**Columbus Eye Associates & Columbus Optical**

# Health Insurance Portability and Accountability Act (HIPAA) Security Policies and Procedures

February 1, 2003



## Revision History

| Date | Revised by | Summary of Changes |
|---|---|---|
| 02-01-03 | Columbus Eye Associates & Columbus Optical Compliance Officer | Initial document creation: Draft 1 |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

## Outstanding Items

<List any outstanding items here.>

# Table of Contents

# 1 Introduction

## 1.1 Document Description

This document describes Columbus Eye Associates & Columbus Optical's policies and procedures relative to the Security part of the Health Insurance Portability and Accounting Act (HIPAA) of 1996. By having this document in place, and exercising the steps required to implement required activities, Columbus Eye Associates & Columbus Optical declares that it has made its best efforts to be compliant with the Security part of HIPPA, as it applies to Columbus Eye Associates & Columbus Optical.

## 1.2 Purpose

The purpose of this document is to list the policies and procedures Columbus Eye Associates & Columbus Optical has documented and follows to remain compliant with the Security part of HIPAA. This document is used as a set of statements and instructions for Columbus Eye Associates & Columbus Optical's workforce to follow, and as a training guide.

## 1.3 Ownership and Revisions

The Columbus Eye Associates & Columbus Optical HIPAA Compliance officer, who is responsible for revisions and updates, owns this document. This is a "living" document. Updates that are a result of new discoveries, such as changing regulations or processes, will be added as needed by the document owner listed on the Revision History page.

## 1.4 Conventions

This document uses the following conventions:

- References to other documents or to sections within a document are underlined.
- Tables appear in Arial font.
- In addition to variable values, italic type indicates emphasis or a new term.

# 2 Administrative Safeguards

Columbus Eye Associates & Columbus Optical has implemented administrative policies and procedures to prevent, detect, contain, and correct security violations. These policies and procedures are described in the following sections.

## 2.1 Risk Analysis and Management

Columbus Eye Associates & Columbus Optical conducts accurate and thorough assessments of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held in its computer systems, on a regular basis. When Columbus Eye Associates & Columbus Optical's Compliance Officer believes any risks exist, the Compliance Officer addresses each risk and completes a risk mitigation report.

Columbus Eye Associates & Columbus Optical has implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the HIPAA Security Rule. These measures are described in detail in Sections 3 and 4 of this document.

## 2.2 Sanction Policy

Columbus Eye Associates & Columbus Optical will apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures, as detailed in Columbus Eye Associates & Columbus Optical's Code of Conduct, which is available for review in Columbus Eye Associates & Columbus Optical's HIPAA Compliance Manual.

## 2.3 Information System Activity Review, Login Monitoring

Columbus Eye Associates & Columbus Optical has implemented the following procedure to regularly review records of information system activity:

1. The Compliance Officer reviews files contained on Columbus Eye Associates & Columbus Optical's computers weekly.
2. Since Columbus Eye Associates & Columbus Optical's computers are basic and do not have the capability of maintaining automated tracking logs, the Compliance Officer regularly monitors usage of Columbus Eye Associates & Columbus Optical's computers by regularly observing employee access and conduct for inappropriate access.

## 2.4 Assigned Security Responsibility

Columbus Eye Associates & Columbus Optical has named its Compliance Officer as the security official who is responsible for the development and implementation of the policies and procedures required by this HIPAA Rule.

## 2.5 Workforce Security, Authorization, Supervision, Clearance Procedure

Columbus Eye Associates & Columbus Optical's policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, to prevent those workforce members who do not have access from obtaining access to electronic protected health information, to authorize and/or supervise workforce members who work with electronic protected health information or in locations where it might be accessed, and to determine that the access of a workforce member to electronic protected health information is appropriate, are listed below:

1. All employees who are allowed access to PHI are assigned passwords by the Compliance Officer to Columbus Eye Associates & Columbus Optical's computers. Passwords are kept locked up and managed by the Compliance Officer during office hours.
2. Employees who do not have access cannot obtain access, as they do not have the passwords
3. Employees with access to PHI are trained in the importance of protecting electronic PHI.
4. The Compliance Officer determines what workforce members appropriately have access to PHI, based upon thorough review and understanding of Columbus Eye Associates & Columbus Optical's PHI Policies and Procedures, which are contained in Columbus Eye Associates & Columbus Optical's HIPAA Compliance Manual.

## 2.6 Termination Procedures

When the employment of a workforce member ends, or should no longer have access to PHI as determined by the Compliance Officer, that workforce member's access to electronic PHI is terminated by removing his or her user ID from Columbus Eye Associates & Columbus Optical's computers.

## 2.7 Security Awareness, Training and Reminders

Columbus Eye Associates & Columbus Optical has security awareness and training program for all members of its workforce (including management). When implementing its HIPAA Compliance Manual, Columbus Eye Associates & Columbus Optical performed training sessions from its HIPAA Security Compliance Policies and Procedures. During regular staff meetings, Columbus Eye Associates & Columbus Optical informs its staff of periodic security updates.

## 2.8 Protection from Malicious Software

Columbus Eye Associates & Columbus Optical's computers have anti-virus scanning software installed, and updates to this software are purchased and

installed when available. This ensures that Columbus Eye Associates & Columbus Optical reasonably guards against, detects and reports malicious software.

## 2.9 Security Incident Procedures, Response and Reporting

Columbus Eye Associates & Columbus Optical's Compliance Officer notes any security issues he/she is aware of in the practice's Compliance Officer Incident Log, contained in Columbus Eye Associates & Columbus Optical's HIPAA Compliance Manual, and addresses them on a case-by-case basis.

## 2.10 Contingency, Data Backup, Disaster Recovery, Emergency Mode Operations, Testing and Revisions

Columbus Eye Associates & Columbus Optical backs up its computer systems nightly to a Tape Drive. The Compliance Manager takes the Tape Drive to a safe, off-site location nightly. Should an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) damage Columbus Eye Associates & Columbus Optical's systems that contain electronic protected health information, the Compliance Officer (or designated representative) takes the backup copy of the patient data, along with the original Tape Drive of Columbus Eye Associates & Columbus Optical's software to a reputable computer service company, and restores the system to its last operational state. The Compliance Officer (or designated representative) operates Columbus Eye Associates & Columbus Optical's systems from that location until the disaster situation is remedied.

Columbus Eye Associates & Columbus Optical's Compliance Officer tests this procedure any time new software programs are installed on Columbus Eye Associates & Columbus Optical's computer, to ensure data can be backed up, restored and operational as soon as possible.

## 2.11 Evaluation

Columbus Eye Associates & Columbus Optical 's Compliance Officer performs a technical and non-technical evaluation of the procedures in this document quarterly, or any time there are significant environmental or operational changes affecting the security of electronic protected health information.

## 2.12 Business Associate Contracts and Other Arrangements.

Columbus Eye Associates & Columbus Optical has Business Associates Agreements in place with its business associates who create, receive, maintain, or transmit electronic protected health information on our behalf, which gives us satisfactory assurances that the business associate will appropriately safeguard the information. A template copy of this agreement can be found in Columbus Eye Associates & Columbus Optical's HIPAA Compliance Manual, and each

associate's agreement is on file with our Compliance Officer. We realize that this standard does not apply with respect to:

1. Transmission by a covered entity of electronic protected health information to a health care provider concerning the treatment of an individual;
2. Transmission of electronic protected health information by a group health plan or an HMO or health insurance issuer on behalf of a group health plan to a plan sponsor, to the extent that the relevant HIPAA requirements apply and are met; or
3. Transmission of electronic protected health information from or to other agencies providing the services when the covered entity is a health plan that is a government program providing public benefits, if the relevant HIPAA requirements are met.

# 3 Physical Safeguards

Columbus Eye Associates & Columbus Optical has implemented physical safeguard-related policies and procedures to prevent, detect, contain, and correct security violations. These policies and procedures are described in the following sections.

## 3.1 Facility Access Controls

Columbus Eye Associates & Columbus Optical has implemented the following policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed:

1. Columbus Eye Associates & Columbus Optical's computers are kept in private areas.
2. Only personnel requiring access to these systems are authorized to use them.

## 3.2 Contingency Operations

Columbus Eye Associates & Columbus Optical has established procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency. See Section 2.10, Contingency, Data Backup, Disaster Recovery, Emergency Mode Operations, Testing and Revisions, for details.

## 3.3 Facility Security Plan

Columbus Eye Associates & Columbus Optical has implemented policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. Computers are kept in secure, private locations and the building is secure from unauthorized access.

## 3.4 Access Control and Validation Procedures

Columbus Eye Associates & Columbus Optical has implemented 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. The Compliance Officer oversees access to facilities and computers.

## 3.5 Maintenance Records

Columbus Eye Associates & Columbus Optical has implemented policies and procedures to document repairs and modifications to the physical components of its facility, related to security. The Compliance Officer ensures, on a daily basis,

that the physical facility is in working order and documents any deficiencies for follow-up and repair.

## 3.6 Workstation Use

Columbus Eye Associates & Columbus Optical has implemented 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 its specific workstation or class of workstation that can access electronic protected health information. Columbus Eye Associates & Columbus Optical's computers are kept in private areas. Only personnel requiring access to these systems are authorized to use them.

## 3.7 Workstation Security

Columbus Eye Associates & Columbus Optical has implemented physical safeguards for all workstations that access electronic protected health information, and has restricted access to authorized users. Columbus Eye Associates & Columbus Optical's computers are kept in private areas. Only personnel requiring access to these systems are authorized to use them.

## 3.8 Device and Media Controls

Columbus Eye Associates & Columbus Optical has implemented policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility. The Compliance Officer oversees the movement, receipt and removal of all hardware and electronic media on an as-needed basis.

## 3.9 Disposal

Columbus Eye Associates & Columbus Optical has implemented policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored. The Compliance Officer oversees the final disposition of any hardware or electronic media, and erases disks and other media as needed upon disposal.

## 3.10 Media Re-Use

Columbus Eye Associates & Columbus Optical has implemented procedures for removal of electronic protected health information from electronic media before the media are made available for re-use. The Compliance Officer oversees the erasure of any electronic media prior to reuse, as applicable.

## 3.11 Accountability

The Compliance Officer maintains a record of the movements of hardware and electronic media and any person responsible therefore.

## 3.12 Data Backup and Storage

The Compliance Officer or designated authorized representative creates a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

# 4 Technical safeguards

Columbus Eye Associates & Columbus Optical has implemented technical safeguard-related policies and procedures in the following areas to prevent, detect, contain, and correct security violations, as described in the following sections.

## 4.1 Access Control

Columbus Eye Associates & Columbus Optical has implemented technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights. See Section 3.4, Access Control and Validation Procedures, for details.

## 4.2 Unique User Identification

Columbus Eye Associates & Columbus Optical assigns a unique name and/ or number for identifying and tracking user identities by setting up login IDs and passwords to each employee, as applicable.

## 4.3 Emergency Access Procedure

Columbus Eye Associates & Columbus Optical has established procedures for obtaining necessary electronic protected health information during an emergency. See Section 2.10, Contingency, Data Backup, Disaster Recovery, Emergency Mode Operations, Testing and Revisions, for more details.

## 4.4 Automatic Logoff

Columbus Eye Associates & Columbus Optical has implemented electronic procedures that terminate an electronic session after a predetermined time of inactivity, through use of a password-protected screen saver.

## 4.5 Encryption, Decryption and Security

Columbus Eye Associates & Columbus Optical has implemented a mechanism to encrypt and decrypt electronic protected health information whenever it is transmitting this information electronically. This mechanism utilizes a software program for encryption and authentication of transmitted data.

## 4.6 Audit Controls

Columbus Eye Associates & Columbus Optical has implemented procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. See Section 3.6, Workstation Use, for details.

## 4.7 Integrity

Columbus Eye Associates & Columbus Optical has implemented policies and procedures to protect electronic protected health information from improper alteration or destruction, to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner, and to verify that a person or entity seeking access to electronic protected health information is the one claimed. Section 3.6, Workstation Use, for details.

# 5 Organizational and Documentation Requirements

Columbus Eye Associates & Columbus Optical has implemented the organizational and documentation requirements mandated by the HIPAA Security Rule. These requirements, and Columbus Eye Associates & Columbus Optical's compliance declarations, are described in more detail in the following sections.

## 5.1 Business Associate Contracts

Columbus Eye Associates & Columbus Optical has ensured that its contracts with its Business Associates address all necessary safeguards required by the HIPAA Security Rule. Contracts between Columbus Eye Associates & Columbus Optical and its Business Associates provide that the business associate will:

1. Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of Columbus Eye Associates & Columbus Optical.
2. Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it.
3. Report to Columbus Eye Associates & Columbus Optical any security incident of which it becomes aware.

Business Associate contracts will also authorize termination of the contract by Columbus Eye Associates & Columbus Optical, if Columbus Eye Associates & Columbus Optical determines that the business associate has violated a material term of the contract

## 5.2 Documentation Form, Retention, Availability and Updates

Columbus Eye Associates & Columbus Optical maintains these policies and procedures implemented to comply with the HIPAA Security Rule in written and electronic form. Columbus Eye Associates & Columbus Optical retains the documentation required by HIPAA Security Rule for seven years from the date of its creation or the date when it last was in effect, whichever is later. Columbus Eye Associates & Columbus Optical makes documentation available to those persons responsible for implementing the procedures to which the documentation pertains. Columbus Eye Associates & Columbus Optical reviews documentation periodically, and updates it as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.

# 6 Reporting and Investigating Security Breaches

Questions about breach of privacy issues will be presented initially to the Compliance Officer or owner of Columbus Eye Associates & Columbus Optical.

Employees who report possible security issues in good faith will not be subjected to retaliation or harassment as a result of the report. Concerns about possible retaliation or harassment will be reported to the primary physician of the practice.

Whenever a security issue has been identified, through monitoring, reporting of possible issues, investigations, or otherwise, the Compliance Officer shall have the responsibility and authority to take or direct appropriate action to address that issue. The corrective action will be set forth in writing

Corrective actions will be designed to ensure that the specific issues are addressed and similar problems do not occur in the future.

Employees who have engaged in willful misconduct will be subject to disciplinary action, up to and including termination in appropriate cases, in accordance with company policies, procedures and codes of conduct.

The results of inquiries will be made available to the primary physician. All employees are directed cooperate fully with any inquiries undertaken pursuant to this plan. To the extent practical and appropriate, efforts will be made to maintain the confidentiality of such inquiries and the information gathered.

The Compliance Officer will maintain an incident log of security concerns that are reported, as described in this document. The log will record the issues, the individuals or departments affected, and the resolutions.

Columbus Eye Associates & Columbus Opticaland its employees are aware of the seriousness of security breaches and understand that appropriate action must be taken to prevent similar instances from occurring.