

   b. We have assessed whether our current security measures are configured and used properly and have determined that

   ______________________________________________________

12. Likelihood of Threat Occurrence. We have assessed the probability of potential risks to e-PHI, including all threat and vulnerability combinations with associated likelihood estimates that may impact the confidentiality, availability and integrity of our e-PHI, and on the basis of that assessment we have determined that the following threats are the threats that are “reasonably anticipated” and are the threats that we must protect against through appropriate security measures:

   ______________________________________________________
   ______________________________________________________

13. Potential Impact of Threat Occurrence. We have also assessed the “criticality,” or impact, of potential risks to the confidentiality, integrity, and availability of e-PHI by considering the magnitude of the potential impact resulting from a threat triggering or exploiting a specific vulnerability.
   a. To make this assessment we have used the following method:

   ______________________________________________________
   ______________________________________________________ [a qualitative or quantitative method or a combination of the two methods].

   b. We have identified the following potential impacts associated with the occurrence of threats triggering or exploiting vulnerabilities that affect the confidentiality, availability and integrity of our e-PHI:

   ______________________________________________________
   ______________________________________________________
14. We have determined the level of risk for each threat and vulnerability combination that we have identified by analyzing the values assigned to the likelihood of threat occurrence and resulting impact of threat occurrence. [OR describe whatever method you decide to use, for example, assigning a risk level based on the average of the assigned likelihood and impact levels.]

15. As a result of determining the level of risk, we have assigned risk levels for all threat and vulnerability combinations that we identified in our risk analysis. Those risk levels are documented in the attached Risk Determination Table. [See Attachment 1 for sample Risk Determination Table.]

16. We have identified the corrective actions to be performed and measures to be taken to mitigate each risk level. Those corrective actions are documented in the attached Safeguard Determination Table. [See Attachment 1 for sample Safeguard Determination Table.]

B. Periodic and Continuing Risk Analysis.

1. Periodic Risk Analysis. We will perform a risk analysis at least [specify a period, such as once a year, every 6 months].

2. Continuing Risk Analysis As Needed. In addition, we will perform a risk analysis as needed to identify when updates to our security measures are needed. In particular, we will conduct a risk analysis whenever we plan to implement new technologies or business operations, for example if there is a change in ownership, management, or key personnel. Whenever we determine that existing security measures are not sufficient to protect against the risks associated with the evolving threats or vulnerabilities, a changing business environment, or the introduction of new technology, we will determine what additional security measures are needed.
II. ADMINISTRATIVE SAFEGUARDS

As required by the Administrative Safeguard Standards and their respective Implementation Specifications, we have developed and shall implement the following policies and procedures to prevent, detect, contain, and correct security violations with respect to our e-PHI.

A. Security Officer. [This is absolutely required.] We have appointed a HIPAA Security Officer who is responsible for developing and implementing our security policies and procedures. The name and contact information for our Security Officer is on the first page of this Manual.


1. Risk analysis (required). We have conducted an initial risk analysis and shall conduct additional risk assessments periodically and as necessary. Our risk analysis policies and procedures and the results of our initial risk analysis are documented in Section I, above, and in Attachment 1.

2. Risk management (required). We have implemented reasonable and appropriate security measures to reduce the risks and vulnerabilities that we have identified. Those security measures and corrective actions are documented in the attached Safeguard Determination Table (part of Attachment 1).

[OR list the risks you have identified together with an explanation of the measures you have in place to mitigate each risk.]

____________________________________________________________
____________________________________________________________

3. Sanction policy (required). All our personnel and our agents and vendors must comply with our security policies and procedures. Anyone who does not comply with security policies and procedures will be sanctioned in accordance with the following sanction policy:

<table>
<thead>
<tr>
<th>Violation</th>
<th>Sanction</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
We will apply these sanctions equally to all individuals.

4. **Information system activity review (required).** We have implemented the following procedures to review regularly all records of information system activity:

   [Insert description of your review mechanisms, e.g., audit logs, access reports, security incident tracking reports and how/when/by whom they will be reviewed for potential security problems.]

C. **Workforce Security.** We have implemented policies and procedures to ensure that all personnel who need access to e-PHI have appropriate access to e-PHI. We have also put in place procedures to ensure that those who should not have access are unable to access e-PHI.

   1. **Authorization and supervision (addressable).** We have implemented the following procedures to authorize and supervise personnel who work with e-PHI or who work in areas where e-PHI might be accessed:

   [Insert description of your review mechanisms, e.g., audit logs, access reports, security incident tracking reports and how/when/by whom they will be reviewed for potential security problems.]

---

1 Whenever an item is “addressable” rather than “required,” you may tailor your implementation of that item to your individual practice or, in some instances, you may dispense with implementation altogether. You must assess whether the “addressable” item is a reasonable and appropriate safeguard in your particular situation. Ask how likely it is to contribute to protecting your e-PHI. If it is “reasonable and appropriate,” then you must implement it. But if it is not reasonable and appropriate, you may choose either (1) to implement an equivalent reasonable and appropriate measure; or (2) not to implement it, if non-implementation is reasonable. Whatever choice you make, you must document not only that choice but also the rationale, based on risk analysis, for your choice.
2. **Workforce clearance procedure (addressable).** We have implemented the following procedures to determine that employee access to e-PHI is appropriate:

________________________________________________________________________

[Supply details about how you will limit access to e-PHI to only those who have appropriate clearance, such as a background check, and a need to access the e-PHI.]

3. **Termination procedures (addressable):** We have implemented the following procedures for terminating access to e-PHI when a person’s employment or relationship with us ends:

________________________________________________________________________

________________________________________________________________________

D. **Information Access Management.** We have implemented policies and procedures on how our workforce will be given access to e-PHI and how access will be limited when appropriate.

1. **Access authorization (addressable):** We have implemented the following policies and procedures for granting access to e-PHI:

________________________________________________________________________

[Provide details – e.g., by limiting access to workstations or offices where e-PHI is stored.]

2. **Access establishment and modification (addressable):** We have implemented the following policies and procedures to establish, document, review, and modify a user’s right of access to workstations, programs, transactions, records, ____________:

________________________________________________________________________

________________________________________________________________________

[Provide details. For example: (a) Users of workstations and laptops may not reconfigure the workstation or the laptop in any way. (b) Up-to-date and functioning virus protection must be installed and working at all times on all workstations and mobile computers. (c) Any security threat, issue, or problem must be reported immediately to the Security Officer. (d) Encryption software must be utilized.]
3. **Isolate health care clearing house functions.**²

E. **Security Awareness and Training.** We have implemented the following security awareness and training program for all personnel, including management:

1. **Manual.** Each member of our workforce will be given a copy of this Manual and shall be responsible for reviewing it carefully. Whenever this Manual is updated, copies of the updates or an updated Manual will be supplied to all personnel, who shall be responsible for reviewing the updated material.

2. **Training.**

   [Describe how current personnel will be trained. Describe how new members of your workforce will be trained. Be sure to include a provision for periodic re-training. The training should be done by or under the supervision of the Security Officer.]

3. **Security reminders (addressable).** Our Security Officer will provide periodic security updates to all affected personnel.

4. **Protection from malicious software (addressable).** To guard against, detect, and report malicious software we require:

   [Describe how current personnel will be trained. Describe how new members of your workforce will be trained. Be sure to include a provision for periodic re-training. The training should be done by or under the supervision of the Security Officer.]

5. **Log-in monitoring (addressable):** We have implemented the following procedures for monitoring log-in attempts and reporting discrepancies:

6. **Password management (addressable):** We have implemented the following procedures for creating, changing, and protecting passwords:

   [For example: Each workforce member shall be assigned a unique user identification and password through which that member and only that

² This is required only if a health care clearinghouse is part of your office, in which case you must protect the e-PHI of the health care clearinghouse from access by your practice.
member may access any network, system, or application containing e-PHI. Passwords shall be changed every _______________________. No one may use another person’s user ID, password, or other authentication information. No one may give another person his or her user ID, password, or other authentication information. You should not make or keep a written record or notation of your user ID or password."

F. Security Incident Procedures. We have implemented policies and procedures to address breaches of security, specifically response and reporting procedures (required) to (i) identify and respond to suspected or known security incidents, including how to report suspected or potential security problems, (ii) mitigate, to the extent practicable, harmful effects of security breaches, and (iii) document security incidents and their outcomes. These policies and procedures are contained in our Policy On Notification of Breaches of Unsecured Protected Health Information, which is Attachment 2 to this Manual.

G. Contingency Plan. We have established and will implement as needed policies and procedures for responding to an emergency or other occurrences (such as fire, vandalism, flood, system failure, theft) that threaten the security of e-PHI.

1. Data backup plan (required). We have implemented the following procedures to create and maintain exact copies of e-PHI:

2. Disaster recovery plan (required). We have established the following procedures to restore any loss of data:

3. Emergency mode operation plan (required). We have established the following plan for continuation of critical business and security of e-PHI while operating in emergency mode:
4. **Testing and revision procedures (addressable).** We have implemented the following procedures for periodic testing and revision of our contingency plans:

____________________________________________________________________________________
____________________________________________________________________________________

5. **Applications and data criticality analysis (addressable).** We have assessed and will continue to assess as necessary the relative criticality of specific applications and data in support of other contingency plan components.

H. **Evaluation.** We shall regularly evaluate all technical and nontechnical systems to ensure that e-PHI is adequately protected. We shall also evaluate all technical and nontechnical systems in response to any environmental or operational changes affecting the security of e-PHI. We will document our periodic evaluations, explaining in particular how our policies and procedures comply with the Security Rule requirements.

I. **Business Associate Contracts.** All our contracts with our Business Associates (as that term is defined in HIPAA/HITECH) shall be in writing and shall incorporate and pass along to each business associate the same obligations that we have as a covered entity to comply with the Security Rule.
III. Physical Safeguards

A. Facility Access Controls. We have implemented the following policies and procedures to limit physical access to e- PHI systems and the facilities in which they are housed, while ensuring that properly authorized access is allowed.

1. Contingency operations (addressable). We have established the following procedures to allow facility access to support restoration of lost data under the disaster recovery plan and emergency mode operation:

____________________________________________________________________________________

[Provide a description tailored to your needs. You might specify, for example, that certain individuals or categories of employees are authorized to retrieve backup data and transfer that data to a different computer system in emergency circumstances, such as a hurricane or electrical storm. If you have dealt with this security concern through compliance with another Implementation Specification (e.g., a technical measure that automatically backs up critical e- PHI to a remote computer) or if your risk analysis has determined that this is not a significant risk, then you may not need to implement this Specification, but be sure to document in writing details showing why.]

2. Facility security plan (addressable). We have implemented the following policies and procedures to safeguard our facility and equipment from unauthorized physical access, tampering, and theft:

____________________________________________________________________________________

____________________________________________________________________________________

____________________________________________________________________________________

3. Access control and validation procedures (addressable). We have put in place the following procedures to control and validate a person’s access to facilities based on his or her role or function:

____________________________________________________________________________________

____________________________________________________________________________________

____________________________________________________________________________________

[Insert details, and be sure to include visitor control, and control of access to software for testing and revision.]
4. **Maintenance records (addressable).** We have implemented the following policies and procedures to document repairs and modifications to the physical parts of our facility related to security:

[Describe how you will check on and repair and modify, e.g., hardware, screens, walls, doors, locks to make sure they are and remain secure.]

**B. Workstation Use.** We have implemented the following policies and procedures that describe appropriate functions for a specific workstation or class of workstations used to access e-PHI:

[Provide details. For example, restrict the e-PHI available on a reception area computer to only the e-PHI needed to schedule or change appointments.]

**C. Workstation Security.** We have in place the following physical mechanisms to ensure that access to workstations with e-PHI is restricted to authorized users:

[Provide details. For example: Computer screens must be turned so they cannot be seen by casual observers.]

**D. Device and Media Controls.** We have implemented the following policies and procedures for the receipt and removal of hardware and electronic media that contain e-PHI into, within, and out of our facility.

1. **Disposal (required).** Our polices and procedures for the final disposition of e-PHI and the hardware or electronic media on which it is stored are as follows:

[The policy might include the following, for example: All our media devices are proprietary and contain information that is our property. At no time shall a media device of any kind be removed or disposed of without the knowledge and consent of our Security Officer. All hardware must be sent to the appropriate contracted vendor for final disposition and may not be disposed of at a remote site. This includes but is not limited to tapes, CDROMs, floppy disks and external hard drives.]
2. **Media re-use (required).** Our policies and procedures for removal of e-PHI from media before they are re-used are as follows:

__________________________________________________________________________

__________________________________________________________________________

3. **Accountability (addressable).** For example: The movements of hardware and electronic media and any person who is responsible for those movements shall be documented.

4. **Data backup and storage (addressable).** For example: Before any equipment is moved, we shall, as necessary, create a retrievable, exact copy of e-PHI.
IV. Technical Safeguards

We have in place policies and procedures that govern the technical aspects of accessing e-PHI within our computer systems. They are as follows:

A. **Access Controls.** Our policies and technical procedures for computer use are to ensure only appropriate access to e-PHI by authorized individuals and software programs.

1. **Unique user identification (required).** Each person shall be assigned a unique name and number for identifying and tracking user identity. Sharing these user identifications is not permitted.

2. **Emergency access procedure (required).** In an emergency, we shall obtain e-PHI using the following procedures:

   [Provide details, for example: If emergency access is necessary, contact the Security Officer, who may grant access as appropriate.]

3. **Automatic logoff (addressable).** We have implemented electronic procedures that terminate a computer session after ________________ of inactivity. Users stepping away from their computers must lock the computer, and, if applicable, their office doors.

4. **Encryption and decryption (addressable).** We have implemented a mechanism to encrypt and decrypt e-PHI. [Provide details as applicable.]

B. **Audit Controls.** We have implemented the following hardware, software, and procedural mechanisms that record and monitor activity on our systems for security breaches:

   [Provide details, for example: We shall maintain a log showing who accessed a particular computer and when. We shall maintain a log of all critical system activity including failures. We shall periodically review user IDs and examine their access to the system or the applications that contain e-PHI. We shall keep network activity logs for all critical network devices. We shall review network system logs on a periodic basis to make sure activity is appropriate. We shall review failed attempts to access systems, records, or accounts to check for unauthorized activity. All systems shall be located behind firewalls and have up-to-date virus protection installed. We shall review firewall logs periodically for potential network intrusion.]
C. **Integrity.** We have implemented policies and procedures to protect e-PHI from improper alteration or destruction, including the following **mechanisms to authenticate e-PHI (addressable)** so that we can corroborate that e-PHI has not been altered or destroyed in an unauthorized way:

__________________________________________________________________

__________________________________________________________________

__________________________________________________________________

D. **Person or Entity Authentication.** The following are our procedures to verify that a person or entity seeking access to e-PHI is in fact who he/she/it claims to be:

__________________________________________________________________

__________________________________________________________________

E. **Transmission Security.** We have implemented the following technical security measures to guard against access to e-PHI that is being transmitted over an electronic communications network:

1. **Integrity controls (addressable).** To ensure that e-PHI is not improperly modified without detection we will _________________________.

2. **Encryption (addressable).** We have in place a computer program that encrypts and decrypts data. **OR** When e-mailing or transmitting patient data, we shall use a secure transmission system or messaging service.
V. DOCUMENTATION

A. Maintaining this Manual

1. Security Officer is Responsible for Maintaining this Manual

This Manual and all our records of how we have complied with the requirements of the Security Rule shall be maintained by the Security Officer in both printed and electronic format. This Manual shall be made available to all persons responsible for implementing and required to comply with any of the policies or procedures contained in it.

2. Updates

We shall promptly update our policies and procedures to comply with any changes in the law or any changes in how we plan to comply with the Security Rule.

Whenever we revise or update this Manual, we will keep a record of the date on which it was revised.

Whenever we revise or update this Manual, a copy of the updates or updated Manual shall be given to all persons responsible for implementing and required to comply with any of the policies or procedures contained in it.

3. How Long

This Security Rule Manual shall be kept for 6 years from either the date it was created or the date it last went into effect, whichever is later. Each update shall be kept for 6 years from the date that it went into effect.

B. Documenting Our Security Rule Compliance

We shall keep written records of all our Security Rule compliance efforts. For example, we will keep written records of who received what training, when, and from whom; we will keep written records of any sanctions that are imposed for security breaches; we will keep written records of our periodic evaluations. All these written records shall be kept by our Security Officer.

This Manual was last updated on ________________________________
## Attachment 1

### Risk Analysis Work Sheets

<table>
<thead>
<tr>
<th>Likelihood of Occurrence Levels</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Likelihood</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Negligible</td>
<td>Unlikely ever to occur</td>
</tr>
<tr>
<td>Very Low</td>
<td>Likely to occur two/three times every five years</td>
</tr>
<tr>
<td>Low</td>
<td>Likely to occur once every year or less</td>
</tr>
<tr>
<td>Medium</td>
<td>Likely to occur once every six months or less</td>
</tr>
<tr>
<td>High</td>
<td>Likely to occur once per month or less</td>
</tr>
<tr>
<td>Very High</td>
<td>Likely to occur multiple times per month</td>
</tr>
<tr>
<td>Extreme</td>
<td>Likely to occur multiple times per day</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Impact Severity Levels</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Insignificant</td>
<td>Little or no impact</td>
</tr>
<tr>
<td>Minor</td>
<td>Minimal effort to repair, restore or reconfigure</td>
</tr>
<tr>
<td>Significant</td>
<td>Small but tangible harm, noticeable to limited number, some effort to repair</td>
</tr>
<tr>
<td>Damaging</td>
<td>Damage or loss to many, significant effort to repair</td>
</tr>
<tr>
<td>Serious</td>
<td>Considerable system outage, compromise of large amount of information affecting many</td>
</tr>
<tr>
<td>Critical</td>
<td>Extended outage, permanent loss or damage, triggering business continuity procedures, complete compromise of information</td>
</tr>
</tbody>
</table>
This table shows the resulting risk level, for each degree of likelihood and each level of severity.

<table>
<thead>
<tr>
<th>Risk Levels</th>
<th>Insignificant</th>
<th>Minor</th>
<th>Significant</th>
<th>Damaging</th>
<th>Serious</th>
<th>Critical</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Negligible</strong></td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td><strong>Very Low</strong></td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Moderate</td>
<td>Moderate</td>
</tr>
<tr>
<td><strong>Low</strong></td>
<td>Low</td>
<td>Low</td>
<td>Moderate</td>
<td>Moderate</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td><strong>Medium</strong></td>
<td>Low</td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td><strong>High</strong></td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td><strong>Very High</strong></td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td><strong>Extreme</strong></td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
</tbody>
</table>
## Risk Determination Table

**Date:** __________

<table>
<thead>
<tr>
<th>Item No.</th>
<th>Threat Name</th>
<th>Vulnerability Name</th>
<th>Risk Description</th>
<th>Existing Controls</th>
<th>Likelihood of Occurrence</th>
<th>Impact Severity</th>
<th>Risk Level</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Safeguard Determination Table

Date:___________________

<table>
<thead>
<tr>
<th>Item No. (from Risk Determination Table)</th>
<th>Recommended Safeguard Description</th>
<th>Residual Likelihood of Occurrence</th>
<th>Residual Impact Severity</th>
<th>Residual Risk Level</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Copyright © 2011 by SVMIC