AOA

HIPAA SECURITY

REGULATION

COMPLIANCE MANUAL

August, 2013

HIPAA SECURITY REGULATION COMPLIANCE

DOCUMENTS

For

(Practice name) ____

____

(Street Address) ____

____

(City, State, ZIP) ____

____

Adopted ________________
(Date)

INTRODUCTION

The federal Health Insurance Portability and Accountability Act's (HIPAA's) Security Regulation requires optometrists and other small health care practices to meet administrative, physical, and technical standards to protect the confidentiality, integrity, and accessibility of their electronic Protected Health Information (ePHI). The Regulation is in large part intended to prevent computer hacking, identity theft-related crime, and similar issues posed by the use of electronic information technology in health care practices and to create a general "culture of security" in those practices. Many of the measures required under the Regulation are common sense steps that many practices are already taking to protect their electronic records and computer equipment. In many cases, compliance with the Regulation will simply mean documenting that these steps are being taken.

The federal Health Information Technology for Economic and Clinical Health (HITECH) Act was passed as part of the American Recovery and Reinvestment Act of 2009 (ARRA) and it broadens the privacy and security protections under HIPAA. Specifically, HITECH requires covered entities to notify affected individuals and the Secretary of Health and Human Services (HHS) in the event of a breach of their "unsecured PHI". Many state laws impose similar or overlapping obligations on businesses.

Another significant change brought about by HITECH is that a covered entity's "business associates" (and their subcontractors) are now directly subject to HIPAA's Security Regulation. HITECH also broadened, (and in some cases, narrowed) the definition of "business associate". Thus, a practice's security program should require the practice to keep a closer eye on its business associate relationships, as discussed in greater detail below.

The HIPAA Final Rule (the "Final Rule"), released on January 17, 2013, amended HIPAA's privacy and security rules to implement the foregoing HITECH requirements. The definition of what constitutes a "breach" of PHI was also broadened by the Final Rule, which now requires a practice to "presume" that any non-permitted acquisition, access, use or disclosure of PHI is a breach under HIPAA requiring notification to affected individuals and HHS in accordance with HIPAA regulations. In determining whether a covered entity can overcome the presumption of a breach, the Final Rule requires covered entities to undergo a "risk assessment" based on several factors to determine whether there was a low probability that the PHI was compromised by the non-permitted acquisition, access, use or disclosure. The Final Rule also increased civil money penalties payable to HHS for uncorrected violations and willful neglect of HIPAA requirements.

HITECH and the Final Rule made few changes to the technical standards of the Security Regulation and a full analysis of HITECH and the Final Rule is therefore beyond the scope of this Manual. Nevertheless, in implementing and maintaining a security program, practices should be aware of the changes summarized above. Now more than ever, HHS is bringing enforcement actions against providers and business associates for breaches of unsecured PHI and has even gone after small providers for breaches involving less than 500 individuals. Given this heightened enforcement environment and the broadening of the privacy and security rules under HITECH and the Final Rule, practices are well advised to increase their focus and involvement in maintaining a strong security program consistent with the Security Regulation.

The Security Regulation applies only to electronic data used, transmitted, or maintained by the practice (unlike the HIPAA Privacy Regulation which covers health information on paper or in any other form). However, practitioners should remember that the Regulation's definition of electronic Protected Health Information includes demographic, health and financial information which might include name, address, Social Security number, credit card numbers, insurance plan numbers, or other identifiers.

Because information technology and the threats to that technology are constantly evolving, the HIPAA Security Regulation is not highly specific. The Regulation essentially requires health care practices to take ***reasonable and appropriate*** measures to protect against ***reasonably anticipatable*** threats to the practice's ePHI. The Regulation sets a series of 18 standards for the protection of electronic health information and a total of 36 implementation specifications to help health care providers address exactly what needs to be done to meet those standards. The HIPAA Security Regulation is outlined in a chart on the following pages with **standards** in **bold lettering** and *implementation specifications* in *italics*.

To help ensure the best protection available in each covered health entity, as well as to make the Regulation less onerous, the Regulation is technology neutral, requiring no specific brands or types of technology be employed, as well as flexible and scalable (to the size of the practice). The Regulation was written to cover a full spectrum of health care providers, from the largest hospitals and health systems to individual health care practitioners. Small health care practices with perhaps one practitioner and a minimal office staff are among the smallest entities covered under the Regulation. In some cases, standards overlap.

Compliance with all standards is ***required***. In most cases, compliance with the implementation specifications under a standard will constitute compliance with the standard. Implementation specifications are divided into ***required*** specifications that must be implemented exactly as indicated and ***addressable*** specifications which can be adapted in a manner reasonable and appropriate to the practice so as to address reasonably anticipatable risks to ePHI. However, the Centers for Medicare and Medicaid Services (CMS), the enforcement agency for the Regulation, emphasizes that "addressable" does not mean "optional". Should a practice not implement an addressable measure exactly as indicated, the practice must document alternative measures and the reason they were taken. **Compliance with all the standards and specifications must be documented.** Enforcement will be complaint-driven.

The AOA HIPAA Security Regulation Compliance Manual is designed to help optometrists begin ePHI security programs in their practices. However, the manual can represent a good first step in establishing the "culture of security" demanded by the regulation. Compliance with the HIPAA Security Regulation is an on-going process with periodic review and evaluation required. Practitioners should periodically reassess the measures and approaches suggested in this manual. Moreover, no security approach is appropriate for all practices. Practitioners should investigate other HIPAA compliance approaches to find the system best suited for their particular practices (see Additional Resources page for examples).

This manual is not legal advice. It is provided as an informational tool to assist you in becoming compliant with HIPAA. Nothing in this Workbook is intended to create any

attorney client relationship between you and either the AOA or the AOA Office of Counsel. For legal advice, you are advised to consult your own private attorney.

HIPAA SECURITY REGULATION

ADMINISTRATIVE SAFEGUARDS – 45 C.F.R. §164.308

1. **Security Management Process.**
   - **a.** *Risk Analysis (Required).*
   - **b.** *Risk Management (Required).*
   - **c.** *Sanction Policy (Required).*
   - **d.** *Information System Activity Review (Required).*
2. **Assigned Security Responsibility.**
3. **Workforce Security.**
   - **a.** *Authorization and/or Supervision Policy (Addressable).*
   - **b.** *Workforce Clearance Procedures (Addressable).*
   - **c.** *Termination Procedures (Addressable).*
4. **Information Access Management.**
   - **a.** *Isolating Healthcare Clearinghouse Function (Required).*
   - **b.** *Access Authorization (Addressable).*
   - **c.** *Access Establishment and Modification (Addressable).*
5. **Security Awareness and Training.**
   - **a.** *Security Reminders (Addressable).*
   - **b.** *Protection from Malicious Software (Addressable).*
   - **c.** *Log-in Monitoring (Addressable).*
   - **d**. *Password Management (Addressable).*
6. **Security Incident Procedures.**
   - **a**. *Response and Reporting (Required).*
7. **Contingency Plan.**
   - **a.** *Data Backup Plan (Required).*
   - **b.** *Disaster Recovery Plan (Required).*
   - **c.** *Emergency Mode Operation Plan (Required).*
   - **d.** *Testing and Revision Procedures (Addressable).*
   - **e.** *Applications and Data Criticality Analysis (Addressable).*
8. **Evaluation.**
9. **Business Associate Contracts and Other Arrangement.**
   - **a.** *Written Contracts or Other Arrangement (Required).*

PHYSICAL SAFEGUARDS – 45 C.F.R. §164.310

10. **Facility Access Controls.**
    - **a.** *Contingency Operations (Addressable).*
    - **b.** *Facility Security Plan (Addressable).*
    - **c.** *Access Control and Validation Procedures (Addressable).*
    - **d.** *Maintenance Records (Addressable).*
11. **Workstation Use.**
12. **Workstation Security.**
13. **Device and Media Controls.**
    - **a.** *Disposal (Required).*
    - **b.** *Media Re-use (Required).*
    - **c.** *Accountability (Addressable).*
    - **d.** *Data Back-up and Storage (Addressable).*

TECHNICAL SAFEGUARDS – 45 C.F.R. §164.312

14. **Access Control.**
    - **a.** *Unique User Identification (Required).*
    - **b.** *Emergency Access Procedure (Required).*
    - **c.** *Automatic Log-Off (Addressable).*
    - **d.** *Encryption and Decryption (Addressable).*
15. **Audit Control.**
16. **Integrity.**
    - **a.** *Mechanism to Authenticate ePHI (Addressable).*
17. **Person or Entity Authentication.**
18. **Transmission Security.**
    - **a.** *Integrity Controls (Addressable).*
    - **b.** *Encryption (Addressable).*

ORGANIZATIONAL REQUIREMENTS – 45 C.F.R. §164.314

19. **Business Associate Contracts or Other Arrangements.**
    - **a.** *Business Associate Contracts (Required).*
    - **b.** *Other arrangements (Required).*
    - **c.** *Business Associate Contracts with Sub-Contractors (Required).*
20. **Requirements for Group Health Plans.**
    - **a.** *Implement Safeguards (Required).*
    - **b.** *Ensure Adequate Separation (Required).*
    - **c.** *Ensure Agents Implement Measures (Required).*
    - **d.** *Report Security Incidents (Required).*

POLICIES, PROCEDURES, AND DOCUMENTATION REQUIREMENTS – 45 C.F.R. §164.316

21. **Policies and Procedures.**
22. **Documentation.**
    - **a.** *Time Limit (Required).*
    - **b.** *Availability (Required).*
    - **c.** *Updates (Required).*

HOW TO USE THIS MANUAL

The American Optometric Association (AOA) HIPAA Security Regulation Compliance Manual, prepared by the AOA Office of Counsel and the AOA Communications Group, provides an orderly compliance approach of 14 steps, each representing one or more standards or specifications. It is based on The Workgroup for Electronic Data Interchange's Small Practice Security Implementation White Paper and other documents (see Additional Resources). The manual is designed to comply with the *HIPAA Security Policies and Procedures and Documentation Requirements (Standard §164.316 Policies and Procedures* -- *Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications of this subpart, taking into account those factors specified in §164.306(b)(2) (i),(ii),(iii), and (iv)* [See Documentation Requirements following the Cross-referenced Outline of Manual]), allowing practices that have adopted the 14 policy documents and attached any appropriate documentation of conformance with the respective policies to demonstrate they have met the required standards.

A brief discussion provides an explanation of each step along with some specific measures practices may wish to consider. A model policy document for each step is provided, stipulating that the practice will comply with all standards and required specifications and implement reasonable and appropriate measures for all addressable specifications. In some cases, forms for documentation of policy conformance have been provided. Practices must attach documentation indicating what alternative measures have been taken (and why) for any addressable step that is not implemented as indicated. In some cases, more than one model policy has been provided (such as a short form for small practices and a longer, more detailed form for larger practices with a complex office staffing structure), allowing practitioners to select the most appropriate. Practices should edit the models as necessary (see examples on following pages). Practitioners should date each form upon adoption.

Practices that use these or other model HIPAA compliance policies should carefully adapt the model policy to reflect state law, the requirements of their practice, or other pertinent factors. Practices should include in their compliance policies only those compliance measures they can and will implement. Practitioners can expose their practices to considerable legal risk if they specify compliance measures in their policies and then fail to actually implement those measures.

A copy of the HIPAA Security Regulation is included at the end of this manual.

Example 1: Edited Policy Document

(Document XX)

Emergency Access Policy

It is the policy of the practice to ensure access to obtain necessary electronic Protected Health Information in the event of an emergency as indicated by options marked below.

- ~~Special user account providing emergency access to all ePHI.~~

- ~~Practitioner user account(s) provide(s) access to all ePHI.~~

- ~~All staff members have access to all ePHI, as required in small practice.~~

- Other: Practitioner and office manager passwords.

(Notations: This is a very small practice with one practitioner and one office manager/staff person. User accounts for both provide access to all files, and special access user accounts are not applicable in this practice.)

> **Explanation: In the example above, the options set out in the law were not applicable given the size of the practice. If the practitioner does not adopt the specification as set out, he/she must determine the most reasonable and appropriate means of achieving compliance. That option is set out, along with an explanation of how or why the method achieves compliance.**

Policy adopted 4/20/05
(Date)

Example 2: Completed Documentation Form

(Document 10-1)

Technical Security Mechanisms Log

Indicate the security-related information software functions installed and activated on practice information processing system as required or addressable under the HIPAA Security Regulation or, if a mechanism is not reasonable and appropriate to protect against reasonably anticipatable risks to ePHI, the alternative measure and the reason for its use. Also indicate the date the feature was installed, activated, updated, or last checked to determine that it is operational.

STANDARDS/SPECIFICATIONS	MEASURES IMPLEMENTED	DATE
Access Control (Required)	(See line below.)	04/20/05
Unique User Identification (Required)	(Password and user ID)	04/20/05
Emergency Access Procedures (Required)	(All passwords/ID's access all ePHI)	04/20/05
Automatic Log-Off (Addressable)	(Password protected screensaver activates in 3 minutes)	04/20/05
Encryption and Decryption (Addressable)	(VisionWeb secures Web site)	04/20/05
Audit Control (Required)	(Microsoft XE log-on tracking)	04/20/05
Integrity (Required)	(See line below.)	04/20/05
Mechanisms to Authenticate ePHI (Addressable)	(Virus protection, firewall)	04/20/05
Person or Entity Authentication (Required)	(Password and user ID)	04/20/05
Transmission Security (Required)	(See lines below)	04/20/05
Integrity Controls (Addressable)	("Patches" regularly installed, anti-intrusion program)	04/20/05
Encryption (Addressable)	(Tumbleweed encrypted e-mail)	04/20/05
Other		

(Notations: ____

____)

____

Documentation Requirements

Standard: Policies and Procedures (§164.316) - Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications of this subpart, taking into account those factors specified in §164.306(b)(2) (i),(ii),(iii), and (iv).

Standard 164.316(b)(1): Documentation - Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form. If an action, activity, or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.

Implementation Specification (b)(2)(i): Time Limit (Required) - Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.

Implementation Specification (b)(2)(ii): Availability (Required) - Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

Implementation Specification (b)(2)(iii): Updates (Required) - Review documents periodically and update as needed in response to environmental or operational changes affecting the security of the electronic protected health information.

CROSS-REFERENCED OUTLINE OF MANUAL

Step 1: Security and Risk Management.

Standard 1 - Security Management Process: Implement policies and procedures to prevent, detect, contain, and correct security violations. [§164.308(a)(1)(i)]

Implementation Specification 1b - Risk Management (Required): Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. The Regulation outlines those measures in the remaining security specifications. [§164.308(a)(1)(ii)(B)]

Step 2: Risk Analysis.

Implementation Specification 1a - Risk Analysis (Required): Practices must conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the small practice or business associate. [§164.308(a)(1)(ii)(A)]

Step 3: Contingency Plan.

Standard 7 - Contingency Plan: Establish and implement, as needed, policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain ePHI. [§164.308(a)(7)(i)]

Implementation Specification 7a – Data Backup Plan (Required): Establish and implement procedures to create and maintain retrievable exact copies of ePHI. [§164.308(a)(7)(ii)(A)]

Implementation Specification 7b - Disaster Recovery Plan (Required): Establish (and implement as needed) procedures to restore any loss of data. [§164.308(a)(7)(ii)(B)]

Implementation Specification 7c - Emergency Mode Operation Plan (Required): Establish and implement as needed procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode. [§164.308(a)(7)(ii)(C)]

Implementation Specification 7d - Testing and Revision Procedure (Addressable): Implement procedures for periodic testing and revision of Contingency Plan. [§164.308(a)(7)(ii)(D)]

Implementation Specification 7e - Applications and Data Criticality Analysis (Addressable): Assess the relative criticality of specific applications and data in support of other Contingency Plan components. [§164.308(a)(7)(ii)(E)]

Implementation Specification 10a - Contingency Operations (Addressable): Establish and implement as needed procedures that allow facility access in support of restoration of lost data under the Disaster Recovery Plan and Emergency Mode Operation Plan in the event of an emergency. [§164.310(a)(2)(i)]

Implementation Specification 14b - Emergency Access Procedure (Required): Establish and implement as needed procedures for obtaining necessary ePHI during an emergency. [§164.312(a)(2)(ii)]

Step 4: Workstation Policy.

Implementation Specification 1d - Information System Activity Review (Required): Implement procedures to regularly review records of information system activity such as audit logs, access reports, and security incident tracking reports. [§164.308(a)(1)(ii)(D)]

Standard 3 - Workforce Security: Practices must implement policies and procedures to ensure all members of its workforce have appropriate access to ePHI and to prevent those workforce members who do not have access from obtaining access to ePHI. [§164.308(a)(3)(i)]

Implementation Specification 3a - Authorization and/or Supervision Policy (Addressable): Practices must implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed. [§164.308(a)(3)(ii)(A)]

Implementation Specification 3b - Workforce Clearance Procedures (Addressable): Implement procedures to determine that the access of a workforce member to ePHI is appropriate. [§164.308(a)(3)(ii)(B)]

Implementation Specification 3c - Termination Procedures (Addressable): Implement procedures for terminating access to ePHI when the employment of a workforce member ends or as required by determinations made as specified in the Security Rule. [§164.308(a)(3)(ii)(C)]

Standard 4 - Information Access Management: Implement policies and procedures for authorizing access to ePHI that are consistent with the applicable requirements of the Security Rule. [§164.308(a)(4)(i)]

Implementation Specification 4b - Access Authorization (Addressable): Implement policies and procedures for granting access to ePHI, for example, through access to a workstation, transaction, program, process, or other mechanism. [§164.308(a)(4)(ii)(B)]

Implementation Specification 4c -Access Establishment and Modification (Addressable): Implement policies and procedures, based upon the practice's

Access Authorization Policy, that establish, review, and modify a user's right of access to a workstation, transaction, program, or process. [§164.308(a)(4)(ii)(C)]

Standards 11 and 12 - Workstation Use and Security (Required): Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surrounding of a specific workstation or class of workstation that can access ePHI. Implement physical safeguards for all workstations that access ePHI to restrict access only to authorized users. [§164.310(b),(c)]

Standard 14 - Access Control (Required): Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access to those persons granted access rights as specified in the Security Rule. [§164.312(a)(1)]

Implementation Specification 14a - Unique User Identification (Required): Assign a unique name and/or number for tracking the identity of each user. [§164.312(a)(2)(i)]

Implementation Specification 14b - Emergency Access Procedure (Required): Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency. [§164.312(a)(2)(ii)] (See Step 3)

Standard 17 - Person or Entity Authentication (Required): Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed. [§164.312(d)]

Step 5: Security Officer.

Standard 2 - Assigned Security Responsibility (Required): Practices must identify the security official responsible for the development and implementation of the policies and procedures required by the Security Rule. [§164.308(a)(2)]

Step 6: Facility Controls.

Standard 10 - Facility Access Controls (Required): Implement policies and procedures to limit physical access to electronic information systems and the facility or facilities in which they are housed while also ensuring that properly authorized access is allowed. [§164.310(a)(1)]

Specification 10b - Facility Security Plan (Addressable): Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. [§164.310(a)(2)(ii)]

Specification 10c – Access control and validation (Addressable): Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision. [§164.310(a)(2)(iii)]

Specification 10d - Maintenance records (Addressable): Implement policies and procedures to document repairs and modifications to the physical components of a facility that are related to security (for example, hardware, walls, doors, and locks). [§164.310(a)(2)(iv)]

Step 7: Data Control Procedures.

Implementation Specification 7a - Data Back-up Plan (Required): Establish and implement procedure to create and maintain retrievable exact copies of ePHI. [§164.308(a)(7)(ii)(A)]

Standard 13 - Device and Media Controls: Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility and the movement of these items within the facility. [§164.310(d)(1)]

Implementation Specification 13a - Disposal (Required): Implement policies and procedures to address the final disposition of ePHI and/or the hardware or electronic media on which it is stored. [§164.310(d)(2)(i)]

Implementation Specification 13b - Media Re-use (Required): Implement procedures for removal of ePHI from electronic media before the media are made available for re-use. [§164.310(d)(2)(ii)]

Implementation Specification 13c - Accountability (Addressable): Maintain a record of the movements of hardware and electronic media and any person responsible therefore. [§164.310(d)(2)(iii)]

Implementation Specification 13d - Data Back-up and Storage (Addressable): Create a retrievable exact copy of ePHI, when needed, before movement of equipment. [§164.310(d)(2)(iv)]

Step 8: Business Associate Agreements.

Standard 9 -Business Associate Contracts and Other Arrangements (Required): A practice may permit a business associate to create, receive, maintain, or transmit ePHI on the practice’s behalf only if the practice obtains satisfactory assurance that the associate will appropriately safeguard the information. Practices must have signed Business Associate Agreements with certain outside parties that have access to the practice’s confidential information. The practice's subcontractors that create, receive, maintain, or transmit ePHI on the practice's behalf must give the practice satisfactory assurances that they will appropriately safeguard the information by entering into a Business Associate Agreement with the practice in accordance with the Final Rule. [§164.308(b)(1) and (2)]

Implementation Specification 9a - Written Contract or Other Arrangements (Required): Document the satisfactory assurances required through a written contract or other arrangement with the Business Associate or the practice's subcontractors that meets the applicable requirements. [§164.308(b)(3)]

Step 9: Training.

Standard 5 - Security Awareness and Training (Required): Practices must implement a security awareness and training program for all members of the practice workforce (including management). [§164.308(a)(5)(i)]

Implementation Specification 5a - Security Reminders (Addressable): The practice Security Officer must issue periodic security updates informing the practice's workforce of any changes that may affect the privacy and security of confidential information. [§164.308(a)(5)(ii)(A)]

Implementation Specification 5b - Protection from Malicious Software (Addressable): Procedures should be outlined for guarding against, detecting, and reporting malicious software. [§164.308(a)(5)(ii)(B)]

Implementation Specification 5c - Log-in Monitoring (Addressable): Establish procedures for monitoring log-in attempts and reported discrepancies. [§164.308(a)(5)(ii)(C)]

Implementation Specification 5d - Password Management (Addressable): Establish procedures for creating, changing, and safeguarding passwords. [§164.308(a)(5)(ii)(D)]

Step 10: Technical Security Mechanisms.

Implementation Specification 1d - Information System Activity Review (Required): Implement procedures to regularly review records of information system activity such as audit logs, access reports, and security incident tracking reports. [§164.308(a)(1)(ii)(D)] (See Step 4)

Standard 14 - Access Control (Required): Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in the Security Rule [§164.312(a)(1)] (See Step 4)

Implementation Specification 14a - Unique User Identification (Required): Assign each workforce member a username and password. [§164.312(a)(2)(i)] (See Step 4)

Implementation Specification 14b - Emergency Access Procedure (Required): Establish (and implement as needed) procedures for accessing necessary ePHI during an emergency in line with the practice Contingency Plan (Standard 10). [§164.312(a)(2)(ii)] (See Steps 3 & 4)

Implementation Specification 14c - Automatic Log-Off (Addressable): Implement electronic procedures that terminate sessions on practice workstations after a pre-determined period of inactivity. [§164.312(a)(2)(iii)]

Implementation Specification 14d - Encryption and Decryption (Addressable): Implement a mechanism to encrypt and decrypt ePHI. [§164.312(a)(2)(iv)]

Standard 15 - Audit Control: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI. [§164.312(b)]

Standard 16 - Integrity: Implement policies and procedures to protect ePHI from improper alteration or destruction. [§164.312(c)(1)]

Implementation Specification 16a - Mechanism to Authenticate ePHI (Addressable): Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in any unauthorized manner including, as appropriate, virus protections, firewall protections, access controls, or other appropriate safeguards. [§164.312(c)(2)]

Standard 17 - Person or Entity Authentication: Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed. [§164.312(d)] (See Step 4)

Standard 18 - Transmission Security: Implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network including mechanisms to ensure information is only transmitted to the intended individual or entity [§164.312(e)(1)]

Implementation Specification 18a - Integrity Controls (Addressable): Implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of. [§164.312(e)(2)(i)]

Implementation Specification 18b - Encryption (Addressable): Implement a mechanism to encrypt ePHI whenever deemed appropriate. [§164.312(e)(2)(ii)]

Step 11: Security Incident Response and Reporting.

Standard 6: Security Incident Procedures: Implement an administrative policy for handling and documenting "security incidents" and their resolution. [§164.308(a)(6)(i)]

Implementation Specification 6a - Response and Reporting (Required): Practices must identify and respond to suspected or known security incidents, mitigate, to the extent practicable, harmful effects of security incidents that are known to the practice (in its capacity as either a business associate or covered entity), and document security incidents and their outcomes. [§164.308(a)(6)(ii)]

Step 12: Sanction Policy.

Implementation Specification 1c - Sanction (Required): Practices must apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the practice. [§164.308(a)(1)(ii)(C)]

Step 13: Evaluation.

Standard 8: Evaluation: Practices must perform a periodic technical and non-technical evaluation based initially on the standards implemented under this rule and, subsequently, in response to environmental or operational changes that affect the security of ePHI. [§164.308(a)(8)]

Implementation Specification 7d - Testing and Revision Procedures (Addressable): Practices must implement procedures for periodic testing and revision of contingency plans. [§164.308(a)(7)(ii)(D)] (See Step 3)

Implementation Specification - Updates (Required): Review documents periodically and update as needed in response to environmental or operational changes affecting the security of the ePHI. [§164.316(b)(2)(iii)]

Step 14: Isolate Healthcare Clearinghouse Function.

Implementation Specification 4a – Isolate Healthcare Clearinghouse Function. [§164.308(a)(4)(ii)(A)]

DOCUMENTATION REQUIREMENTS

45 C.F.R. §164.316

Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form. If an action, activity, or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment. Retain the documentation required by paragraph (b)(1) of this section for 6 (six) years from the date of its creation or the date when it last was in effect, whichever is later. Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains. Review documents periodically and update as needed in response to environmental or operational changes affecting the security of the ePHI. (See Step 13)

Step 1: Security Management and Risk Management.

The HIPAA Security Regulation requires every covered health care practice to adopt a formal process to protect ePHI in the practice, including a Risk Management Plan to address reasonable and anticipatable risks and vulnerabilities as identified in a formal Risk Analysis process (Step 2). The measures required under those policies will be embodied in the remaining standards and implementation specifications set down under the Regulation (Steps 3 through 14). Risk management is not static – it is an ongoing process. It entails not only the act of implementing security safeguards and controls but also monitoring for changes and responding with enhanced strategies.

Adopt Security Management Policy using model Document 1, if desired, adapting the document as appropriate to reflect state law, the requirements of the practice, or other pertinent factors. If the practice is not covered under the HIPAA Security Regulation, complete Document 1-1, documenting why under "Notations".

(Document 1)

SECURITY MANAGEMENT POLICY

The optometric practice of ____, in compliance with the federal Health Insurance Portability and Accountability Act (HIPAA) Security Regulation, hereby establishes a security program of administrative, physical, and technical steps to ensure the confidentially, integrity, and accessibility of the electronic Protected Health Information (ePHI) received, generated, maintained, processed, transmitted, or otherwise used by the practice, meeting all standards and addressing or meeting all specifications of the Regulation, with special attention to security risks determined to pose the greatest threat to the ePHI in the practice as determined by a formal Risk Analysis (see Document 2). The practice also hereby establishes and implements measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level with specific measures taken to meet each of the indicated standards and address or meet each of the indicated specifications documented on the following pages.

(Notations: ____

____
)
____

Policy adopted ____________________
(Date)

(Document 1-1 – alternate)

SECURITY MANAGEMENT POLICY

A formal security management process and related steps required under the HIPAA Security Regulation are not deemed necessary for this practice because the practice utilizes no ePHI, keeping all records on paper or for other reasons stated below. However, the practice will periodically evaluate its need for such security management and, should future events warrant (e.g., practice begins processing insurance claims electronically, contracts for Internet service, or otherwise begins utilizing ePHI), the practice will reassess its policy and consider formal measures to protect ePHI in line with the regulation.

(Notations: ____

____
)
____

Policy adopted ____________________
(Date)

Step 2: Risk Analysis.

When considering the potential risks to a practice and its protected information, natural or man-made disasters may be the first factors that come to mind. The possibility of computer hacking attempts or computer virus attacks should also probably be considered. Many security breaches will be incidents in which staff or other persons inadvertently or purposely access or misuse protected information. However, the theft of practice equipment is statistically the largest threat to ePHI. According to the HHS's Office of Civil Rights, which is responsible for the enforcement of HIPAA's privacy rules, thefts accounted for 37% of ePHI breaches as of July 17, 2013. Thefts of laptops and portable media/devices are a significant source of such breaches. How does the physical plant of the practice (be it free-standing, a medical building, or an office plaza) serve to either protect or expose the practice to the possibility of burglary or theft? Could practice equipment (such as laptop computers, personal digital assistants, or cell phones) that contains ePHI be stolen or tampered with if taken from the practice? In preparing the risk analysis practitioners should complete an inventory of all devices or systems in the office used for ePHI and make sure threats to each of those systems or devices is considered. Practices should also inventory the security technology utilized on their information processing system. Practices should also assess the physical security of their offices.

Conduct a Risk Analysis using the Risk Analysis Outline (Document 2) or other appropriate methodology (see additional resources). To formally prioritize the vulnerabilities identified in the risk analysis, practitioners may wish to conduct a qualitative and quantitative analysis, adapting the Vulnerability Worksheet (Document 2- 1) and the Vulnerability Matrix, (Document 2-2) to list the vulnerabilities determined to be most relevant to their individual practices.

(Document 2)

Risk Analysis Outline
(Courtesy: Susan A. Miller, J.D.)

The risk assessment **must**:

1) Identify your tools that hold ePHI and

2) Identify the threats to that ePHI and

3) Identify the vulnerabilities in your system that would permit these threats to impact your ePHI and

4) Identify what the loss or destruction of ePHI would mean to your organization and;

5) Identify what controls your organization can put in place to protect your ePHI.

A *hardware and software* risk assessment should consider:

1. All servers;

2. Your entire network, including:

   - --Topology;

   - --Local area networks;

   - --Wide-area networks;

   - --Communication servers;

   - --Bandwidth connectivity; and --Storage.

3. All data bases with ePHI;

4. All computers that are connected to ePHI for data processing and analysis; and

5. All practice-owned cell phones, laptops and mobile computing devices or media.

A *systems inventory* should include:

1. All policies and procedures that impact the security of ePHI;

2. All information systems with a focus on critical/sensitive ePHI processed by the systems;

3. All business associates and how they process /use ePHI;

4. All biomedical equipment that contains ePHI;

5. All employees that have remote access OF ANY KIND to ePHI; and

6. All vendor partners who have access to ePHI.

After all your data has been collected and analyzed, perform a gap analysis to identify your areas of exposure and/or vulnerabilities within each area and how they interconnect. This will assist you in predicting the probability of occurrence and the loss with a catastrophic security breach.

In the end your risk analysis should demonstrate at a minimum the following:

- The risk level associated with each potential vulnerability;
- Steps to be taken to reduce such vulnerability; and
- The processes to maintain no more than the acceptable level of risk.

A risk assignment should include:

1. Analysis of loss potential;

2. Analysis of your user community;

3. Workforce security;

4. Analysis of the attack including probability, type and source of attack;

5. Level of security;

6. Ease of use and access;

7. Cost/benefit analysis for each solution; and

8. Coordinate each solution to your contingency plan.

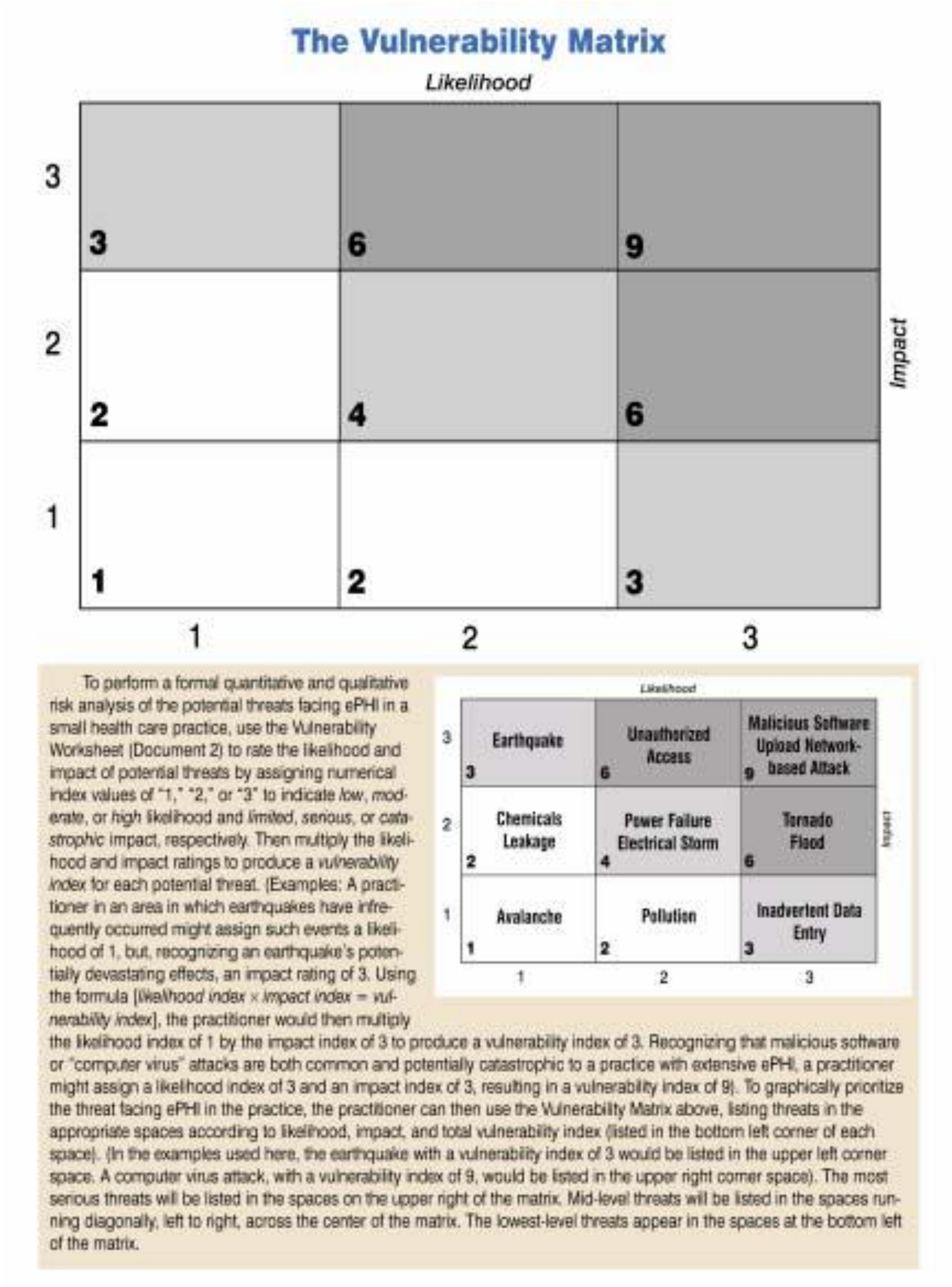
Conduct a Risk Analysis using the Risk Analysis Outline (Document 2) or other appropriate methodology (see additional resources). To formally prioritize the vulnerabilities identified in the risk analysis, practitioners may wish to conduct a qualitative and quantitative analysis, adapting the Vulnerability Worksheet(Document 2- 1) and the Vulnerability Matrix, (Document 2-2) to list the vulnerabilities determined to be most relevant to their individual practices.

(Document 2-1)

VULNERABILITY WORKSHEET

Natural Threats	**IMPACT INDEX**	**X**	**LIKELIHOOD INDEX**	**=**	**VULNERABILITY INDEX**
Flood		X		=	
Earthquake		X		=	
Tornado		X		=	
Landslide		X		=	
Avalanche		X		=	
Electrical storm		X		=	
Fire		X			
Other		X		=	
Human Threats					
(Unintentional)					
Inadvertent data entry		X		=	
Other		X		=	
(Deliberative)					
Network-based attacks		X		=	
Malicious software upload		X		=	
Unauthorized access to confidential information		X		=	
Theft		X		=	
Other		X		=	
Environmental Threats					
Long-term power failure		X		=	
Pollution		X		=	
Chemicals		X		=	
Liquid leakage		X		=	
Other		X		=	

(Document 2-2)



The Vulnerability Matrix

Likelihood

3	3	6	9
2	2	4	6
1	1	2	3
	1	2	3

Impact

To perform a formal quantitative and qualitative risk analysis of the potential threats facing ePHI in a small health care practice, use the Vulnerability Worksheet (Document 2) to rate the likelihood and impact of potential threats by assigning numerical index values of "1," "2," or "3" to indicate *low*, *moderate*, or *high* likelihood and *limited*, *serious*, or *catastrophic* impact, respectively. Then multiply the likelihood and impact ratings to produce a *vulnerability index* for each potential threat. (Examples: A practitioner in an area in which earthquakes have infrequently occurred might assign such events a likelihood of 1, but, recognizing an earthquake's potentially devastating effects, an impact rating of 3. Using the formula [*likelihood index* × *impact index* = *vulnerability index*], the practitioner would then multiply the likelihood index of 1 by the impact index of 3 to produce a vulnerability index of 3. Recognizing that malicious software or "computer virus" attacks are both common and potentially catastrophic to a practice with extensive ePHI, a practitioner might assign a likelihood index of 3 and an impact index of 3, resulting in a vulnerability index of 9). To graphically prioritize the threat facing ePHI in the practice, the practitioner can then use the Vulnerability Matrix above, listing threats in the appropriate spaces according to likelihood, impact, and total vulnerability index (listed in the bottom left corner of each space). (In the examples used here, the earthquake with a vulnerability index of 3 would be listed in the upper left corner space. A computer virus attack, with a vulnerability index of 9, would be listed in the upper right corner space). The most serious threats will be listed in the spaces on the upper right of the matrix. Mid-level threats will be listed in the spaces running diagonally, left to right, across the center of the matrix. The lowest-level threats appear in the spaces at the bottom left of the matrix.

Likelihood

3	Earthquake 3	Unauthorized Access 6	Malicious Software Upload Network-based Attack 9
2	Chemicals Leakage 2	Power Failure Electrical Storm 4	Tornado Flood 6
1	Avalanche 1	Pollution 2	Inadvertent Data Entry 3
	1	2	3

Impact

Step 3: Contingency Plan.

Practices must establish procedures for restoration of lost ePHI in the event of an adverse incident — be that a fire, natural disaster, or other incident that damages the entire practice or failure of the practice information processing system itself. In establishing such procedures, practices should consider the reasonably anticipatable risks and vulnerabilities identified in the Risk Analysis (Documents 2 and 2-1). Focusing, in part, on large hospitals that must remain in operation following a natural disaster or system failure, the Regulation calls for both a Disaster Recovery Plan (the process of restoring a practice or health provider organization, its information processing system, or its ePHI) and an Emergency Mode Operation Plan (the process of remaining in operation until the practice or health provider organization, its information processing system, or ePHI is restored). For most small health practices, such Disaster Recovery and Emergency Mode Operation Plans will be relatively straightforward. Most small health practices can remain closed or without access to their ePHI for a few days without posing undue harm to patients. However, small practitioners should consider the steps that would be necessary to restore their practices, its information processing system, or its ePHI. And practices should not just focus on major disasters. For example, the temporary loss of Internet service could effectively hinder practice operations. Practitioners should consider what they would do in the case of such minor disasters.

Emergency mode operations for a small health practice may entail locating a nearby practice (preferably with a compatible information processing system) which can be used as a temporary base of operations or a place to which to refer patients. Restoration may rest on being able to quickly contact vendors who can supply necessary repairs or equipment. Practices can use the disaster preparedness materials accompanying this section to chart a preparedness plan.

In any practice that utilizes ePHI, the success of both Emergency Mode Operation and Disaster Recovery Plans will be contingent on the ability of the practice to restore that information through the use of back-up copies. (See Step 7) After the event, the practice should prepare a detailed record of the event which includes: (1) a list of patient records affected; (2) a description of the recovery efforts taken; and (3) a description of the outcomes of these recovery efforts. In the case of reconstruction of information, it should be documented, including the method used and the basis for authentication. If the practice discloses patient information with missing portions or that is reconstructed due to a disaster, it should disclose the associated disaster record also.

The Institute for Business & Home Safety's Open for Business TM project offers a format for the development of a small business disaster recovery plan including forms provided on the following pages (also useful for compliance with some other HIPAA Security Regulation requirements).

Under a small practice Emergency Mode Operation Plan, the practice Security Officer may be responsible for:

- Reloading and restoring operating programs and practice files.

- Employee contact and coordination.

- Patient contact and scheduled appointment coordination.
- Vendor and business partner contact.
- Coordination of deliveries.
- Contact with computer hardware or software vendor or programming consultant to secure new hardware or software or restore operation of the system.
- Securing, if necessary, a temporary work site, with all necessary equipment (including computers) and utilities (including telephones) and coordinating the move of staff and equipment to that location.
- Maintaining the availability of a temporary practice location or practice to which patients can be referred through, for example, an agreement with a nearby practice having compatible operating software on which practice records can be accessed and through which operations (e.g., billing and ordering) can be continued in the normal manner.
- Documenting all such incidents and the practice's response and maintaining the documentation with the practice's HIPAA Security Records.
- A formal Application and Data Criticality Analysis to determine the most important programs or files to reload first in order to restore operations and protect patient welfare (in line with Implementation Specification 7e – See Step 3) may not be entirely appropriate given the size of information processing systems in a small practice. However, it may be advantageous for the practice Security Officer to load programs in the following order:
    - Basic operating system.
    - Virus protection packages (to ensure all subsequently loaded files are scanned for viruses prior to installation).
    - Practice management or other function programs necessary for practice.
    - Practice files.

(Disaster preparedness forms from the Institute for Business & Home Safety's ® Open for Business SM property protection and business continuity planning tool are provided on pages 27-37. An Internet based, interactive version of the Institute for Business & Home Safety's® Open for BusinessSM property protection and business continuity planning tool is available to customers of the Institute's member insurance and reinsurance companies. To view a list of these companies, visit www.ibhs.org. A print version of the tool, available to the general public, is also available at this Web site.)

Adopt Practice Contingency Plan using model Document 3, if desired, adapting the policy to reflect state law, the requirements of the practice or other pertinent factors. If additional action, *activity, or assessment is required to be documented, attach a written record. The Institute for Business & Home Safety's® Open for BusinessSM forms can be used for such supplemental information.*

(Document 3)

PRACTICE CONTINGENCY PLAN
(Emergency Mode Operation and Disaster Recovery Plan)

In the event that operation of the practice is jeopardized because electronic Protected Health Care Information (ePHI) is lost or substantially impaired (due to catastrophic computer system malfunction, physical damage to the practice, or other factors), it is the policy of the practice to restore practice operations within a reasonable period. The practice Security Officer will be responsible for:

- Reloading and restoring operating programs and practice files.
- Employee contact and coordination.
- Patient contact and scheduled appointment coordination.
- Vendor and business partner contact.
- Coordination of deliveries.
- Contact with computer hardware or software vendor or programming consultant to secure new hardware or software or restore operation of the system.
- Securing, if necessary, a temporary work site with all necessary equipment (including computers) and utilities (including telephones) and coordinating the move of staff and equipment to that location.
- Maintaining the availability of such a temporary practice location or practice to which patients can be referred through, for example, an agreement with a nearby practice having compatible operating software on which practice records can be accessed and through which operations (e.g., billing and ordering) can be continued in the normal manner.
- Documenting all security incidents and the practice's response and maintaining the documentation with the practice's HIPAA Security Records (See Privacy and Security Incident Form).
- Other:

(Notations: ____

____
)
____

Policy adopted ____________________
(Date)

(Document 3-1)

EMERGENCY CONTACTS
(SM)Institute for Business & Home Safety®

Keep this emergency contact list available for you and your employees in the event of an emergency. Attach a list of employee emergency contact numbers to this form.

Local Police Department: ______________________________

Local Fire Department: ______________________________

Ambulance Service: ______________________________

Hospital: ______________________________

Insurance Company: ______________________________

Agent: ______________________________

Policy Number: ______________________________

Telephone Company: ______________________________

Gas/Heat Company: ______________________________

Electric Company: ______________________________

Building Manager: ______________________________

Building Security: ______________________________

Local Small Business Administration Office: ______________________________

Federal Emergency Management Agency Regional Office: Local Newspaper: ___________

Local Radio Stations: ______________________________

____

Local Television Stations: ______________________________

____

(Document 3-2)

DISASTER SUPPLY CHECKLIST
SM Institute for Business & Home Safety®

Use this check-off list to ensure you have all the supplies you need in the event of a disaster.

	Need	Have
NOAA Weather Radio		
First Aid Kit		
Flashlights/Batteries		
Waterproof Plastic Bags		
Camera/Film		
Pens/Pencils/Paper		
Water/Food supplies		
Generator		
Mops/Pails		
Tool kit (basic tools, gloves, etc.)		
Contact sheets		

Other:		

INSTITUTE FOR Business & Home Safety

(Document 3-3)

INSURANCE COVERAGE DISCUSSION FORM

SM Institute for Business & Home Safety®

Use this form to discuss your insurance coverage with your agent. Having adequate coverage now will help you recover more rapidly from a catastrophe.

Insurance Agent: ____

Address: ____

Phone: ____________ Fax: ____________ Email: ____________________

INSURANCE POLICY INFORMATION

Type of Insurance	Policy No.	Deductibles	Policy Limits	Coverage (General Description)

YES NO

Do you need Flood Insurance?

Do you need Earthquake Insurance?

Do you need Business Income and Extra Expense Insurance?
Other disaster-related insurance questions:

____

(Document 3-4)

CREDITOR CONTACT INFORMATION
^{SM} Institute for Business & Home Safety®

Use this form to keep a list of the major creditors you need to contact in the event of a disaster. Make additional copies as needed. Keep one copy of this list in a secure place on your premises and another in an off-site location.

Bank Name:

Street

Address:

City: State:_______Zip: ________

Phone: Fax: Email:

Contact Name: Account Number:

Bank Name:

Street

Address:

City: State:_______Zip: ________

Phone: Fax: Email:

Contact Name: Account Number:

Company Name

Street Address:

City: State:_______Zip: ________

Contact Name: Account Number:

CREDITOR CONTACT INFORMATION

$^{\text{SM}}$ **Institute for Business & Home Safety®**

Company Name ______________________________

Street Address: ______________________________

City: ____________________ State:_______Zip: ________

Contact Name: ____________________ Account Number: ____________

Company Name ______________________________

Street Address: ______________________________

City: ____________________ State:_______Zip: ________

Contact Name: ____________________ Account Number: ____________

Company Name ______________________________

Street Address: ______________________________

City: ____________________ State:_______Zip: ________

Contact Name: ____________________ Account Number: ____________

Company Name ______________________________

Street Address: ______________________________

City: ____________________ State:_______Zip: ________

Contact Name: ____________________ Account Number: ____________

INSTITUTE FOR
Business &
Home Safety

(Document 3-5)

SUPPLIER CONTACT INFORMATION
(SM)Institute for Business & Home Safety®

Use this form to:
I. *Keep a list of the major suppliers you need to contact in the event of a disaster.*

II. *Know what their disaster plans are in the event that they experience a disaster.*

Make additional copies as needed. Keep one copy of this form in a secure place on your premises and another in an off-site location.

1. Company Name: ____

Street Address: ____

City: ____________________________ State: _ Zip: ______________

Phone: ______________ Fax: ____________ Email: ______________

Contact Name: Account #:

Materials /Service Provided:

If this company experiences a disaster, we will obtain supplies/materials from the following:

1A. Company Name: ____

Street Address: ____

City: ____________________________ State: _ Zip: ______________

Phone: ______________ Fax: ____________ Email: ______________

Contact Name: Account #:

Materials /Service Provided:

2. Company Name: ____

Street Address: ____

City: ____________________________ State: _ Zip: ______________

Phone: ______________ Fax: ____________ Email: ______________

Contact Name: Account #:

Materials /Service Provided:

If this company experiences a disaster, we will obtain supplies/materials from the following:

2A. Company Name: ____

Street Address: ____

City: ____________________________ State: _ Zip: ______________

Phone: ______________ Fax: ____________ Email: ______________

Contact Name: Account #:

Materials /Service Provided:

SUPPLIER CONTACT INFORMATION (continued)
(SM)Institute for Business & Home Safety®

3. Company Name: ____

Street Address: ____

City: ____________________________ State: _ Zip: ______________

Phone: ______________Fax: __________Email: ______________

Contact Name: Account #:

Materials /Service Provided: ____________________________________

If this company experiences a disaster, we will obtain supplies/materials from the following:

3A. Company Name: ____

Street Address: ____

City: ____________________________ State: _ Zip: ______________

Phone: ______________Fax: __________Email: ______________

Contact Name: Account #:

Materials /Service Provided: ____________________________________

4. Company Name: ____

Street Address: ____

City: ____________________________ State: _ Zip: ______________

Phone: ______________Fax: __________Email: ______________

Contact Name: Account #:

Materials /Service Provided: ____________________________________

If this company experiences a disaster, we will obtain supplies/materials from the following:

4A. Company Name: ____

Street Address: ____

City: ____________________________ State: _ Zip: ______________

Phone: ______________Fax: __________Email: ______________

Contact Name: Account #:

Materials /Service Provided: ____________________________________

(Document 3-6)

COMPUTER HARDWARE INVENTORY

^{SM} Institute for Business & Home Safety®

Use this form to:

- *Log your computer hardware serial and model numbers. Attach a copy of your vendor documentation to this form.*
- *Record the name of the company from which you purchased or leased this equipment and the contact name to notify for your computer repairs.*
- *Record the name of the company that provides repair and support for your computer hardware.*

Make additional copies as needed. Keep one copy of this list in a secure place on your premises and another in an off-site location.

Hardware (CPU, Monitor, Printer, Keyboard, Mouse)	Hardware Size, RAM & CPU Capacity	Model Purchased	Serial Number	Date Purchased	Cost

COMPUTER HARDWARE INVENTORY (continued)

SM Institute for Business & Home Safety®

Hardware Vendor or Leasing Company Information

Company Name: ______________________________

Street Address: : ______________________________

City: : ____________________ State: __________ Zip Code: ________

Phone: : ______________________________

Fax: : ______________________________

E-mail: ______________________________

Contact Name: ______________________________

Account Number: ______________________________

Hardware Supplier/Repair Vendor Information

Company Name: ______________________________

Street Address: : ______________________________

City: : ____________________ State: __________ Zip Code: ________

Phone: : ______________________________

Fax: : ______________________________

E-mail: ______________________________

Contact Name: ______________________________

Account Number: ______________________________

(Document 3-7)

COMPUTER SOFTWARE INVENTORY
SM Institute for Business & Home Safety ®

Use this form to:

- *Log your computer software serial and license numbers and attach a copy of your licenses to this document.*
- *Record the name of the company from which you purchased or leased this software and the contact name to notify for your software support.*
- *Record the name of the company where you store back-ups of your computer information, the name of your contact, and how often back-ups are sent to this location.*

Make additional copies as needed. Keep one copy of this form in a secure place on your premises and another in an off-site location.

Software Title and Version	Serial/Product ID Number	No. of Licenses/ License Numbers	Date Purchased	Cost

ADDITIONAL DISASTER PLANNING RESOURCES

Open for Business: A Disaster Planning Toolkit for the Small Business Owner.^{SM} Developed by the Institute for Business & Home Safety® and the U.S. Small Business Administration. Institute for Business & Home Safety®, 4775 E. Fowler Avenue, Tampa, FL 33617, Voice - (813) 286-3400, Fax - (813) 286-9960. E-mail: info@ibhs.org. Downloadable at www.ibhs.org/business_protection/

Emergency Management Guide for Business & Industry: A Step-by-Step Approach to Emergency Planning Response and Recovery for Companies of All Sizes. Sponsored by a public partnership with the Federal Emergency Management Agency. Downloadable at www.fema.gov/pdf/library/bizindst.pdf

Step 4: Workstation Policy.

The HIPAA Security Regulation requires practices to implement administrative policies governing the use of information system workstations, thereby protecting the ePHI they are used to process. Access to ePHI should be authorized only by staff members who have successfully undergone a security clearance. (In a small practice, the routine background check required as part of the employment application may be sufficient. The objective is to ensure that ePHI is not being handled by a convicted felon.) Access to ePHI should come in the form of a user ID and password for the practice information processing system (or through the use of new technology such as fingerprint recognition systems, "card swipe" devices, or token-based devices) with authorized workforce advised to use "strong" passwords (designed to be hard to guess, with a minimum of eight characters, numbers, or symbols incorporated, with at least one capital letter required, and passwords or ID used for other purposes [such as bankcards] banned as passwords or IDs for the practice system). Workforce members should be required to memorize their password and ID and be barred from posting it (such as with a sticky note) either on or near their workstation where it might be seen by an unauthorized person. Authorized workforce users should be required to log off their workstations if they leave the workstation for more than a few minutes. Workforce members should be barred from logging on with another workforce member's password or ID or providing their password or ID to any other person. Should a workforce member terminate employment (or under any other applicable circumstances), the workforce member's user ID and password should be removed from the system in a timely manner, and the practice Security Officer should check thereafter to ensure that the password and ID are no longer recognized by the system.

In line with the HIPAA Security Regulation, access to ePHI should be the minimum necessary, and access should be role-based. In small practices it will often be necessary for all staff members to have access to all levels of data. However, if role-based access (with different levels of access for front desk persons, billing staff, patient records clerks, etc.) is practical in the practice, it should be implemented. Adjust the system to provide the appropriate level of access when a given ID and password are entered. In such practices, access for each staff member should be reviewed periodically as well as when any staff member is promoted or changes jobs within the practice to assure access continues to be appropriate. Practices with such multi-tiered access must ensure that at least some practitioners or staff have access codes that can provide emergency (so-called "break the glass") access to ePHI (as required under *Implementation Specification 14b*; see cross reference Step 4).

Workstations should be logged off during non-working hours. Workforce should be diligent to ensure that visitors to the office, including delivery or repair persons, do not view ePHI on workstations. Privacy or anti-glare screens should be used on all workstations. Ideally, workstations used to access confidential information should be located only in controlled areas. Fax machines, if operated independent of the office information processing system, are not covered by the HIPAA Security Regulation but are covered if operated as a part of such system. Electronic PHI printed on such a fax or on the office printer should be guarded with the same diligence as ePHI on a workstation screen. Electronic PHI on digital ophthalmic devices, cell phones, PDAs, or other devices in the practice must also be protected. Home office or other remote workstations used to access ePHI are subject to the same security requirements as in-office computers.

Regular Information System Activity Reviews, including any audit logs, access reports, and security incident tracking reports that can be produced by the practice information-processing system, are required under *Implementation Specification 1d* to determine if any electronic confidential information is being used or disclosed in an inappropriate manner and to ensure that any such systems are activated and operating properly. (See cross reference, Step 4.)

Adopt Workstation Use and Security Policies using model Document 4, if desired, on the following page as an example, adapting the policy to reflect state law, the requirements of the practice, or other pertinent factors. Workforce Password and USER ID Log, Document 4-1, and/or Workforce ePHI Access Log, Document 4-2, may be used as documentation. Reminder: include only those policies or procedures that will be used by the practice for compliance.

(Document 4)

WORKSTATION USE AND SECURITY POLICY

It is the policy of the practice to:

- Ensure all members of its workforce have appropriate access to electronic Protected Health Information (ePHI) and to prevent those workforce members who do not have access from obtaining access to ePHI.
- Implement, as appropriate, procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed.
- Implement, as appropriate, procedures to determine that the access of a workforce member to ePHI is appropriate.
- Implement, as appropriate, procedures for terminating access to ePHI when the employment of a workforce member ends or as required by determinations made as specified in the Security Rule.
- Implement policies and procedures for authorizing access to ePHI that are consistent with the applicable requirements of the Security Rule.
- Implement, as appropriate, policies and procedures for granting access to ePHI, for example, through access to a workstation, transaction, program, process, or other mechanism.
- Implement, as appropriate, policies and procedures that, based on the practice's authorization policies, establish, review, and modify a user's right of access to a workstation, transaction, program, or process.
- Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI.
- Implement physical safeguards for all workstations that access ePHI to restrict access to authorized users.
- Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs granted access rights as specified in the Security Rule.
- Assign a unique name and/or number for tracking user identity.
- Establish and implement as needed procedures for obtaining necessary ePHI during an emergency.
- Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.
- Other

(Notations: ____)

Policy adopted _________________
(Date)

(Document 4-1)

WORKFORCE PASSWORD AND USER ID LOG			
WORKFORCE MEMBER NAME	**DATE PASSWORD ASSIGNED**	**DATE USER ID ASSIGNED**	**DATE DELETED**

(Document 4-2)

WORKFORCE ePHI ACCESS LOG

(For use in practices that authorize various levels of access to workforce members based on job function.)

STAFF MEMBER	SUPER-USER (ALL LEVELS)	APPOINT-MENTS	PATIENT FILES	INSURANCE	OTHER
	______/______ AUTH/TERM DATE	______/______ AUTH/TERM DATE	______/______ AUTH/TERM DATE	______/______ AUTH/TERM DATE	______/______ AUTH/TERM DATE
	______/______ AUTH/TERM DATE	______/______ AUTH/TERM DATE	______/______ AUTH/TERM DATE	______/______ AUTH/TERM DATE	______/______ AUTH/TERM DATE
	______/______ AUTH/TERM DATE	______/______ AUTH/TERM DATE	______/______ AUTH/TERM DATE	______/______ AUTH/TERM DATE	______/______ AUTH/TERM DATE
	______/______ AUTH/TERM DATE	______/______ AUTH/TERM DATE	______/______ AUTH/TERM DATE	______/______ AUTH/TERM DATE	______/______ AUTH/TERM DATE
	______/______ AUTH/TERM DATE	______/______ AUTH/TERM DATE	______/______ AUTH/TERM DATE	______/______ AUTH/TERM DATE	______/______ AUTH/TERM DATE
	______/______ AUTH/TERM DATE	______/______ AUTH/TERM DATE	______/______ AUTH/TERM DATE	______/______ AUTH/TERM DATE	______/______ AUTH/TERM DATE
	______/______ AUTH/TERM DATE	______/______ AUTH/TERM DATE	______/______ AUTH/TERM DATE	______/______ AUTH/TERM DATE	______/______ AUTH/TERM DATE
	______/______ AUTH/TERM DATE	______/______ AUTH/TERM DATE	______/______ AUTH/TERM DATE	______/______ AUTH/TERM DATE	______/______ AUTH/TERM DATE
	______/______ AUTH/TERM DATE	______/______ AUTH/TERM DATE	______/______ AUTH/TERM DATE	______/______ AUTH/TERM DATE	______/______ AUTH/TERM DATE
	______/______ AUTH/TERM DATE	______/______ AUTH/TERM DATE	______/______ AUTH/TERM DATE	______/______ AUTH/TERM DATE	______/______ AUTH/TERM DATE
	______/______ AUTH/TERM DATE	______/______ AUTH/TERM DATE	______/______ AUTH/TERM DATE	______/______ AUTH/TERM DATE	______/______ AUTH/TERM DATE

Step 5: Security Officer.

Practices must identify a Security Officer who is responsible for the development and implementation of the policies and procedures required under the Security Regulation. The practice Security Officer should be adequately trained in the Security Regulation, reporting and response requirements, and technical aspects of the office computer system. The individual serving as the practice's HIPAA Privacy Officer may be named the practice's Security Officer as many of the regulatory requirements and responsibilities overlap. Duties may include:

- Developing and managing administrative processes, including policies and procedures.
- Understanding and working with staff responsible for physical security, including security consultants and vendors.
- Maintaining records documenting the practice's rationale for its security policies and procedures, the policies and procedures themselves, and related forms and records.
- Coordinating policy and procedure development, internal complaint processing, and enforcement with the practice Privacy Officer.
- Collaborating with the practice regarding the analysis and resolution of joint security and privacy issues that arise.
- Communicating with all members of the workforce, to include providing training, selecting controls, and describing the risk analysis to the practice staff and management.

If a staff person is appointed Security Officer, the appointment should be noted in the staff member's personnel records. A salary adjustment may be considered. A third party, outside the practice, may be retained as the Security Officer if desired.

Appoint practice Security Officer using model Document 5, if desired, as an example, including only those duties applicable to the practice. Policies should reflect state law, the requirements of the practice, or other pertinent factors.

(Document 5)

SECURITY OFFICER

The optometric practice of ____ hereby appoints ____ as Security Officer with duties to include:

- Developing and managing administrative processes, including policies and procedures.
- Working with staff responsible for physical security, including security consultants and vendors.
- Maintaining records documenting the practice's rationale for its security policies and procedures, the policies and procedures themselves, and related forms and records.
- Coordinating policy and procedure development, internal complaint processing, and enforcement with the practice Privacy Officer.
- Collaborating with the practice regarding the analysis and resolution of joint security and privacy issues that arise.
- Communicating with all members of the workforce, to include providing training, selecting controls, and describing the risk analysis to the practice staff and management.
- Other: ____

(Notations: ____
____)

Policy adopted _______________________
(Date)

Step 6: Facility Controls.

The practice must develop and use procedures for securing physical access to the office itself (e.g., locking doors, computers, and storage areas). The practice will also need to develop and implement policies and procedures to limit physical access to the practice's computer systems and the areas in which they are housed while still ensuring that properly authorized access is allowed.

The practice needs to assess the overall physical security needs of the practice, including facility location, layout, design, and construction. Small practices should consider the need for and reasonableness of stronger or different entry door locks, alarm systems, and anti-intrusion devices. Identification badges, suggested to help restrict access in larger facilities, may not be appropriate in a small practice. Similarly, role-based access to various areas may not always be practical in a small practice. However, adequate control of patients and other visitors in the practice is essential. One of the best ways to secure a small practice during offices hours is to have workforce members located in places where they can see and control what is going on in the practice. In many small practices, the receptionist may play a central role in controlling access and ensuring only authorized individuals have access to confidential information. In most small practices, space is at a premium, and it is important to design policies and procedures in a manner that does not interfere with the ability to provide timely, quality care to patients.

To comply with the HIPAA physical safeguard standards, practices must have written policies and procedures. The policies and procedures do not have to be lengthy or elaborate, but they do need to be properly documented. Practices should also document repairs and modifications to the physical components of their facilities that are related to security (for example, hardware, walls, doors, and locks).

Adopt Facility Controls Policy using model Document 6, if desired, on the following page as an example, adapting the policy to reflect state law, the requirements of the practice, or other pertinent factors. Practices may use model Document 6-1, Maintenance Record, if desired, to document any repairs and modifications made to the physical components of its facility that are in line with its Security Management Policy or in response to changes in the practice environment.

(Document 6)

FACILITY CONTROLS POLICY

It is the policy of the practice to:

- Limit physical access to electronic information systems and the facility or facilities in which they are housed while also ensuring that properly authorized access is allowed.
- Safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft through the use of entry door locks, alarm systems, anti-intrusion devices, and other physical protective measures.
- Periodically assess the overall physical security needs of the practice, including facility location, layout, design, and construction.
- Periodically assess any need for and reasonableness of stronger or different entry door locks, alarm systems, and anti-intrusion devices.
- Adequately confirm the identities of visitors to the practice.
- Locate workforce members in places where they can see and control access to the practice and ensure that only authorized individuals have access to confidential information.
- Repair and modify the physical components of a facility that are related to security (for example, hardware, walls, doors, and locks) as necessary. (See Document 6-1).
- Other: ____

(Notations: ____
____)

Policy adopted ________________________
(Date)

(Document 6-1)

MAINTENANCE RECORD

The practice implements repairs and modifications to the physical components of its facility in line with its facility security plan or in response to changes in the practice environment. Such repairs and modifications are documented below.

DATE	REPAIR/ MODIFICATION	CONTRACTOR/ INSTALLER	DEVICE MFGR SERIAL#	COMMENT

Step 7: Data Control Procedures.

Practices must establish and implement procedures to create and maintain retrievable exact copies of ePHI. All electronic practice records should be backed up regularly to disk, CD-ROM, DVD, tape, or other appropriate media with back-up copies stored off-site (preferably at least 50 miles from the practice) in a secure location, preferably in a fire-resistant data safe. Many data experts recommend rotating more than one back-up disk or CD-ROM so more than one copy of the practice records exists (e.g., one for each day of the week). Files may be backed up "manually" with the practice Security Officer creating backup copies or automatically by activating software features that regularly create back-up copies on a predetermined schedule (in which case, the changing of the back-up media is the only manual action required). New on-line automatic data back-up services might also be considered.

There are several kinds of back-ups. A *full back-up* makes a copy of all data on a drive. An *incremental back-up* file is a copy only of changes that have occurred since the last full or incremental back-up. An incremental back-up takes less time than a full back-up and might be used on a daily basis. A *differential back-up* may be used to cumulatively record the changes filed in more than one incremental back-up (e.g., the changes that occur over a two or three day period). A typical manual back-up process might involve removing the tape that ran the previous day, labeling the tape (e.g., Server or System name, Day, Date), properly storing the back-up tape, inserting the tape for the present day, and logging that the back-up was completed with the date and name or initials of the person changing the media.

An example data back-up schedule follows:

- Daily incremental back-up using a set of five rotated media (one for each day).
- Weekly differential back-up of all files, regardless of whether they have changed since the last full backup, using two different media, rotated monthly.
- Monthly full back-up.
- One yearly back-up tape.

Data should be backed up prior to the moving of any equipment or media containing ePHI as data may be lost or damaged during movement (*Implementation Specification 13-d*, see cross reference, Step 7).

Each practice should maintain an up-to-date inventory of all of its computer equipment and related software as required under the Contingency Plan (Documents 3-6 and 3-7 and under *Implementation Specification 3-a: Authorization and/or Supervision*, see cross reference Step 4). Depending on the risk identified in the practice Risk Assessment, that may include keeping track of CDs, DVDs, disks, and other forms of media that may be shared throughout the office to facilitate a quick response should a workforce member bring a malicious virus into the practice after using a disk at home.

Implementation Specification 13-c (see cross reference Step 7) indicates practices should keep a record of any ePHI or office equipment (such as laptop computers or cell phones) storing ePHI that are taken off the premises (for example, records or billing codes taken from the practice for work at home by a billing clerk or laptop computers used for a presentation at a meeting). This can be accomplished through the use of a formal log. Small practices may wish to restrict, by policy, who is authorized to take hardware or software from the practice and for what purposes, stipulating that the hardware and software be used only in HIPAA secure environments such as outlined under the practice Workstation Management Policy (Step 4). Practices may wish to consider labeling or tagging computer hardware or software to make it more identifiable if lost or utilize new tracking devices for hardware.

Each practice must implement policies and procedures to address the final disposition of ePHI and/or the hardware or electronic media on which it is stored. The practice must ensure proper disposal of electronic confidential information. Simply deleting a file or reformatting a hard drive is not sufficient. Many current examples of privacy breaches revolve around an old computer or equipment that was discarded or donated to another organization without being cleansed (or "sanitized”) of data first. Technological advances have made it difficult to easily erase information. A practice should carefully consider methods to correctly dispose of hardware containing ePHI. Some methods are fairly straightforward and inexpensive, e.g. destroying CDs by scratching them deeply three or four times and then breaking them in half. Paper documents containing confidential or Protected Health Information should be securely stored until they are destroyed by shredding, pulping, or burning. Prescription bottles, labels, CD-ROMs or other items with ePHI that cannot go into a paper shredder must be properly destroyed through burning, pulverization, or high-pressure compression. Reformatting of CD-ROMs is not sufficient.

Common practices include:

- “Sanitizing” hard disk drives and other types of “non-volatile” computer memory devices at least three times with random patterns of “1s” and “0s” before they are sold, given away, re-used, or thrown away.
- “Degaussing” hard drives, floppy disks, and back-up tapes through the application of a strong magnetic field prior to disposal.
- Physically damaging media beyond repair by drilling a hole in or cutting media with wire cutter or scissors prior to disposal.
- Physically damaging optical disks prior to disposal.

Small practices must implement procedures for removal of ePHI from electronic media before the media are made available for re-use. Just as it is critical to sanitize equipment when disposing of computer hardware or similar devices, it is important to assure that storage media, such as disks, CDs, and DVDs are carefully cleansed before reuse. The practice may reuse its own media. However, the practice should destroy all media that it no longer needs. Common practices include:

- Storage media (disks, CDs, DVDs) that contains ePHI may be reused, but only within the practice.
- Any and all electronic media that may have been used for ePHI will be cleansed with a strong magnetic instrument designed for that purpose or other appropriate means before that media is used in the practice.

- No storage media may be taken from the practice for reuse outside the practice.

Adopt Data Control Policy using model Document 7, if desired, on the following page as an example, adapting the policy to reflect state law, the requirements of the practice, or other pertinent factors. Data Back-up Plan, Document 7-1, may be used, if appropriate, as a supplement.

(Document 7)

DATA CONTROL POLICY

It is the policy of the practice to:

- Create and maintain retrievable exact copies of electronic Protected Health Information (ePHI). (Back-up procedures may be attached.)
- Document the receipt and removal of hardware and electronic media that contain ePHI into and out of the facility and movement of these items within the facility.
- Require proper disposition of ePHI and/or the hardware or electronic media on which it is stored. (Consider documenting disposal of software and/or hardware.)
- Remove ePHI from electronic media before the media are made available for reuse.
- Other:
- Other: ____

(Notations: ____
____)

Policy adopted ________________________
(Date)

(Document 7-1, supplemental, if required)

DATA BACK-UP PLAN

It is the policy of the practice to routinely make duplicate copies (back-ups) of electronic Protected Health Information (ePHI) on a regular basis using one of the following options:

- Automatically (daily, weekly, etc.), using Internet-based data back-up service.
- Automatically, in-office to disk/CD-ROM or other appropriate media.
- Manually, in-office by the practice Security Officer (daily, weekly, etc.).
- Other: ____

Back-up media are stored on-/off-site at the following location: (Name, address, city, state, ZIP code, telephone number, other contact information, exact location [e.g., address if off-site, data safe, file drawer]): ____

____

(Notations: ____

____

____

(Note back-up schedule [daily, weekly, etc.] and other pertinent information.)

The practice tests its data back-up procedures periodically to ensure that exact copies of confidential data can be retrieved and made available as well as whenever computer hardware or software are modified. (Documentation of testing may be attached.)

Policy adopted ______________________
(Date)

Step 8: Business Associates and Business Associate Agreements.

Practices must have signed Business Associate Agreements with certain outside parties that have access to the practice’s confidential information, providing satisfactory assurances that the associates will appropriately safeguard the practice's PHI. Practices may enter into numerous Business Associate Agreements, each with customized activities, processes and expectations. Thus, practices should keep a record of the Business Associate Agreements to which they are a party (as either a covered entity or as a business associate) and their effectiveness and terms. Larger practices may also consider implementing a procedure for approval and authorization of Business Associate Agreements requested from third parties. In appropriate circumstances, legal counsel should be consulted to review Business Associate Agreements requested by outside entities or vendors. Many times Business Associate Agreements are not required and a practice would be well within its rights to decline to enter into a Business Associate Agreement with a third party and thereby avoid the administrative and contractual obligations such an agreement would otherwise impose on the practice.

The HITECH Act, enacted in 2009 as part of the American Reinvestment and Recovery Act, now applies the Security Regulation directly to business associates. Thus, a practice's business associates (and their subcontractors who receive, transmit, maintain or create PHI on their behalves) must now follow all of the above Security Regulation standards. This means the practice's business associates have the same security obligations as the practice and must appoint their own security officers and train their employees on the protection and safeguarding of PHI like any covered entity under HIPAA. Accordingly, when entering into relationships with business associates who receive, create, maintain or transmit a practice's PHI, the practice should conduct "due diligence" with respect to each business associate to ensure the business associate has the appropriate security standards, safeguards and policies in place and that they are in compliance with the Security Regulation. This is important because under the Final Rule, which was released in January 2013, a covered entity such as an optometry practice may be held vicariously liable for the actions of its business associates who mishandle the practice's PHI. Thus, practices should request and thoroughly review a business associate's security policies, procedures and protocols and do their best to ensure that the business associate is in compliance with the Security Regulation before entering into a Business Associate Agreement with another entity.

To the extent a practice's business associate is working with vendors or subcontractors who will also handle the practice's PHI, those subcontractors, too, are now subject to HIPAA's Security Regulation. These subcontractors must follow the same security standards, safeguards and requirements as any covered entity under HIPAA. Moreover, there is a question whether the "vicarious liability" discussed above could be imputed to a practice all the way up the chain of the business associate's subcontractors, such that a practice could be liable for even the actions of a distant subcontractor who mishandled the practice's PHI. Therefore, to the extent possible, practices should determine up front exactly who each of their business associates will be working with in connection with the practice's PHI. Practices should also ensure that their Business Associate Agreements require their business associates to in turn require their subcontractors to observe HIPAA's Security Regulation. A form of Business Associate Agreement incorporating such requirements is set forth below. This form of Business Associate Agreement should be entered into with the practice's business associates by September 23, 2013, which is the compliance date of the HIPAA Final Rule.

Obtain signed copies of Business Associate Agreements from all appropriate business associates and vendors using model Document 8, if desired, on the following pages as an example, adapting the document as necessary to reflect any additional requirements appropriate to the practice, state law, or other pertinent factors. Model Document 8 is designed to address requirements of both the HIPAA Privacy Rule and the HIPAA Security Regulation. Practices that have already implemented Business Associate Agreements in compliance with the HIPAA Privacy Regulation should replace those agreements with the document on the follow page or similar document that covers both requirements by September 23, 2013, as this is the compliance date of the Final Rule.

(Document 8)

BUSINESS ASSOCIATE AGREEMENT

THIS BUSINESS ASSOCIATE AGREEMENT ("Agreement") is made and entered into on this _____day of ______________, 2013, by and between _______________________________ ("Covered Entity"), and ________________________ ("Business Associate"). Covered Entity and Business Associate are sometimes referred to herein collectively as the "parties" and individually as a "party".

WHEREAS, Business Associate performs certain functions on behalf of and/or provides certain services that qualifies it as a "business associate" of Covered Entity pursuant to 45 C.F.R. § 160.103;

WHEREAS, in the performance of such functions and/or the provision of such services, Business Associate may require access to Protected Health Information (defined below) in possession, custody, or control of Covered Entity, or may create or receive Protected Health information on behalf of Covered Entity for the limited purposes identified in this Agreement;

WHEREAS, pursuant to the Federal Standards for Privacy and Security of Individually Identifiable Health Information, 45 C.F.R. Parts 160 and 164, as established under the Health Insurance Portability and Accountability Act (HIPAA), Covered Entity cannot disclose Protected Health Information to or authorize the creation or receipt of Protected Health Information on its behalf by Business Associate unless Covered Entity obtains from Business Associate satisfactory assurances that Business Associate will properly safeguard such information; and

WHEREAS, Business Associate is willing to provide such assurances to Covered Entity under the terms specified herein.

NOW, THEREFORE, the parties agree as follows:

I. Definitions.

(a) *Breach.* "Breach" shall have the same meaning as the term "breach" in 45 C.F.R. § 164.402.

(b) *Business Associate.* "Business Associate" shall mean ________________________.

(c) *Covered Entity.* "Covered Entity" shall mean ____________________________________.

(d) *Electronic Health Record.* "Electronic Health Record" shall have the same meaning as the term "electronic health record" in American Recovery and Reinvestment Act of 2009, § 13400(5).

(e) *Electronic Protected Health Information.* "Electronic Protected Health Information" shall have the same meaning as the term "electronic protected health information" in 45 C.F.R. § 160.103.

(f) *Electronic Transactions Rule.* "Electronic Transactions Rule" shall mean the regulations issued by HHS concerning standard transactions and code sets under 45 C.F.R. Parts 160 and 162.

(g) *HHS.* "HHS" shall mean the Department of Health and Human Services.

(h) *Privacy Rule.* "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Parts 160 and 164, subparts A and E.

(i) *Protected Health Information.* "Protected Health Information" shall have the same meaning as the term "protected health information" in 45 C.F.R. § 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

(j) *Required By Law.* "Required by Law" shall have the same meaning as the term "required by law" in 45 C.F.R. § 164.103.

(k) *Security Incident.* "Security Incident" shall have the same meaning as the term "security incident" in 45 C.F.R. § 164.304.

(l) *Security Rule.* "Security Rule" shall mean the Security Standards and Implementation Specifications at 45 C.F.R. Parts 160 and 164, subpart C.

(m)*Subcontractor.* "Subcontractor" shall have the same meaning as the term "Subcontractor" in 45 C.F.R. § 164.103.

(n) *Transaction.* "Transaction" shall have the meaning given the term "transaction" in 45 C.F.R. § 160.103.

(o) *Unsecured Protected Health Information.* "Unsecured protected health information" shall have the meaning given the term "unsecured protected health information" in 45 C.F.R. § 164.402.

II. Safeguarding Privacy and Security of Protected Health Information

(a) **Permitted Uses and Disclosures.** Business Associate is permitted to use and disclose Protected Health Information only as set forth below:

(i) **Functions and Activities on Covered Entity's Behalf.** To perform functions on behalf of Covered Entity as such functions are agreed upon by Covered Entity and Business Associate pursuant to an underlying agreement between the parties (the "Services Agreement").

(ii) **Business Associate's Operations.** For Business Associate's proper management and administration or to carry out Business Associate's legal responsibilities, provided that, with respect to disclosure of the Protected Health Information, either:

(A) The disclosure is Required by Law; or

(B) Business Associate obtains reasonable assurance from any other person or entity to which Business Associate will disclose Covered Entity's Protected Health Information that the person or entity will:

(1) Hold the Protected Health Information in confidence and use or further disclose the Protected Health Information only for the purpose for which Business Associate disclosed the Protected Health Information to the person or entity or as Required by Law; and

(2) Promptly notify Business Associate of any instance of which the person or entity becomes aware in which the confidentiality of the Protected Health Information was breached.

(iii)**Minimum Necessary.** Business Associate will, in its performance of the functions, activities, services, and operations specified above, make reasonable efforts to use, to disclose, and to request only the minimum amount of the Protected Health Information reasonably necessary to accomplish the intended purpose of the use, disclosure or request, except that Business Associate will not be obligated to comply with this minimum-necessary limitation of 45 C.F.R. § 164.502(b) if neither Business Associate nor Covered Entity is required to limit its use, disclosure or request to the minimum necessary. Business Associate and Covered Entity acknowledge that the phrase "minimum necessary" shall be interpreted in accordance with 45 C.F.R. § 164.502(b).

(iv)**Mitigation.** Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of the Protected Health Information by Business Associate in violation of the requirements of this Agreement and to assist Covered Entity's efforts to mitigate any such harmful effect.

(b) **Required Uses and Disclosures.** Business Associate shall disclose Protected Health Information (i) when required by the Secretary of DHHS under 45 C.F.R. Part 160, Subpart C to investigate or determine Business Associate's compliance with Subchapter C of 45 C.F.R., Subtitle A, and (ii) to Covered Entity, the individual or the individual's designee, as necessary to satisfy Covered Entity's obligations under 45 C.F.R. § 164.524(c)(2)(ii) and (3)(ii) with respect to the individual's request for an electronic copy of his or her Protected Health Information.

(c) **Prohibition on Unauthorized Use or Disclosure.** Business Associate will neither use nor disclose the Protected Health Information, except as permitted or required by this Agreement or in writing by Covered Entity or as Required by Law. This Agreement does not authorize Business Associate to use or disclose the Protected Health Information in a manner that will violate the Privacy Rule.

(d) Information Safeguards.

(i) **Privacy of Protected Health Information.** Business Associate will comply with the Privacy Rule to the extent applicable to Business Associate. The Business Associate's Privacy Rule safeguards must reasonably protect the Protected Health Information from any intentional or unintentional use, access or disclosure in violation of the Privacy Rule and limit incidental use, access or disclosure made pursuant to a use, access or disclosure otherwise permitted by this Agreement.

(ii) **Security of Electronic Protected Health Information.** Business Associate will comply with the Security Rule and will use appropriate administrative, technical, and physical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of Electronic Protected Health Information that Business Associate creates, receives, maintains, or transmits on Covered Entity's behalf as required by the Security Rule. Business Associate shall review and modify the security measures implemented in accordance with the above as needed to continue provision of reasonable and appropriate protection of Electronic Protected Health Information. Business Associate shall update documentation of such security measures in accordance with 45 C.F.R. § 164.316(b)(2)(iii) and shall designate a Security Officer and undertake appropriate training of its personnel in accordance with the Security Rule.

(e) **Subcontractors and Agents.** Business Associate will ensure that any of its Subcontractors and agents, to whom it provides Protected Health Information and/or Electronic Protected Health Information received from, or created or received by the Business Associate on behalf of, the Covered Entity agree to the same restrictions and conditions that apply to the Business Associate with respect to such information. Business Associate may permit a business associate that is a Subcontractor to create, receive, maintain, or transmit Electronic Protected Health Information on its behalf only if Business Associate obtains satisfactory assurances, in accordance with 45 C.F.R. § 164.314(a), that the Subcontractor will appropriately safeguard such information. Business Associate agrees that any of Business Associate's Subcontractors that create, receive, maintain or transmit Protected Health Information or Electronic Protected Health Information on behalf of Business Associate shall comply with the applicable requirements of 45 C.F.R. Part 164, Subpart C by entering into a contract or other arrangement with such Subcontractor that complies with 45 C.F.R. § 164.314(a)(2)(i).

(f) **Prohibition on Sale of Records.** Effective September 23, 2013, Business Associate shall not engage in any sale of Protected Health Information as defined in 45 C.F.R. § 164.501.

III. Compliance with Electronic Transactions Rule. If Business Associate conducts in whole or part electronic Transactions on behalf of Covered Entity for which HHS has established standards, Business Associate shall comply, and will require any Subcontractor it involves with the conduct of such Transactions to comply, with each applicable requirement of the Electronic Transactions Rule. Business Associate shall also comply with the National Provider Identifier requirements, if and to the extent applicable.

IV. Individual Rights.

(a) **Access.** Business Associate will make available Protected Health Information in accordance with 45 C.F.R. § 164.524, upon request from Covered Entity, so that Covered Entity may meet its access obligations under 45 C.F.R. § 164.524. Effective September 23, 2013, if the Protected Health Information is maintained electronically in a designated record set in the Business Associate's custody or control, then the Covered Entity shall have a right to obtain from Business Associate a copy of such information in an electronic format.

(b) **Amendment.** Business Associate will, upon receipt of written notice from Covered Entity, promptly amend or permit Covered Entity access to amend any portion of an individual's Protected Health Information that is in a designated record set in the custody or control of the Business Associate, so that Covered Entity may meet its amendment obligations under 45 C.F.R. § 164.526.

(c) **Disclosure Accounting.** Business Associate will make available the information required to provide an accounting of disclosures in accordance with 45 C.F.R. § 164.528, upon request from Covered Entity, to allow Covered Entity to meet its disclosure accounting obligations under 45 C.F.R. § 164.528. Business Associate will maintain the Disclosure Information for six (6) years following the date of the accountable disclosure to which the Disclosure Information relates.

(d) **Restriction Agreements and Confidential Communications.** Business Associate will comply with any agreement that Covered Entity makes that either (i) restricts use, access or disclosure of Covered Entity's Protected Health Information pursuant to 45 C.F.R. § 164.522(a), or (ii) requires confidential communication about Covered Entity's Protected Health Information pursuant to 45 C.F.R. § 164.522(b), provided that Covered Entity notifies Business Associate in writing of the restriction or confidential communication obligations that Business Associate must follow. Covered Entity will promptly notify Business Associate in writing of the termination of any such restriction agreement or confidential communication requirement and, with respect to termination of any such restriction agreement, instruct Business Associate whether any of Covered Entity's Protected Health Information will remain subject to the terms of the restriction agreement.

V. Reporting.

(a) **Breach or Unauthorized Use, Access or Disclosure.** Business Associate will report to Covered Entity any potential Breach of Unsecured Protected Health Information or any other non-permitted use, access or disclosure of Protected Health Information as soon as reasonably practicable and not more than five (5) calendar days after discovery of such potential Breach or such other non-permitted use, access or disclosure of such Protected Health Information. Business Associate will treat a potential Breach as being discovered in accordance with 45 C.F.R. § 164.410. Business Associate will make the report to Covered Entity's Privacy Officer. If a delay is requested by a law-enforcement official in accordance with 45 C.F.R. § 164.412, Business Associate may delay notifying Covered Entity for the applicable time period. Business Associate's report will include at least the following, provided that absence of any information will not be cause for Business Associate to delay the report:

(i) Identify the nature of the Breach or other non-permitted or violating use, access or disclosure by Business Associate or its Subcontractors;

(ii) Identify the Protected Health Information used, accessed or disclosed by Business Associate or its Subcontractors;

(iii) Identify which individual made the Breach or other non-permitted or violating use or access or received the non-permitted or violating disclosure;

(iv) Identify what corrective action Business Associate or its Subcontractors took or will take to prevent further Breaches or other non-permitted or violating uses, accesses or disclosures;

(v) Identify what Business Associate or its Subcontractors did or will do to mitigate any harmful effect of the Breach or other non-permitted or violating use, access or disclosure; and

(vi) Provide such other information, including a written report and risk assessment of Business Associate or its Subcontractors under 45 C.F.R. § 164.402, as Covered Entity may reasonably request.

(b) **Security Incidents.** Business Associate will provide notice to Covered Entity of any Security Incident of which Business Associate becomes aware. Business Associate will make the report in the form noted in Section V.(a) above and will cooperate with Covered Entity to promptly address and correct the Security Incident.

(c) **Notice.** For purposes of notifying Covered Entity of privacy Breaches, Security Incidents or an unauthorized use, access or disclosure of Protected Health Information, notices shall be deemed given when properly addressed to a party's privacy contact upon the date of receipt if hand-delivered or emailed, or three (3) business days after deposit in the U.S. mail if mailed by registered or certified mail, postage prepaid, or one (1) business day after deposit with a national overnight courier for next business day delivery, or upon the date of electronic confirmation of receipt of a facsimile transmission.

(d) **Address for Notice.** Notice of a privacy Breach, Security Incident or unauthorized use, access or disclosure shall be communicated to Covered Entity as follows:

Contact Office: Privacy Office

____
____
____

Telephone: _____________________

Fax: _____________________

Email: _____________________

VI. Term and Termination.

(a) **Term.** The term of this Agreement shall be effective as of ________________, 2013, and shall terminate when the underlying Services Agreement between the parties has terminated, subject to obligations of the parties which extend beyond or survive such termination, including those obligations related to return or destruction of Protected Health Information upon termination of this Agreement.

(b) **Right to Terminate for Cause.** Covered Entity or Business Associate may terminate this Agreement if it determines, in its sole discretion, that the other party has breached any material term of this Agreement, and upon written notice to the breaching party of the breach, the breaching party fails to cure the breach within ten (10) calendar days after receipt of the notice. Any such termination will be effective immediately or at such other date specified in a notice of termination.

(c) **Right to Termination Upon Change in Regulations.** Either party may terminate this Agreement if amendment or addition to 45 C.F.R. Parts 160-64 affects the obligations under this Agreement of the party exercising the right of termination. The party so affected may terminate this Agreement by giving the other party written notice of such termination at least 90 days before the compliance date of such amendment or addition to 45 C.F.R. Parts 160-64.

(d) **Return or Destruction of Covered Entity's Protected Health Information as Feasible.** Upon termination of this Agreement, Business Associate will, if feasible, return or destroy all Protected Health Information received from, or created or received by the Business Associate or its Subcontractors on behalf of, the Covered Entity that the Business Associate or its Subcontractors still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of this Agreement to the information and limit further uses, accesses and disclosures to those purposes that make the return or destruction of the information infeasible. Business Associate will complete these obligations, and shall cause its Subcontractors to comply with these obligations, as promptly as possible, but in no event later than thirty (30) calendar days following the effective date of termination of this Agreement.

(e) **Continuing Privacy and Security Obligation.** Business Associate's obligation to protect, and to cause its Subcontractors to protect, the privacy and safeguard the security of Covered Entity's Protected Health Information as specified in this Agreement will be continuous and will survive termination or other conclusion of this Agreement.

VII. Indemnification.

(a) **Indemnification.** Business Associate agrees to indemnify, defend, and hold harmless Covered Entity and its employees, directors, officers, subcontractors, agents or other members of its workforce (each an "Indemnified Party") against all actual and direct losses or damages suffered by the Indemnified Party and all liability to third parties arising out of or in connection with any alleged breach of this Agreement by Business Associate or from any alleged negligence or wrongful acts or omissions of Business Associate, including failure of Business Associate to perform its obligations under this Agreement, under the Privacy Regulations or under the Security Rule. Accordingly, on demand, Business Associate shall reimburse any Indemnified Party for any and all actual and direct losses, liabilities, damages, lost profits, fines, penalties, costs or expenses (including reasonable attorney fees) which may be imposed upon any Indemnified Party by reason of any suit, claim, action, proceeding or demand by any third party resulting from Business Associate's breach of this Agreement.

VII. General Provisions.

(a) **Definitions.** All terms that are used but not otherwise defined in this Agreement shall have the meaning specified under HIPAA, including its statute, regulations and other official government guidance.

(b) **Inspection of Internal Practices, Books, and Records.** Business Associate will make its internal practices, books, policies, procedures and records relating to its use and disclosure of Covered Entity's Protected Health Information available to HHS to determine compliance with the HIPAA Rules.

(c) **Amendment to Agreement.** This Agreement may only be amended or modified by a written instrument signed by the parties. In the event of a change of applicable law, the parties agree to negotiate in good faith to adopt such amendments to this Agreement as are necessary to comply with such change in law.

(d) **No Third-Party Beneficiaries.** Nothing in this Agreement shall be construed as creating any rights or benefits to any third parties.

(e) **Interpretation.** Any ambiguity in this Agreement shall be resolved to permit Covered Entity and Business Associate to comply with the applicable requirements under HIPAA.

(f) **Supersession.** This Agreement shall supersede and replace in its entirety any Business Associate Agreement previously in place between the parties as of the date of this Agreement.

IN WITNESS WHEREOF, each of the undersigned has caused this Agreement to be duly executed in its name and on its behalf effective as of the date first above written.

"COVERED ENTITY"

____

____

By: ______________________________________

__________________________ [print name]

Its: ___________________________ [print title]

"BUSINESS ASSOCIATE"

____

____

By: ______________________________________

__________________________ [print name]

Its: ___________________________ [print title]

Step 9: Training.

Training and awareness on the security of ePHI are considered essential to compliance with the HIPAA Security Regulation. The Security Officer is free to determine the information appropriate for the training and the exact form the training takes. However, training on protection from malicious software, log-in monitoring, and password management are identified as implementation specifications. Trainees should be made aware of the need for adequate security in the practice (creating a "culture of security"). Security training requires education concerning the vulnerabilities of ePHI (as identified in the Risk Analysis) and the practice's policies and procedures to protect that confidential information (as outlined under the Risk Management Plan). A review of the security rule's standards and specifications would not be inappropriate. Additional "update" training must be provided to all staff "periodically" (many read that to mean annually) as well as in the event of any substantial change in the office environment (e.g., new software system). Training must be provided to new employees within a reasonable time after they join the practice. Training must be documented in the practice's HIPAA compliance records. Small practices may wish to select one of the following models:

- A very simple training program that might involve a discussion of each of the top five priority risks identified during the practice's Risk Analysis (Document 9-2, Example 1).
- A more comprehensive training program that might involve a review of each of the standards and specifications of the security rule using this manual as a guide (Document 9-2, Example 2).
- A more in-depth training curriculum as provided in Document 9-3.

It is recommended that practices also issue periodic security updates, informing the small practice's workforce of any changes that may affect the privacy and security of confidential information. The updates are also intended to inform the workforce as quickly as possible of any identified security incidents and any corrective action to prevent recurrence of a similar incident. Reminders may be provided at staff meetings, as well as via e-mails, bulletin board, or pamphlets. The practice should document the provision of the security reminders.

Adopt Security Awareness and Training Policy using model Document 9, if desired, on the following pages, as an example. Policies should reflect state law, the requirements of the practice, or other pertinent factors. Security Awareness Training Log, Document 9-1, may be used for documentation. Security Training Course, Example 1, Example 2, or Example 3, Documents 9-2 and 9-3, may be used as models for training. Security Reminders Log, Document 9-4, may be used to document reminders.

(Document 9)

SECURITY AWARENESS AND TRAINING POLICY

It is the policy of the practice to provide security training for all staff members (including management). Training includes protection from malicious software, log-in monitoring, password protection, vulnerabilities of the practice's ePHI as identified in the practice's Risk Analysis (see Document 2), the practice security policies and procedures, and other pertinent topics. The training also emphasizes the need for a "culture of security" in the practice.

- Training is to be provided to all current staff members prior to the April 20, 2005 implementation of the HIPAA Security Regulation and logged on the accompanying training chart.
- Training is provided to new staff members, including temporary employees, interns, externs, residents, and others with potential access to ePHI within a reasonable time after they join the practice.
- Training updates are provided all staff members periodically and in the event of a major change in the practice environment (new information processing hardware or software, practice move or reconfiguration, security breach).
- All staff members must provide signed acknowledgement of the training.
- Security reminders are provided by the practice Security Officer to all staff members periodically and/or in the event of any changes that may affect the privacy or security of ePHI in the practice. Such reminders are used to update staff members if a security breach or threat is identified or any corrective or preventive action is taken.
- Other: ____

(Notations: ____

____

____)

Policy adopted ____________________
(Date)

(Document 9-1)

SECURITY AWARENESS TRAINING LOG

TRAINING PROGRAM	STAFF MEMBER (PRINT)	STAFF MEMBER (SIGNATURE)	DATE

(Document 9-2)

SECURITY TRAINING COURSE, EXAMPLE 1

- Inform staff that the HIPAA Security Regulation covers the practice.
- Briefly review the regulation using the “introduction” page of this manual.
- Emphasize the need for an awareness of the need for security in the practice.
- Discuss each of the priority risks facing the practice based on the Risk Analysis.
    - (Risk one) ____
    - (Risk two) ____
    - (Risk three)____
    - (Risk four)____
    - (Risk five) ____
- Obtain signed documentation of training from staff.

SECURITY TRAINING COURSE, EXAMPLE 2

- Inform staff that the HIPAA Security Regulation covers the practice.
- Briefly review the regulation using the “introduction” page of this manual.
- Emphasize the need for an awareness of the need for security in the practice.
- Discuss each of the regulations using standards and implementation specifications or using the pages of this manual as an outline
- Obtain signed documentation of training from staff.

(Document 9-3)

SECURITY TRAINING COURSE, EXAMPLE 3

(Courtesy: Tom Walsh Consulting)

(1) Goal of Training.

(2) What is HIPAA?

(3) HIPAA Key Terms.

(4) Designation of Organized Health Care Arrangement.

(5) Why the concern over security?

(6) HIPAA Enforcement.

(7) What HIPAA Requires Health Care Practices to Do.

a. Identify ePHI.

b. Where do you find ePHI?

c. What does ePHI not include?

e. Learning through case scenarios.

f. Compliance process.

g. Accounting of disclosures.

h. Verification.

i. Compliance documentation.

j. State and federal law preemption analysis.

k. Research provision.

(8) Other HIPAA Requirements.

a. Authorization.

b. Notice of Privacy Practices.

c. Restrictions.

d. Access.

e. Staff Access.

f. Amendment.

g. Accounting of Disclosures.

h. Verification.

i. Compliance process and documentation.

(9) Integration of Security with Privacy

a. General Security Awareness.

b. System Access.

c. Computer Virus Protection.

d. Password Management.

(10) Questions and Answers.

(Document 9-4)

SECURITY REMINDER LOG	
DATE	SUBJECT

Step 10: Technical Security Mechanisms.

In addition to the administrative measures outlined under Step 4, the Security Regulation requires practices to take advantage of the technical mechanism that can be implemented on most information processing systems to protect ePHI.

As discussed under Step 4: Workstation Policy, practices are required to provide access to ePHI only through unique user identifications and passwords. Password protection software is included in most computer operating systems. If a practice does not currently have password protection software, it should be installed and unique user identifications and passwords should be issued to all practice workforce members.

Practices are also required to ensure "break the glass" access to ePHI in emergencies. In larger practices (in which not all workforce members have access to all information in the office computer system) the practice owner, practice Security Officer, or other appropriate person should be issued a master password and ID that can be used to provide access to all information in the system in emergency situations.

Practices must address the use of automatic log-off features, built into many operating systems, which generally take one of two forms. Most contemporary operating systems, like Microsoft XP Professional or Microsoft Windows 2000 Professional, can be set up to use screensavers programmed to appear if the computer goes unused for a few minutes, with an option to require users to enter their log-on information before resuming use of the computer. In addition, most operating systems provide "locks" that effectively freeze the keyboard and computer if the computer goes unused for a period of time (generally longer than the period used to trigger the screensaver). In either event, the user will be required to enter password and identification in order to unlock the computer and resume work. (It should be noted that older operating systems may not be as secure as newer systems and system updates may be necessary for compliance.) Additionally, one can manually "lock" a computer, by pressing CTL+ALT+DEL at the same time, and then selecting the "Lock Computer" option. This "lock" can be invoked at any time, when one might walk away from their computer, and doesn't want anyone else to access the computer while they are not present.

Practices must address whether or not to encrypt confidential information when it is sent via an "open" network such as the Internet. Practices should also consider whether encryption is appropriate to protect ePHI stored in office workstations or in other office equipment (such as laptops), particularly those that might be lost or stolen. Encryption means an electronic message has been "scrambled" so as to be understood only by the intended receiver. Encryption programs often "lock" files using a secure password. There are various levels of encryption. Virtually all e-mail services such as Hotmail or AOL utilize minimal levels of encryption. In part due to demand from health care providers, new, more secure e-mail services such as Tumbleweed have been introduced, utilizing more sophisticated levels of encryption. Virtual private networks use encryption and in-house servers to connect a limited number of related Internet users in a closed system. However, they may be more practical for large practices with multiple locations than for small practices. "Secure" Web sites used for commercial transactions (including insurance company sites used for claims processing and health provider Web portals such as VisionWeb) employ an advanced level of encryption. Practices using e-mail may wish to communicate with patients using e-mail only when the patient signs a statement that he or she understands that e-mail is not secure and may be intercepted and the patient’s privacy may be breached.

Practices are required to implement audit features that provide for the monitoring of workstation activity such as log-ons, log-offs, file access, updates, edits, or security incidents. Although in small practices (in which all workforce members have access to all information and are constantly logging onto the system) such logs may be of limited value, logging mechanisms should be activated and the log should be inspected periodically for evidence of improper log-ons (e.g., log-on after normal working hours) or other suspicious activity.

In addition to implementing policies and procedures discussed elsewhere in the Regulation, practices are required to secure the integrity of their ePHI by addressing mechanisms to authenticate that ePHI has not been altered or destroyed in any unauthorized manner including virus protections, firewall protections, access controls, or other appropriate safeguards. Regularly updated and properly used virus protections and firewalls are generally considered basic and essential to secure computer use in any system with Internet access.

In a small practice, required person or entity authentication (to verify that a person or entity seeking access to ePHI is the one claimed) can be accomplished with the previously discussed log-on password and audit trail. (Each time an employee logs on using their user name and password, they are authenticated.)

Required Transmission Security measures are intended to ensure information is only transmitted to the intended individual or entity. They may be accomplished by addressing integrity controls, the most common of which are:

- Properly configuring operating systems (including removing any unnecessary services or programs, closing extraneous networks ports, renaming the manufacturer’s defaults or system administrator accounts, and changing associated passwords when a software system is installed).
- Routinely checking for security bulletins and alerts that warn about newly discovered vulnerabilities or malicious codes (often available through software vendor Web sites or software programmer organizations such as the federally funded Software Engineering Institute (www.cert.org)).
- Routinely checking for and utilizing, as necessary, software updates (known as “patches” or “hot fixes”) offered by software makers to address such problems.
- Employing appropriate network security programs including firewalls, routers, and intrusion detection systems.
- Employing appropriate policies, procedures, and technology to protect wireless information processing equipment in the office. It can also be addressed through encryption as discussed above.

FOCUS: Technical Security Mechanisms for Wireless Networking and Mobile Devices:

Practices employing wireless networking should address the security implications of these networks. With the addition of new speed improvements and prominent security standards, wireless local area networks ("WLANs") are considered reliable and practical media. However, they are not without risks. These risks include:

- unsecured access points;
- hardware left with factory default settings or improperly configured, which is thus easy to crack;
- "eavesdroppers" listening to transmissions on the WLAN;
- forged MAC addresses of authorized clients to gain WLAN access;
- recording valid user's authentication transmission sequence and playing it back later to gain access;
- cracking WEP encryption keys;
- forced wireless device between user transmission and access point whereto traffic is routed and recorded;
- intentional interference with frequency; and
- flooding the network with MAC addresses or association attempts to use up process resources and cause users to disconnect.

There are numerous security mechanisms available for wireless technologies and practices should research options, taking into consideration their budget and bandwidth needs, before deploying a WLAN. Certain configuration options a practice may consider in setting and configuring its WLAN include:

- Configuring their WLAN such that the service set identifier ("SSID") will not be broadcast except to the most advanced wireless analysis applications. Furthermore, practices should consider naming their SSID so as to avoid attracting attention (example: "12345"; not: "General Hospital").
- WEP encryption.
- Allow only MAC addresses specified in an address list to associate with the WLAN.
- Limit range of WLAN so as to avoid high-risk areas such as waiting rooms.
- Utilize wireless user authentication such as remote authentication dial-in user service.

In addition, practices should be aware of security standards and may want to further research their applicability to their needs.

The use of mobile devices poses unique risks. Practices should consider implementing certain security techniques which can be leveraged to mitigate risks to mobile devices and include:

- Requiring a unique password to power on the device;
- Configuring the device to automatically lock up after a certain period of time;
- Implementing two-factor authentication for access to systems that contain PHI;

- Requiring password changes every 90 days;
- Establishing data encryption; and
- Allowing only signed applications to be loaded onto devices (S/MIME, Token-based).

Adopt Technical Security Mechanisms Policy using model Document 10, if desired, on the following pages, as an example, adapting the policy to reflect state law, the requirements of the practice, or other pertinent factors. Technical Security Mechanisms Log, Document 10-1, may be used for documentation.

(Document 10)

TECHNICAL SECURITY MECHANISMS POLICY

It is the policy of the practice to utilize all reasonable and appropriate technical security mechanisms on electronic information systems that maintain ePHI in the practice, including but not limited to:

- Access Controls to allow access only to those persons or software programs that have been granted access rights including but not limited to:
    - Unique User Identification: assigning each workforce member a username and password.
    - Emergency Access Procedures: appropriate safeguards to ensure appropriate emergency access to ePHI.
    - Automatic Logoff: electronic procedures that terminate sessions on practice workstations after a predetermined period of inactivity.
- Encryption and Decryption, as reasonable and appropriate to the practice.
- Audit Controls to record and examine activity in information systems that contain or use electronic protected health information.
- Integrity Controls to protect ePHI from improper alteration or destruction including but not limited to:
    - Mechanisms to authenticate ePHI.
    - Person or entity authentication to verify that a person or entity seeking access to ePHI is the one claimed.
    - Transmission security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network, addressing, as reasonable and appropriate to the practice, including but not limited to:
        - Integrity controls to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of.
        - Encryption of ePHI whenever deemed appropriate.
- Other: ____

(Notations: ____

____

____)

Policy adopted ________________________
(Date)

(Document 10-1)

TECHNICAL SECURITY MECHANISMS LOG

Indicate below the security-related information software functions installed and activated on practice information processing system as required or addressable under the HIPAA Security Regulation or, if a mechanism is not reasonable and appropriate to protect against reasonably anticipatable risks to ePHI, note any alternative measures and the reasons for their use. Also note the date when the feature was installed, activated, or last checked to be operational.

STANDARD OR SPECIFICATION	SOFTWARE FUNCTION	DATE INSTALLED OR ACTIVATED
Access Controls (Required)		
Unique User Identification (Required)		
Emergency Access Procedures (Required)		
Automatic Log-Off (Addressable)		
Encryption and Decryption (Addressable)		
Audit Controls (Required)		
Integrity Controls (Required)		
Mechanism to Authenticate ePHI (Addressable)		
Person or Entity Authentication (Required)		
Transmission Security (Required)		
Integrity Controls (Addressable)		
Encryption (Addressable)		
Other		

(Notations:____

____

____)

Step 11: Security Incident Response and Reporting.

A security incident is defined as "attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system." To protect against such incidents, practices must use the most up-to-date anti-virus programs, firewalls, and intrusion alert programs (which notify a workstation user in real time if a hacker is attempting to enter the system), train staff members to recognize the alerts such programs provide in the event of virus infection or hacking attempt, and require staff members to notify the practice Security Officer immediately should such an incident occur. Staff should be able to reach the practice Security Office or a designee quickly. Practice policy might also require the practice Security Officer to be well-versed in the procedures required by such programs to clear viruses from a system or how to implement further protective measures should a system be successfully entered by a hacker.

Adopt Security Incident Response and Reporting Procedures using model Document 11, if desired, on the following page as an example, and adapting or replacing Policy 26-A in the HIPAA Privacy Compliance Manual. Mitigation of Known Harm from an Improper Disclosure of Protected Health Information, Document 11-2, may be adapted to include both privacy and security incidents. Report of Privacy or Security Incident form, Document 11-2, can be used to document the report and response in the case of privacy or security incidents. Policies should reflect state law, the requirements of the practice, or other pertinent factors.

(Document 11)

PRIVACY AND SECURITY INCIDENT RESPONSE AND REPORTING POLICY

"Privacy or Security incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. Incidents may include, but are not limited to:

- Accidental user error.
- Improper use of access privileges.
- Employee access for the purpose of damaging or stealing information.
- Physical breach.
- External breach to illegally access information.
- Technical breach impacting operations or compromising systems or information.

It is the policy of the practice to:

- Require each workforce member to report a privacy or security incident to the Privacy and/or Security Officer immediately upon discovery of the incident or the suspicion of such an incident. The purpose of the reporting of an incident is to allow for mitigating any damage that may have occurred (see Document 11-1) and repairing or correcting the cause of the incident to assure the incident does not recur. Examples of incidents that shall be reported are:
    - Attempts to gain unauthorized access to files, systems or data.
    - Unwanted disruption or denial of service.
    - Unauthorized use or access of a system for transmission, processing, or storage, exploitation tool placement, or degradation of data.
    - Changes to system hardware, firmware, and/or usage of software characteristics without the knowledge, instruction, or consent of the Privacy or Security Officer.
    - Discovery of malicious code which includes, but is not limited to, worms, viruses, Trojans, web defacement, etc.
    - Any breach of the computing environment that has the potential to spread outside of the practice's immediate control.

If the incident was accidental or the result of workforce negligence, the Privacy and/or Security Officer may determine that re-education on privacy and security procedures is necessary for the Workforce. If the incident was caused by a computer/information system "breakdown" and cannot be corrected by the practice technical expert, outside technical expertise will be sought. The practice will continually upgrade the system privacy and security software upon recommendation of the system manufacturer/provider.

- Document all privacy or security incidents. Whenever an incident occurs, the Privacy and/or Security Officer shall be responsible for the completion of a Report of Privacy or Security Incident form (see Document 11-2) or other applicable documentation. The form shall be kept by the practice for at least six (6) years or until all questions and/or legal actions are completed, whichever is later.
- Sanction workforce members for failure to comply or ensure compliance with the reporting of privacy or security incident requirements which may result in disciplinary action up to and including dismissal (see Sanction Policy).
- Require at regularly scheduled intervals of not less than once per year the Privacy and/or Security Officer to review the incident reports associated with compliance with the HIPAA's Privacy and Security Rules to determine the existence of incident patterns, outliers, or unusual behavior related to access and security and take corrective actions if necessary.
- Require, in the event a Business Associate reports a security incident, the Business Associate to complete an incident report including its actions to remedy the problem. Failure to report and/or remedy the problem may give rise to a breach of the Business Associate Agreement.
- Other ____

(Notations: ____

____

____)

Policy adopted __________________
(Date)

(Document 11-1)

MITIGATION OF KNOWN HARM FROM AN IMPROPER DISCLOSURE OF PROTECTED HEALTH INFORMATION

In order to comply with HIPAA's Privacy and Security Rules, it is the policy of this office to mitigate known harm from an improper disclosure of Protected Health Information (PHI/ePHI), when it is practicable to do so.

Whenever we learn of harm caused by an improper disclosure of our protected health information, including electronic Protected Health Information (ePHI), we will take reasonable steps to mitigate the harm. We will take these steps whether the improper disclosure was made by us or by one of our Business Associates.

Our Privacy Officer, Security Officer, and/or Public Information Officer will determine what specific steps are appropriate to mitigate particular harm. It is our policy to tailor mitigation efforts to individual harm. Examples of some mitigation steps include:

Getting back Protected Health Information that was improperly disclosed.

Preventing further disclosure through agreements with the recipient.

We do not consider money reparations to be appropriate mitigation.

If a Business Associate has made the improper disclosure, we will require the Business Associate to cure the problem to our satisfaction or terminate the relationship with the Business Associate.

Policy adopted ___________________
(Date)

(Document 11-2)

Report of Privacy/Security Incident

I. Instructions: *This form shall be used to report any acts or omissions that result in (1) the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or (2) interference with system operations in an information system.*	
II. Type of Incident:	**III. Date & Time of Incident:**
IV. Procedure or System Compromised/Damage Caused:	
V. Employee(s) Involved:	
VI. Initial Action Taken:	**VII. Remedy Implemented:**
VIII. Remedy Date:	
IX. Date Reported to Privacy/Security Officer:	
X. Person Reporting: ______________________ **Work Location:** (If more than one office) ______________________ ______________________________________ Signature	
(For use by Privacy/Security Officer) **XI. Follow-up Action:**	

Step 12: Sanction Policy.

Document 12 provides a model sanction policy. In addition, practices may wish to consider the following in a sanction policy:

1. Identify all persons to which the policy applies, including employees (including the doctors), trainees (particularly if your practice serves as an externship or residence site for one of the optometry schools), contractors, volunteers, or others that may come in contact with PHI/ePHI.

   List examples of varying severity such as leaving the workstation where others, including patients, can view the screen, knowingly using someone else's password, not logging off when going to lunch, leaving patient files open and in view of unauthorized persons, or providing PHI/ePHI to persons without checking their authority to receive such information.

   Based on the severity of the violation, develop varying levels of disciplinary action, such as verbal warning, written warning, retraining/re-education, removal of system privileges, suspension or suspension without pay, termination of employment, or, in the case of a Business Associate, contract penalties.

   Include notice that civil or criminal penalties may arise for misuse or misappropriation of PHI/ePHI.

   Workforce should be aware that violations may result in notification to law enforcement or regulatory officials, including licensing organizations.

The following are examples of additional specific provisions that a practice may wish to include. Each practice should evaluate its systems and procedures to determine the likelihood of violations of the Privacy/Security Regulations and develop disciplinary procedures accordingly. At any stage of disciplinary action, re-education or retraining sessions in the policies and procedures for maintaining privacy and security of PHI/ePHI may be recommended.

Examples of actions or omissions that may lead to sanctions include, but are not limited to:

- Violations considered so serious that such a violation will result in IMMEDIATE DISCHARGE:
  - Intentional misuse, destruction, or damage to systems, programs, or files containing patient PHI/ePHI.
  - Unauthorized removal, alteration, or destruction of patient PHI/ePHI.
  - Intentional release of patient PHI/ePHI to unauthorized persons or entities.
  - A pattern of failing to follow verification procedures prior to releasing PHI/ePHI to outside persons or entities requesting same.
- Less serious violations that warrant lesser sanctions might include:
  - Accessing PHI/ePHI computer files without appropriate authorization.
  - Failure to timely notify Privacy/Security Officer of a known or suspected privacy or security breach.

Minor violations that warrant various types of warnings and/or retraining might include:

- Any negligence or carelessness in handling PHI/ePHI.
- Use of office computer for personal e-mail or Internet access which may expose the system to viruses or access by outside entities.

Adopt Sanctions for Violating Privacy and Security Policies and Procedures using model Document 12, if desired, on the following page, as an example, adapting the policy to reflect state law, the requirements of the practice, or other pertinent factors.

(document 12)

SANCTIONS FOR VIOLATING PRIVACY AND SECURITY POLICIES AND PROCEDURES

Members of the workforce are subject to disciplinary action for violation of policies and procedures. Violations that jeopardize the privacy or security of PHI/ePHI are particularly serious. This seriousness will be reflected in the nature of the disciplinary action, up to and including termination of employment.

1. All members of the workforce will be treated fairly and equitably in the imposition of sanctions for privacy and security violations.
2. Sanctions will be integrated into the Practice's overall employee discipline policy. This policy will be in writing.
3. Disciplinary actions due to breaches of privacy or security of PHI/ePHI will be documented, and the documentation must be retained for 7 (seven) years.
4. Disclosure of PHI/ePHI in violation of policy is reportable under the Accounting of Disclosures of Protected Health Information Policy.
5. No member of the workforce will be subject to sanctions for a disclosure of PHI/ePHI made in good faith in accordance with the following policies:
    - Disclosure of protected health information by "whistleblowers".
    - Disclosures of protected health information by workforce members who are the victims of a crime.
6. Disciplinable actions include but are not limited to:
    - Intentional misuse, destruction, or damage to systems, programs, or files containing patient PHI/ePHI.
    - Unauthorized removal, alteration, or destruction of patient PHI/ePHI.
    - Intentional release of patient PHI/ePHI to unauthorized persons or entities.
    - A pattern of failing to follow verification procedures prior to releasing PHI/ePHI to outside persons or entities requesting same.
    - Accessing PHI/ePHI computer files without appropriate authorization.
    - Failure to timely notify Privacy/Security Officer of a known or suspected privacy or security breach.
    - Any negligence or carelessness in handling PHI/ePHI.
    - Use of office computer for personal e-mail or Internet access which may expose the system to viruses or access by outside entities.
7. Other ____

(Notations:____

____)

Policy adopted ________________
(Date)

Step 13: Evaluation.

All documented policies and procedures required under the HIPAA Privacy or Security Regulation must be periodically reviewed and updated, as necessary, in response to any environmental, organizational, or operational changes. At least once a year, or when a major change occurs (new computer, new operating system, new software program, Internet or e-mail use is initiated, change in staffing level, reconfiguration of the office, etc.), small practices should evaluate how they are doing, if the level of risk faced by the practice is still at an acceptable level, and if it is not acceptable, determine what changes need to be made to reduce the risk to an acceptable level. The practice must be sure to review all components – administrative, physical, and technical – of the safeguards.

Each practice should periodically review its Contingency Plan to ensure that it is up-to-date. In addition, each practice should test its contingency plan periodically to ensure that it actually works. Focus on the ability to actually access the alternative computer and site in a timely fashion, load and run any necessary programs, and load, view, and use confidential data. Staff should take part in these tests.

Practices should also review:

- Privacy/Security Incident Reports (Document 11-2) to determine if adequate measures have been taken to prevent similar security breaches in the future in compliance with HIPAA's Security and Privacy Standards.
- Staff job changes, at least annually, to ensure access authorized to each workforce member remains appropriate to their job responsibilities in line with Implementation Specification 4c: Access Establishment/Modification (See cross reference Step 4).
- Ensure that user IDs and passwords for any workforce members who have terminated employment with the practice have been removed from the system by attempting to enter the system with those passwords and IDs and remove them if they are still recognized by the system in line with Implementation Specification 3c: Terminations Procedures (See cross reference Step 4).

Adopt Evaluation Policy using, if applicable, model Document 13 on the following page, as an example, adapting the policy to reflect state law, the requirements of the practice, or other pertinent factors. Attach appropriate documentation as necessary to demonstrate compliance with the policy, using, if applicable, Security Evaluation Log, Document 13-1.

(Document 13)

EVALUATION POLICY

It is the policy of the practice to periodically:

- Perform a technical and non-technical evaluation based, initially, on the standards implemented under the HIPAA Security rule and, subsequently, in response to environmental or operational changes that affect the security of electronic protected health information.
- Review and update documentation periodically, as needed, or in response to environmental or operational changes.
- Test and, if warranted, revise the practice Contingency Plan (Document 3).
- Review Privacy/Security Incident Reports (Document 11-2) to determine if adequate measurers have been taken to prevent similar security breaches in the future.
- Review staff job changes at least annually to ensure access authorized to each workforce member remains appropriate to their job responsibilities.
- Ensure that user IDs and passwords for any workforce members who have terminated employment with the practice have been removed from the system by attempting to enter the system with those passwords and IDs and remove them if they are still recognized by the system.
- Other: ____

(Notations: ____

____)

Policy adopted _________________
(Date)

(Document 13-1)

<table>
<tr><th colspan="2">SECURITY EVALUATION LOG</th></tr>
<tr><td colspan="2">Technical and non-technical evaluation of the security of electronic Protected Health Information in the practice based on the HIPAA’s Security standards conducted periodically or in response to environmental or operational changes that affect.</td></tr>
<tr><td>Results:</td><td></td></tr>
<tr><td colspan="2">Review and update documentation periodically, as needed, or in response to environmental or operational changes affecting the security of the practice.</td></tr>
<tr><td>Results/documentation updated:</td><td></td></tr>
<tr><td colspan="2">Test and, if warranted, revise the practice Contingency Plan (Document 3), as appropriate.</td></tr>
<tr><td>Results/Contingency Plan Revisions:</td><td></td></tr>
<tr><td colspan="2">Review Privacy/Security Incident Reports to determine if adequate measures have been taken to prevent similar security breaches in the future.</td></tr>
<tr><td>Results:</td><td></td></tr>
<tr><td colspan="2">Review staff job changes to ensure access authorized to each workforce member remains appropriate to their job responsibilities.</td></tr>
<tr><td>Results/Access Modifications:</td><td></td></tr>
<tr><td colspan="2">User IDs and passwords for any workforce members who have terminated employment with the practice are checked to ensure such passwords and IDs have been removed from the system by attempting to enter the system with those passwords and IDs and remove them if they are still recognized by the system.</td></tr>
<tr><td>Results:</td><td></td></tr>
<tr><td colspan="2">Periodically assess the overall physical security needs of the practice, including facility location, layout, design, and construction and periodically assess any need for and reasonableness of stronger or different entry door locks, alarm systems, and anti-intrusion devices as required under Standard 10: Facility Access Controls.</td></tr>
<tr><td>Results:</td><td></td></tr>
<tr><td>Other:</td><td></td></tr>
<tr><td>Results:</td><td></td></tr>
</table>

(Notations: ____

____

____)

Evaluation completed: ________________________
(Date)

Step 14: Isolate Healthcare Clearinghouse Function.

Clearinghouses include billing services, re-pricing companies, community health management information systems, and value-added networks and switches that convert financial and administrative transactions from non-standard format to standard format or standard format to non-standard format. In most small health care practices, compliance with this required specification will simply mean completing a form stating that the practice does not operate a health care clearinghouse. Practitioners who believe a clearinghouse function may be included in their practice operations should consult an attorney for additional guidance.

Adopt Statement Regarding Health Care Clearinghouse Function using model Document 14, if desired, on the following page, as an example. Policies should reflect state law, the requirements of the practice, or other pertinent factors.

(Document 14)

STATEMENT REGARDING HEALTHCARE CLEARINGHOUSE FUNCTION

The optometric practice of does not operate an information clearing house and therefore meets the HIPAA's Security Regulation requirement for "Isolating Health Care Clearinghouse Function" by either not using the services of a health care clearinghouse or isolates such services by relating them solely to an outside clearinghouse.

Policy adopted __________________
(Date)

REQUIREMENTS FOR GROUP HEALTH PLANS

The HIPAA's Security Regulation includes standards and specifications pertaining specifically to relationships with group health plan sponsors ensuring the protection of ePHI created, received, maintained, or transmitted by the sponsor. Most optometric practices probably will not be subject to these requirements. However, a practice that in any way offers its own eye or vision care plan might. Such practices will be covered by several additional standards and implementation specifications:

- Administratively protect ePHI.
    - Group health plan sponsors will reasonably and appropriately safeguard ePHI created, received, maintained, or transmitted to or by the plan sponsor on the practice's behalf.
    - Plan documents must require the plan sponsor to implement administrative, physical, and technical safeguards that will reasonably and appropriately safeguard ePHI that it creates, receives, maintains, or transmits on the practice's behalf.
- Ensure Adequate Separation.
    - Plan documents must describe those employees or classes of employees or other persons under the control of the plan sponsor to be given access to the PHI/ePHI to be disclosed.
    - Plan documents must describe any employee or person under the control of the plan sponsor who receives PHI relating to payment under health care operations of or other matters pertaining to the group health plan in the ordinary course of business.
    - Plan documents must restrict the access to and use of PHI by those employees or persons under the control of the plan sponsor to only the plan administrative functions that the plan sponsor performs for the group health plan.
    - Plan documents must provide an effective mechanism for resolving any issues of non-compliance by employees or persons under the control of the plan sponsor with any of the provisions of your plan documents.
- Ensure Agents Protect ePHI.
    - Plan documents must require the plan sponsor to ensure that any agent, including a subcontractor, to whom it provides ePHI, agrees to implement reasonable and appropriate security measures to protect the information.
- Report Incidents to Group Health Plans.
    - Plan documents must require the plan sponsor to report to the group health plan any security incident of which it becomes aware.

Practitioners who believe they may fall under the HIPAA's Security Regulation group health plan requirements should consult their attorney for advice on properly formulating required policies and procedures.

ADDITIONAL RESOURCES

An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule (NIST Special Publication 800-66), (Draft) National Institute of Standards and Technology. Downloadable free of charge at http://csrc.nist.gov/publications/nistpubs/.

Small Practice Security Implementation White Paper, Workgroup for Electronic Data Interchange Strategic National Implementation Process (WEDI-SNIP); free of charge, Workgroup for Electronic Data Interchange, 12020 Sunrise Valley Dr., Suite 100, Reston, VA 2019, telephone (703) 391-2716; fax 703-391-2759. Downloadable from www.wedi.org/snip.

Risk Analysis White Paper, Workgroup for Electronic Data Interchange Strategic National Implementation Process (WEDI-SNIP); free of charge, (see above).

Security Policies and Procedures (P&P) White Paper, Workgroup for Electronic Data Interchange Strategic National Implementation Process (WEDI-SNIP); free of charge, (see above).

HIPAA Security Analysis Manual Susan A. Miller, J.D., Telephone (978) 369-2092, fax: (978) 369-6296, Web site: *www.HealthTransactions.com*.

Security Roadmap Sample Implementation Guide, Southern Healthcare Administrative Regional Process (SHARP). www.sharpworkgroup.com.

Handbook for HIPAA Security Implementation, American Medical Association, ($149) available from AMA Press (www.ama-assn.org) or *Tom Walsh Consulting*
(www.tomwalshconsulting.com).

Common Sense Guide to Cyber Security for Small Business, prepared by the National Cyber Security Alliance, 1150 18th St. NW Suite 1010, Washington DC 20036-3824.
Phone (202) 331-5350, *Fax (202) 872-4318*.

Security Risk Analysis and Management: An Overview (Updated), Tom Walsh, CISSP, American Health Information Management Association, available at: http://library.ahima.org/.

Disaster Planning for Health Information (Updated), Patricia Cunningham, MS, RHIA, American Health Information Management Association, available at: http://library.ahima.org/.

A HIPAA Security Overview (Updated), William Miaoulis, CISA, CISM, American Health Information Management Association, available at: http://library.ahima.org/.

Securing Wireless Technology for Healthcare (AHIMA Practice Brief), John Retterer and Brian W. Casto, BSEE, CET, American Health Information Management Association, available at: http://library.ahima.org/.

Mobile Device Security, NIST HIPAA Conference, May 19, 2009, available free of charge at: http://csrc.nist.gov/news_events/HIPAA-May2009_workshop/presentations/7-051909-new-technologies-mobile-devices.pdf.

Healthcare Breach Management: Business Associate Agreement Addendum, Beth Hjort, RHIA, CHPS and Harry Rhodes, MBA, RHIA, CHPS, CPHIMS, FAHIMA, January 22, 2010, available free of charge at: http://www.ahima.org/downloads/pdfs/advocacy/HealthcareBreachmanagement_BAAAddendum.pdf.

Keeping an Eye on Business Associates, Health Data Management, available free of charge at: http://www.healthdatamanagement.com/issues/19_11/hipaa-privacy-security-business-associates-43504-1.html?zkPrintable=1&nopagination=1.

ACKNOWLEDGEMENTS

The AOA Office of Counsel and AOA Communication Group wish to gratefully acknowledge the assistance and contributions of:

The Workgroup for Electronic Data Interchange (WEDI) Strategic National Implementation Process (SNIP), 12020 Sunrise Valley Dr., Suite 100 Reston, VA. 20191, telephone: 703-391-2714, fax: 703-391-2759, Web site: *www.wedi.org/snip*.

The North Carolina Healthcare Information and Communications Alliance (NCHICA) offering 3200 Chapel Hill/Nelson Blvd, Cape Fear Building, Suite 200, PO Box 13048, Research Triangle Park, NC 27709, telephone: 919-558-9258, fax: 919-558-2198 Web site: *www.nchica.org*.

Susan A. Miller, J.D., Workgroup for Electronic Data Interchange (WEDI) Strategic National Implementation Process (SNIP)co-chair, WEDI SNIP Executive Committee Member, WEDI SNIP Steering Committee member, WEDI SNIP Security and Privacy Work Group Co-chair, New England HIPAA Workgroup (NEHW) Steering Committee, SHARP Advisory Committee member and Security Workgroup co-chair, for expert review. Telephone (978) 369-2092, fax: (978) 369-6296, Web site: *www.HealthTransactions.com*.

Tom Walsh, CHS, CISSP, Tom Walsh Consulting, LLC, 6108 W 121st Street, Overland Park, KS 66209, office telephone: 913-696-1573, cell phone: 913-669-5314 e-mail: *twalshconsulting@aol.com*, Web site: *www.tomwalshconsulting.com*

Toni G. Sutter, MSW, LCSW(P), Office Manager Robert J. Sutter, O.D., 3215 S. Providence Road, Ste. C, Columbia, MO 65203, telephone for expert editing, formatting and review of this manual.

Curtis E. Turner, Jr., MBA, NREMT, CPOT, COA, OA, chair elect, American Optometric Association, Paraoptometric Section Council, 2890-A GA Hwy 212, Box 224 Conyers, Georgia 30094, for review of this manual

Jeffrey A. Kempf, O.D., of Becherer, Becherer & Associates Limited, Belleville, Illinois for initial manuscript review.

HIPAA Security Regulation

For further information, please see the HIPAA Security Rule which may be accessed through the following links:

45 C.F.R. Part 160: http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&SID=b7d02f5e5bbe2a74630fa1f4518bebaf&rgn=div5&view=text&node=45:1.0.1.3.75&idno=45

45 C.F.R. Part 164, Subpart A: http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&rgn=div6&view=text&node=45:1.0.1.3.78.1&idno=45

45 C.F.R. Part 164, Subpart C: http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&SID=ec2c5f3a0314ad3bf6a65c9252665d54&rgn=div6&view=text&node=45:1.0.1.3.78.3&idno=45