Compliance Program Manual

Policies and Procedures

Derek Hamilton, OD, PA dba Hamilton Eye Associates

15550 RR 620N

Austin, TX 78717

512-251-4040

Authored and Compiled by: Compliance Specialists, LLC

Licensed to: Derek Hamilton, OD, PA dba Hamilton Eye Associates License #: 1451

This manual was printed on 5/18/2021

This manual will be kept Posted to www.hamiltoneyeatx.com/compliance

Table of Contents

Statement of Purpose

This manual contains policies and procedures that support the work of Derek Hamilton, OD, PA dba Hamilton Eye Associates while ensuring leadership and staff know what is expected of them regarding compliance and HIPAA security. Our practice is committed to achieve the following goals:

- To provide the highest quality care;
- To protect our patient's privacy;
- To properly document the nature of professional care provided to our patients;
- To submit claims for reimbursement to federal health care programs and other third-party payers in a timely and compliant manner;
- To continually educate and keep all employees of the Practice informed as to changes and updates to federal and state rules, statutes and regulations;
- To strive to achieve zero mistake billing;
- To promptly correct any billing errors that may be discovered;
- To review and update our Compliance and HIPAA Programs on a regular basis.

This Compliance Program ("Program") will provide guidance to avoid improper referrals or other circumstances that may create an appearance of unauthorized conduct so that the Practice will remain in compliance with all government rules and regulations and contract terms with third party payers.

References used within this manual include, but are not limited to:

- The Physician Self-Referral Law (aka Stark Law): Statute: 42 U.S.C. § 1395nn
- The Federal Anti-Kickback Statute: Statute: 42 U.S.C. § 1320a-7b(b)
- The False Claims Act: Statute: 31 U.S.C. §§ 3729-3733
- The Health Insurance Portability and Accountability Act (HIPAA): Public Law 104-191
- Civil Monetary Penalties Law: 42 U.S.C. Section 1320a-7a
- Exclusion Statutes; Authorities: 42 U.S.C. Section 1320a-7; OIG
- Criminal Health Care Fraud Statute: Statute: 18 U.S.C. §§ 1347, 1349
- Theft or Embezzlement in Connection with Health Care: (18 U.S.C. 669)
- The Social Security Act: Section 1861

Additional information on each of these references can be found in Policy III in this manual. The Compliance Officer (see Policy I) or other designated personnel will update this manual based upon periodic releases and changes from government offices. In the event of any changes, the Compliance Officer or other designated personnel will ensure staff has been made aware of these changes. A copy of the prior manual (electronic or paper) will be kept for historical purposes.

The manual will be retained on-line with a paper manual made available upon request. Other copies will be distributed at the discretion of the practice.

If any employee or Derek Hamilton, OD, PA dba Hamilton Eye Associates leader has questions or concerns, they should immediately bring those items to the attention of the Derek Hamilton, OD, PA dba Hamilton Eye Associates Compliance Officer and/or other

designated personnel.

Organization and Affiliation

Derek Hamilton, OD, PA dba Hamilton Eye Associates is committed to adherence to all health care rules and regulations. If at any time a change in the practice's legal identity occurs, updates to the Provider Enrollment Chain and Organization System (PECOS) will be within the 30 day period as required by federal law. Our organizational structure is as follows:

IRS Form CP575 shows the company name as: Derek Hamilton, OD, PA

Derek Hamilton, OD, PA dba Hamilton Eye Associates tax reporting status is listed as

Derek Hamilton, OD, PA dba Hamilton Eye Associates has additional locations at: (n/a if none listed)

Derek Hamilton, OD, PA dba Hamilton Eye Associates ownership is as follows:

Derek Hamilton - NPI: 1578582037 - % Owned: 100

(Attach a copy of your organizational chart)

Policy I

Compliance Officer; Privacy Officer; Public Information Officer and Security Officer

The Compliance Officer will oversee the compliance program to ensure Derek Hamilton, OD, PA dba Hamilton Eye Associates is following the policies and procedures outlined in this manual. Duties include:

- Leads the compliance/HIPAA programs within Derek Hamilton, OD, PA dba Hamilton Eye Associates;
- Understands of HIPAA and Compliance requirements;
- Proactively works with the team to identify areas where improvement is needed;
- Able to review all facts before making judgment;
- Willing to work through identified and reported issues;
- Able to complete all necessary reporting, including state and federal reporting as required by law;
- Able to administer sanctions as needed;
- Act as and/or assist Privacy, Security and Public Information Officers as needed.

The Privacy Officer is responsible for Derek Hamilton, OD, PA dba Hamilton Eye Associates HIPAA Privacy Program. Duties include:

- Works collaboratively with the Compliance Officer and other team members to ensure the security of protected health information (PHI)
- Creates, implements, educates and monitors adherence to policies and procedures related to privacy and the protection of PHI
- Develops the education training plan for Derek Hamilton, OD, PA dba Hamilton Eye Associates and ensures training assignments are complete
- Proactively works with the team to identify areas where improvement is needed
- Able to review all facts before making judgment
- Willing to work through identified and reported issues
- Able to complete all necessary reporting, including state and federal reporting as required by law
- Able to administer sanctions as needed

The Public Information Officer will monitor complaints and/or requests for access to protected health information and determine if appropriate. Duties include:

- Maintains in-depth knowledge of the HIPAA privacy rules and Derek Hamilton, OD, PA dba Hamilton Eye Associates's privacy policies and procedures
- Ability to explain privacy policies and procedures to patients, staff and/or other parties as needed
- Knowledge of organizational structure as well as escalation process for all identified issues
- Proactively works with the team to identify areas where improvement is needed
- Able to review all facts before making judgment
- Willing to work through identified and reported issues
- Able to complete all necessary reporting, including state and federal reporting as required by law

- Able to administer sanctions as needed

The Security Officer is responsible for the ongoing management of information security policies, procedures and technical systems for Derek Hamilton, OD, PA dba Hamilton Eye Associates. Duties include:

- Works collaboratively with the Compliance and Privacy Officers as well as other team members to ensure the physical and technical security of protected health information
- Creates, implements, educates and monitors adherence to policies and procedures
- Work with staff/vendors/contractors responsible for physical and technical security
- Maintains forms and records as needed regarding technical and physical security, including but not limited to:
  - Maintenance Log;
  - User audit report;
  - Log in audit report.
- Proactively works with the team to identify areas where improvement is needed
- Creates, implements, educates and monitors adherence to policies and procedures related to physical and technical security
- Able to review all facts before making judgment
- Willing to work through identified and reported issues
- Able to complete all necessary reporting, including state and federal reporting as required by law
- Able to administer sanctions as needed
- Perform regularly scheduled Privacy and Security Risk Analysis

Assignment of Officer Roles:

Role	Assigned Staff Member(s) / Designated Individual(s)
Compliance Officer	Derek Hamilton, OD
Privacy Officer	Derek Hamilton, OD
Security Officer	Derek Hamilton, OD
Public Information Officer	Derek Hamilton, OD

Addendum to Policy I

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)

Policy II

Business Associates

Business Associates

Business Associates of Derek Hamilton, OD, PA dba Hamilton Eye Associates may include, but are not limited to:

- Billing service, Electronic Health Record, Practice Management System, Clearinghouse
- Service delivery
- Quality assurance
- Staff Training
- Legal
- Accounting
- Consulting, Information Technology Vendors
- Management

BAAs will be requested from all vendors/contractors of Derek Hamilton, OD, PA dba Hamilton Eye Associates when access to protected health information is part of the vendor/contractor role with the company. Note: Some Business Associate Agreements are part of the vendor contract and will be stored accordingly.

Derek Hamilton, OD, PA dba Hamilton Eye Associates will sign and keep on file all BAAs requested from Derek Hamilton, OD, PA dba Hamilton Eye Associates by our vendors.

Retention of Business Associate Agreements:

- Derek Hamilton, OD, PA dba Hamilton Eye Associates will maintain copies of all signed Business Associate Agreements (BAA) for the term of the contract.
- Copies of inactive BAAs will be kept on file for a minimum of six years. (Section 164.316(b)(2)(i))

Addendum to Policy II

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)

Policy III

Practice Standards, Procedures and

Adherence to Health Care Laws and Regulations

As outlined in the Statement of Purpose, the following regulations were used as a reference in the creation of this manual. These regulations, along with other applicable state and federal guidelines, affect the policies, procedures and business practices of Derek Hamilton, OD, PA dba Hamilton Eye Associates.

The Physician Self-Referral Law: 42 U.S.C. § 1395nn

Prohibits the referral of Medicare and Medicaid beneficiaries by a physician to an entity for the provision of "designated health services" if the physician, or the physician's immediate family member, has a financial relationship with the entity, unless a statutory exception applies to that financial relationship.

The Federal Anti-Kickback Statute: 42 U.S.C. § 1320a-7b (b)

Prohibits providers of services or goods covered by a federal healthcare program from knowingly and willingly soliciting or receiving or providing any remuneration, directly or indirectly, in cash or in kind, to induce either the referral of an individual, or furnishing or arranging for a good or service for which payment may be made by a Federal Healthcare Program

Imposes liability upon any person who knowingly submits or causes the submission of false or fraudulent claims for payment or approval. Under the False Claims Act's qui tam provisions, a person with evidence of fraud against the government (known as a "whistle-blower") is authorized to file a case in federal court and sue on behalf of the government.

Health Insurance Portability and Accountability Act (HIPAA) of 1996: Law 104-191

HIPAA or the Health Insurance Portability and Accountability Act was passed by Congress in 1996. HIPAA, in part, provides guidance on the following:

- Provides the ability to transfer and continue health insurance coverage for millions of American workers and their families when they change or lose their jobs;
- Reduces health care fraud and abuse;
- Mandates industry-wide standards for health care information on electronic billing and other processes; and
- Requires the protection and confidential handling of protected health information

Civil Monetary Penalties (CMP) Law: 42 U.S.C. Section 1320a-7a

May be imposed for a variety of conduct, and different amounts of penalties and assessments may be authorized based on the type of violation at issue. Penalties range from up to $10,000 to $50,000 per violation. CMPs can also include an assessment of up to 3 times the amount claimed for each item or service, or up to 3 times the amount of remuneration offered, paid, solicited, or received.

Exclusion Statute: 42 U.S.C. Section 1320a-7

OIG is required to impose exclusions from participation in all federal health care programs on health care providers and suppliers who have been convicted of:

- Medicare fraud, as well as any other offenses related to the delivery of items or services under
- Medicare;
- Patient abuse or neglect;
- Felony convictions for other health care-related fraud, theft, or other financial misconduct; or
- Felony convictions for unlawful manufacture, distribution, prescription, or dispensing of controlled substances.

Criminal Health Care Fraud Statute: 18 U.S.C. §§ 1347, 1349

Prohibits knowingly and willfully executing, or attempting to execute, a scheme:

- To defraud any health care benefit program; or
- To obtain (by means of false or fraudulent pretenses, representations, or promises) any of the money or property owned by, or under the custody or control of, any health care benefit program; in connection with the delivery of or payment for health care benefits, items, or services.

Proof of actual knowledge or specific intent to violate the law is not required.

Penalties for violating the Criminal Health Care Fraud Statute may include fines, imprisonment, or both.

Theft or Embezzlement in Connection with Health Care: (18 U.S.C. 669)

It is a crime to knowingly and willfully embezzle, steal or intentionally misapply any of the assets of a health care benefit program. Note that this law applies not only to federal health care programs, but to most other types of health care benefit programs as well.

The penalty may include the imposition of a fine, imprisonment of up to 10 years, or both. If the value of the asset is $100 or less, the penalty is a fine, imprisonment of up to a year, or both.

The Social Security Act: Section 1861

The Act was an attempt to limit what were seen as dangers in the modern American life, including old age, poverty, unemployment, and the burdens of widows and fatherless children.

Coding and Billing

It is the policy of Derek Hamilton, OD, PA dba Hamilton Eye Associates that its qualified health care professionals and all employees strive to provide the highest quality of care for its patients, while effectively managing the cost of that care. To achieve this goal, Derek Hamilton, OD, PA dba

Hamilton Eye Associates is committed to providing complete and thorough information to its patients and to appropriately document and bill for the services performed.

Derek Hamilton, OD, PA dba Hamilton Eye Associates recognizes the importance of accurately recording and billing for all services provided to our patients.

The Practice acknowledges that there are some services which may not be covered for payment from a third-party carrier and will make efforts to ensure patient understanding and obtain proper forms prior to performing the service.

Our policy is outlined as follows:

- Will have one fee schedule for all services rendered;
- Will accurately bill for items or services which were rendered by the Practice;
- Will only submit claims for equipment, medical supplies and services that are reasonable and are necessary for the patient;
- Will not charge more for identical services to third party payers than to patients;
- Will charge patients for routine services delivered, not covered by third party plans;
- Will avoid any double billing for services or items;
- Will not bill for non-covered services (except to obtain a denial allowing us to submit to secondary payers);
- Will only use appropriate provider identification numbers;
- Will use coding modifiers when appropriate;
- Will not unbundle services unless appropriate;
- Will use the appropriate code for the service performed;
- Will follow published guidance from Medicare, Medicaid, other applicable payers, CPT and/or ICD10 when available;
- Will prepare medical record documentation to support billing.

Hold Bills until Questions are Answered

In the event of any questions concerning coding, a bill will not be submitted until the question has been resolved.

Review of Rejected Claims

The Compliance Officer or other designated personnel will review claims that were rejected by the payer and determine an appropriate resolution. Education will be performed as indicated.

Reasonable and Necessary Services

The qualified health care professionals (QHCP) of Derek Hamilton, OD, PA dba Hamilton Eye Associates shall make independent professional judgments concerning the care and treatment of the patient based upon their independent professional judgment and standard of care guidelines. Providers will, where appropriate, order diagnostic tests that his/her judgment indicates is appropriate for patients whether third parties will pay for such services. Occasionally, there are services that may be appropriate, but which are not covered for reimbursement through Medicare or the patient's medical coverage plan (see also Advanced Beneficiary Notice). If the patient has a secondary payer, a physician may bill Medicare for the service to obtain a denial of coverage so that the group may seek reimbursement from the secondary payer.

Advanced Beneficiary Notices and Other Notices of Potential Non-Payment

The Practice will obtain an Advanced Beneficiary Notice for diagnostic testing not meeting published medical necessity criteria (National and Local Coverage Decisions). Each ABN must:

- Be reviewed with the patient prior to the test being performed
- Identify the service(s) that may be denied (by procedure name and code)
- Include the estimated charge the patient will be responsible for;
- State the reason why the physician believes that service coverage may be denied; and
- Require the patient's acknowledgement and signature.

Blank ABN forms should never be presented to a patient for signature. Derek Hamilton, OD, PA dba Hamilton Eye Associates will use the current ABN form available at cms.hhs.gov.

Derek Hamilton, OD, PA dba Hamilton Eye Associates recognizes that the ABN form is for Medicare Part B patients seen in their clinic. Other payers, including Medicare Advantage Plans may require different notices be provided.

Demographic Information

The Practice will make every effort to collect demographic information from the patient. This includes but is not limited to:

- Name
- Date of Birth
- Current Address
- Phone Number
- Insurance Carrier
- Emergency Contact Information

Derek Hamilton, OD, PA dba Hamilton Eye Associates also attempts to collect N/A for all patients of the clinic.

All copies made for identification or payment purposes will be kept be secure with the Practice.

Documentation

Derek Hamilton, OD, PA dba Hamilton Eye Associates is responsible for timely and accurate documentation for all services provided and/or ordered, including assessment/diagnosis and instructions to patients.

Practice will follow acceptable published documentation guidelines, which may include but is not limited to:

- 1995 or 1997 Evaluation and Management Guidelines
- CPT
- Standard of Care

Documentation will:

- Be comprehensive, complete and timely.

- State the chief compliant as outlined by the patient
- Specify relevant history, the examination, the clinical impression or diagnosis, the instructions to the patient or the plan of care, the date of the visit/test or procedure, and the identity of the physician conducting the evaluation
- Where appropriate, health risk factors should be identified.
- On subsequent visits, the patient's progress, their response to treatment, any changes in the diagnosis or treatment plan should be documented.
- The appropriate CPT and ICD10 codes, supported in the documentation, will be assigned and billed

Modifiers

When indicated by the service(s) performed, the Practice will add the appropriate modifier to the charge. A listing of valid modifiers can be found:

- CPT book
- HCPCS book
- CMS Medicare Carrier Websites

Diagnostic Testing Ordered by an Outside Provider

If a patient is referred by another QHCP for diagnostic testing only, the Practice will make no changes to that order until a new order from the treating physician/practitioner has been received. Similarly, if the result of an ordered diagnostic test is normal and the interpreting physician believes that another diagnostic test should be performed an order from the treating physician must be received prior to performing the unordered diagnostic test.

Improper Inducements, Kickbacks, Referrals

It is the policy of the Practice that its QHCPs shall make informed professional judgments in the best interests of the patient.

Derek Hamilton, OD, PA dba Hamilton Eye Associates will not offer, pay, solicit, or receive any remuneration directly or indirectly to induce or reward referrals of items or services reimbursable by a Federal health care program. When a provider offers, pays, solicits, or receives unlawful remuneration, the provider violates the Anti-Kickback Statute. Remuneration includes anything of value, such as cash, free rent, expensive hotel stays and meals, and excessive compensation for medical directorships or consultancies.

If the Practice and/or QHCP has any contractual relations with third parties regarding referrals all such contracts or arrangements will be reviewed by legal counsel for the Practice to verify the arrangements are in compliance with the current law.

Derek Hamilton, OD, PA dba Hamilton Eye Associates will restrict providers from referring patients for certain designated health services payable by Medicare or Medicaid to an entity where the physician (or an immediate family member) has an ownership/investment interest or a compensation arrangement, unless an exception applies

Professional Courtesy and Deductible Waivers and Routine Waivers of Co-payments and Deductibles

The practice will not routinely provide free services or waive patient balances. Collection procedures will be followed to identify cases in which outstanding patient balances will cause financial hardship for the patient and/or family. When identified as a financial hardship case, the Practice will make final judgement on what, if anything to collect. Documentation will be kept supporting this decision.

Under no circumstances, will the practice or any of the QHCPs decide during the exam process, whether a visit is a no-charge visit nor waive any financial responsibility of the patient/beneficiary.

Reasonable collection efforts will be made for all outstanding patient balances. Careful review and consideration will occur to ensure reasonable efforts have been made prior to adjustment any patient balance. Documentation to support reasonable collection efforts will be maintained.

Gifts and Business Courtesies

Gifts to Patients: Derek Hamilton, OD, PA dba Hamilton Eye Associates will not provide gifts to patients exceeding $10.00 per item or $50.00 annually.

Gifts to Providers: Compensation from an entity in the form of items or services (not including cash or cash equivalents such as gift cards) that does not exceed an aggregate of $407 per year (2018), if all the following conditions are satisfied. The total aggregate amount is published each calendar year.

- The compensation is not determined in any manner that considers the volume or value of referrals or other business generated by the referring physician.
- The compensation may not be solicited by the physician or the physician’s practice (including employees and staff members).
- The compensation arrangement does not violate the Anti-Kickback Statute or any federal or state law or regulation governing billing or claims submission

Of Note: Many drug and biologic companies provide physicians with free samples they may give to patients free of charge. It is legal to give these samples to your patients for free, but it is illegal to sell them. The Federal Government prosecutes physicians for billing Medicare for free samples. If you choose to accept samples, you need reliable systems in place to safely store the samples and ensure samples remain separate from your commercial stock.

Certification of Medical Equipment, Supplies and Home Health Services

It is the policy of Derek Hamilton, OD, PA dba Hamilton Eye Associates that Certificates of Medical Necessity (CMN) will only be signed by QHCPs of the Practice if:

- The physician is the patient's treating physician and the physician will verify the NAME and NPI and address are correct;
- The entire CMN was completed by the supplier in advance of the physician's signature; and
- The item or service is reasonable and necessary based the patient’s conditions and Billing for Non-Covered Services

Occasionally a service will be provided which is not covered by Medicare, but which is covered

under a secondary payer program. Claims may be submitted to Medicare to obtain a denial from Medicare thereby making the claim eligible for the secondary payer.

Third Party Billing Services

If the Practice elects to use a third-party billing service, the billing service must have a written compliance program which substantially meets the obligations described in the Practice's Compliance Program. In addition, the arrangement with the billing service will provide that any billing must be done under the Practice's name and tax identification number and that all receipts from such billings must be deposited into an account controlled by the Practice.

Rental of Space or Equipment

Any rental agreement between Derek Hamilton, OD, PA dba Hamilton Eye Associates and any party which may make referrals to the Practice or may accept referrals from the Practice shall be in writing with a term of one (1) year. The rental fees must be consistent with fair market value in the area and may not be related to the volume or value of referrals or business otherwise generated by referrals between the parties.

Theft or Embezzlement in Connection with Health Care: (18 U.S.C. 669)

Derek Hamilton, OD, PA dba Hamilton Eye Associates will report to the appropriate authorities any embezzlement that occurs within the practice. Legal counsel for the practice will determine if the crime included monies paid by a health care benefit program.

False Statements Relating to Health Care Matters (18 U.S.C. 1035)

Derek Hamilton, OD, PA dba Hamilton Eye Associates will not knowingly falsify or make material false statements regarding delivery of or payment for health care benefits, services or items.

Obstruction of Criminal Investigations of Health Care Offenses (18 U.S.C. 1518)

Derek Hamilton, OD, PA dba Hamilton Eye Associates will not obstruct any criminal investigations, including but not limited to bribery to obstruct or delaying/ preventing communication of information.

Mail and Wire Fraud (18 U.S.C. 1341 and 1343)

Derek Hamilton, OD, PA dba Hamilton Eye Associates will not knowingly participate in any fraudulent schemes, including using mail or electronic transfers for obtaining monies or property under false or fraudulent pretenses.

Criminal Penalties for Acts Involving Federal Health Care Programs (42 U.S.C. 1320a-7b)

Derek Hamilton, OD, PA dba Hamilton Eye Associates will not knowingly and/or willingly make false

statements or representations of material fact for any benefit or payment made under a Federal health care program.

Anti-Kickback Statute

Derek Hamilton, OD, PA dba Hamilton Eye Associates will not knowingly or willfully improperly provide, attempt or offer any money, credit, gratuity or other thing of value for improperly obtaining favorable treatment in connection to supplies, services, materials or equipment.

Derek Hamilton, OD, PA dba Hamilton Eye Associates will not solicit, accept or attempt to accept any money, credit, gratuity or other thing of value for improperly obtaining favorable treatment in connection to supplies, services, material or equipment.

False Claims Act (31 U.S.C. 3729-3733)

Derek Hamilton, OD, PA dba Hamilton Eye Associates will not:

- Knowlingly present, or cause to be presented, a false or fraudulent claim for payment or approval;
- Knowlingly make, use, or cause to be made or used, a false record or statement material to a false or fraudulent claim;
- Has possession, custody, or control of property or money used, or to be used, by the Government and knowlingly delivers, or causes to be delivered, less than all of that money or property;
- Authorize any person to make or deliver a document certifying receipt of property used, or to be used, by the Government and, intending to defraud the Government, makes or delivers the receipt without completely knowling hat the information on the receipt is true;
- Knowlingly buy, or receive as a pledge of an obligation or debt, public property from an officer or employee of the Government, or a member of the Armed Forces, who lawfully may not sell or pledge property;
- Knowlingly make, use, or cause to be made or used, a false record or statement material to an obligation to pay or transmit money or property to the Government, or knowingly conceal or knowingly and improperly avoid or decreases an obligation to pay or transmit money or property to the Government;
- Conspire to commit a violation of any of the above

Exclusion of Certain Individuals and Entities from Participation in Medicare and other Federal Health Care Programs (2 U.S.C. 1320a-7)

Derek Hamilton, OD, PA dba Hamilton Eye Associates will ensure no providers, staff, contractors or vendors are excluded from participation in Medicare and State Healthcare programs by reviewing the Medicare Exclusion (https://exclusions.oig.hhs.gov) prior to offering a position or entering into a contract and annually thereafter.

Addendum to Policy III

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)

Policy IV

Record Retention, Privacy and Security

Derek Hamilton, OD, PA dba Hamilton Eye Associates the importance of preserving the confidentiality of all patient records and to restrict access to such records to authorized personnel. Documents completed by the patient or practice required for compliance or HIPAA regulations will be maintained with the medical record, including but not limited to, acknowledgments of privacy practices and HIPAA consent release forms.

Security of Records

Medical records of patients, whether electronic or paper, will be identified by the individual's first name, last name and other demographic data as needed. Only designated persons shall have access to patient records. Records will be maintained either electronically or in a centralized filing system. Patient files will be maintained on-site until there has been no contact with the patient for a period of five (5) years at which point in time the file may be removed to an off-site storage.

Patient records may be disposed once the practice has not had contact with the patient for the time period designated by state statue. Paper records may be properly destroyed following conversion to an electronic format.

Except upon prior expressed consent from the Security Officer, other designated personnel or the owner/president of the Practice, no medical records in electronic form may be duplicated by any employee except in the case of routine computer backup.

Electronic Transmission

In the event the transmission of medical records is required electronically, appropriate security precautions will be in place.

Business Information

All documents and information regarding the business of Derek Hamilton, OD, PA dba Hamilton Eye Associates including billing and collections shall be retained for a period of seven (7) years or longer if indicated by state statute.

Archival of Records

Derek Hamilton, OD, PA dba Hamilton Eye Associates will maintain a copy of all Compliance and HIPAA manuals in the event a historical review of polices or procedures is required.

Uses and Disclosures of Protected Health Information

It is the policy of this office to obtain a signed patient authorization before making a use or disclosure of PHI, except in those circumstances in which HIPAA does not require such an authorization. As stated in HIPAA, we will not obtain a signed patient authorization in the following circumstances:

- Uses and disclosures for treatment, payment, or health care operations. This includes, among other activities:
  - Providing care to patients in our office;
  - Seeking assistance from medical consultants;
  - Making referrals of patients for follow-up care;
  - Writing/sending, and filling prescriptions for drugs, supplies and materials
  - Preparing and submitting claims and bills;
  - Receiving /posting payments, and collection efforts;
  - Managed care credentialing;
  - Professional licensure and specialty board credentialing;
  - Quality assurance;
  - Financial audits/management;
  - Training of professional and non-professional staff, including students;
  - Office management;
  - Fraud and abuse prevention activities;
  - Personnel activities.
  - Disclosures to business associates that have signed a business associate contract with us.
  - Disclosures that are required by our state law, if we disclose only the precise PHI required, and only to the recipient required.
  - Disclosures to state, local, or federal government public health authorities to prevent or control disease, injury, or disability.
  - Disclosures to local, state, or federal government agencies to report suspected child abuse or neglect.
  - Disclosures to individuals or organizations under the jurisdiction of the United States Food and Drug Administration (FDA), such as drug or medical device manufacturers, regarding the quality or safety of drugs or medical devices.
  - Disclosures to local, state, or federal governmental agencies to report suspected abuse, neglect, or domestic violence regarding adults, provided we:

- Get an informal agreement from the patient unless:
- Someone else is acting on behalf of the patient and we think that this person is the abuser and that telling him or her would not be in the best interest of the patient.

    - We are required by law to report our suspicions;
  - We are permitted, but not required by law to disclose the PHI, and we believe that a report is necessary to prevent harm to our patient or other potential victims;
    - We tell the patient that we are making this disclosure, unless:
    - Telling the patient would put the patient at risk for serious harm, or;

  - Disclosures for health oversight audits, investigation, or disciplinary activities; provided we only disclose to a federal, state or local government agency (or a private person or organization acting under contract with or grant of authority from the governmental agency) that is authorized by law to conduct oversight activities.
  - Disclosures in response to a court order, provided we disclose only the precise PHI ordered, and only to the person ordered.
  - Disclosures in response to proper subpoena, provided that:
  - We make sure that either we or the person seeking the subpoenaed information makes a reasonable effort to notify the patient in advance, and the patient has a chance to object to the court about the disclosure.
  - We make sure that either we or the person seeking the subpoenaed information makes a reasonable effort to have the court issue a protective order.
  - Disclosures to police or other law enforcement officers regarding a crime that we think

happened at our office, provided we reasonably believe that the PHI is evidence of a crime.
    - Uses of PHI to market or advertise our own health care products or services, or for any other marketing exception.
    - Disclosures to a researcher with a waiver of authorization from an IRB or privacy board; to a researcher using the PHI only for purposes preparatory to research or to a researcher only using the PHI of deceased patients, provided that the researcher gives us the assurance required by HIPAA.
    - Any other routine disclosures without patient consent include: None
- If at any time a proposed use or disclosure does not fit exactly into one of the exceptions to the need for an authorization described above, we will obtain a signed patient authorization before making the disclosure.

Providing Information to Family and Friends of Patients Involved in Care

It is the policy of this office to give patients a chance to agree or object to providing PHI to close family or friends who are helping with the patient's care.

If we feel that it is necessary or appropriate to inform a close family member or friend who is involved in a patient's care about certain PHI relevant to their involvement, we will give the patient a chance to agree or object to such disclosure before we make it. If the patient is present or available when this need arises, we will do any of the following:

- Get an oral agreement from the patient that the disclosure is acceptable.
- Give the patient a chance to object to the disclosure.
- Infer from the circumstances that the patient does not object. For example, we can reasonably infer that the patient does not object if the family member or friend is in the examining room with the patient.
- If the patient is not present or available when the need arises, we will use our best judgment about whether it is in the patient's best interest to disclose the information. An example might be when a family member or friend comes to our office to pick up materials and/or supplies that the patient previously ordered, as a convenience to the patient.
- If we make a disclosure to a close family member or friend under the circumstances described above, we will only disclose information that is relevant to the family member or friend's involvement with the patient's care. Examples:
    - If the patient's spouse will pick up the ordered materials and/or supplies, we will provide the materials and/or supplies but not disclose any diagnoses or special features of the materials and/or supplies.
    - If a son or daughter will assist a patient with administering prescription medications, we will provide instruction for the administration but will not disclose the patient's diagnosis.
- If someone claiming to be a family member or friend of the patient initiates contact with us seeking information, we will:
    - Verify the identity of the caller and the relationship with the patient.
    - Determine if they are involved in the patient's care.
    - Determine if the patient is available (by phone, email, or other communications method) to either agree or object to the disclosure. We will give the patient the chance to agree or object. If the patient objects, we will not disclose any information to the caller. If the patient is not available by any reasonable means, we will use our best judgment to determine whether disclosure of information is in the patient's best interest.

Marketing

It is the policy of this office to require a signed patient authorization to use or disclose PHI for marketing or advertising purposes, subject to the conditions and exceptions described in this policy.

With the changes to the Omnibus Rule of 2013, Marketing is defined as a communication about a product or service that encourages recipients of the communication to purchase or use the product or service. In addition, financial remuneration was defined as a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.

We use PHI in connection with a marketing communication if we review patient data bases or records to target the communication to specific recipients. We disclose PHI in connection with a marketing communication if the content of the communication includes PHI (photographs, testimonials, and the like).

If a marketing communication discloses PHI in any such manner, we will always get a signed patient authorization prior to disclosing the information.

If we use PHI in connection with a marketing communication, we will get a signed patient authorization, except for:

- Marketing communications about our own health care products or services;
- Communications made during treatment, case management, or care coordination for an individual patient;
- Communications regarding government and government-sponsored activities;
- Face-to-face communications even if remuneration is received from a third party, or a promotional gift of nominal value is provided by the covered entity;
- Refill reminders, medication management reminders, etc.;
- Where financial remuneration consists of only the actual costs of labor, supplies and postage;
- Communications falling into these specified categories do not require a signed patient authorization.

When we need an authorization, we will include information about any money or other valuable thing that we get from someone else in common with the communication.

Many marketing communications do not use or disclose PHI. These communications are not affected by HIPAA's Privacy Rule. Examples of these communications are:

- General TV ads;
- Brochures mailed to "occupant" using a zip code data base.

The Privacy Officer or other designated personnel is responsible for obtaining signed patient authorizations for marketing, when they are required, and for making sure that the authorization discloses any money or thing of value that we get from someone else in connection with the marketing communication.

Sale of PHI

We will not sell the PHI for any type of financial remuneration. The exceptions to sale of PHI are:

- For treatment purposes;
- For payment of treatment rendered;
- For Public Health Reasons;
- For sale of our covered entity to another covered entity;
- If it is required by law;
- For any business associate activities;
- For research;
- In an individual for access and accounting;
- Any other permissible purpose if remuneration is limited to reasonable, cost-based fee for preparation and transmittal.
- The fee for copies of records given to the patient will be $18.00

Fundraising

PHI from our patient may be used in fundraising activities that our practice is involved in.

Patients have a right to opt out of all fundraising activities. Each communication will include a method to opt out of all fundraising activities. The method will not impose any burden on the patient. If a patient elects to opt out of fundraising activities, our practice will assure:

- The method of opt out is not burdensome on the patient;
- It will not impact patient care or treatments they are receiving;
- No future communications regarding fundraising will be sent to the patient;
- If a patient chooses to opt back into fundraising communications at a future time, they can contact the Privacy Officer or other designated personnel.

Disclosures for Research

It is the policy of this office to obtain a signed patient authorization before using or disclosing PHI for research purposes, unless the research satisfies one of HIPAA's exceptions to the need for authorization. In accordance with HIPAA's exceptions:

- We will not obtain a signed patient authorization if a researcher has obtained, and presents to us, a proper waiver of authorization from an Institutional Review Board (IRB) or Privacy Board.
- An IRB is an interdisciplinary group convened to oversee the protection of human subjects in research, pursuant to regulations of the U.S. Food and Drug Administration or the "common rule". A Privacy Board is an interdisciplinary group that has members from a variety of professions relevant to protecting privacy, has at least one member that is not connected with the researcher or the organization holding the PHI, and does not allow anyone to participate in the review of research if that person has a conflict of interest.

To be a proper waiver, the following criteria must be satisfied, we must have documentation that the IRB or the Privacy Board determined that a waiver is appropriate because:

- The use or disclosure of PHI during research poses no more than minimal risk to the privacy of the research participants;

- The PHI is necessary for the research;
- As a practical matter, the research could not proceed without a waiver;
- We must have documentation of the IRB of the Privacy Board specification of what PHI can be used or disclosed as part of the waiver;
- We must have documentation that the IRB or the Privacy Board made all its determinations according to proper procedures;
- The documentation must be signed by the chair of the IRB or Privacy Board. The documentation must include the name of the IRB or Privacy Board and the date of its approval of a waiver.

The Privacy Officer or other designated personnel is responsible for obtaining proper IRB or Privacy Board waivers of authorization for research that we want to conduct without a signed patient authorization. Our Privacy Officer or other designated personnel will consult with the IRB or Privacy Board to determine what information the IRB or Privacy Board wants to make its determinations. If an outside researcher wants to use PHI about our patients, our Privacy Office or other designated personnel is responsible for reviewing all documents that the researcher presents to us in support of a waiver of authorization, to verify their sufficiency.

The Privacy Officer or other designated personnel is responsible for any ongoing communication with an IRB or Privacy Board that has granted a waiver of authorization, if any is needed.

We will rely upon the IRB or Privacy Board's statement of the PHI that is subject to the waiver as being the minimum amount of PHI that is necessary for the research.

We will not obtain a signed patient authorization if a researcher gives us specific assurances that:

- The researcher wants to review or disclose PHI solely to prepare a research protocol or take other steps in preparation for research. These might include checking a database to see if any patients are good candidates for the research;
- The researcher will not take any PHI off-site from where it is held;
- The researcher needs the PHI for research purposes.

Our Privacy Officer or other designated personnel is responsible for reviewing all assurances that an outside researcher may give us in support of a disclosure of PHI. The Privacy Officer or other designated personnel is also responsible for providing specific assurances whenever we want to obtain PHI from someone else for activities preparatory to research.

We will not obtain a signed patient authorization if a researcher wants the PHI to conduct research solely on deceased patients and provides specific assurances that:

- The researcher is asking for PHI strictly to conduct research;
- The person identified in the PHI add is deceased. The researcher should apply for a death certificate;
- The researcher needs the PHI to perform research.

If an authorization is needed, our Privacy Officer or other designated personnel is responsible for obtaining it, if we want to conduct the research. Our Privacy Officer or other designated personnel is also responsible for reviewing all authorizations presented to us by outside researchers.

Conditioned and unconditioned authorizations maybe used and combined into one document if:

- The two different studies are clearly identified on the consent form;
- A signature is required for both research studies;
- The unconditioned authorization may not be an automatic opt in, and will require an additional

signature

Personal Representatives for Patients

It is the policy of this office to allow properly authorized personal representatives access to protected health information as needed to exercise all patient rights regarding the use and disclosure of PHI.

Adult patients and emancipated minors:

Adult patients are those over the age of eighteen (18) years.

Emancipated minors are people under the age of eighteen (18) years who have the legal right to be treated as an adult. This happens if the child is married or has voluntarily left the parental home for any reason and established independent living arrangements, other than being away from home for school or health reasons. Once a child is emancipated, the emancipation is permanent.

Generally, adults and emancipated minors personally handle all matters regarding their PHI. Sometimes, however, they may be unable to do so because of mental incapacity. In this case, the following people can substitute for the adult or emancipated minor to sign all permissions and exercise all rights regarding PHI:

- A court appointed full guardian for a developmentally disabled individual or incapacitated individual;
- The patient advocate named in a patient advocate designation; or
- The person granted a power of attorney

Un-emancipated minors:

An un-emancipated minor is a person under the age of eighteen (18) years.

Generally un-emancipated minors are not able to handle any matters regarding their PHI because the law presumes them to be incapacitated. The following people can handle signing all permissions and exercise all rights regarding an un-emancipated minor's PHI:

- Either parent unless the parental rights have been terminated;
- A court appointed guardian;
- People who are considered "in loco parentis", that is, who have juvenile legal custody or physical custody and are responsible for support and care

Deceased patients:

Per section 164.51(b) (5), PHI of deceased patients is no longer protected under HIPAA Privacy requirements after fifty (50) years past the death of the patient. Prior to fifty years past the death of the patient, state law may govern which people have the authority to sign permission and exercise rights regarding the PHI of deceased patients.

Derek Hamilton, OD, PA dba Hamilton Eye Associates will review all applicable state laws prior to the release of deceased patients protected health information. In the absence of state law, section 164.510(b) (5) will be followed:

- A covered entity may disclose to a family member, other relative, or a close friend of the individual, or any other person identified by the individual, the protected health information directly relevant

to such person's involvement with the individual's health care or payment related to the individual's health care.

- A covered entity may use or disclose protected health information to notify or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death.

Notice of Privacy Practices

It is the policy of Derek Hamilton, OD, PA dba Hamilton Eye Associates to:

- Prominently post the Notice of Privacy within the office and on any web site maintained that provides information about our practice's customer services or benefits;
- Distribute a Notice of Privacy Practices (NPP) to every patient at their first appointment, materials and/or supplies pickup, or similar encounter;
- Verify the status of the NPP at every visit and obtain when indicated;
- Request patient to sign an Acknowledgement of Receipt (AOR) of the NPP;
- Maintain a copy of the signed AOR;
- If the patient refuses to sign, a note will be made within the patient's record.

The NPP and AOR currently in use is attached to this Policy. The Privacy Officer or other designated personnel has authority to change these documents. In the event the NPP is updated, all patients must acknowledge receipt of the updated notice.

The Notice of Privacy Practices is posted Patient waiting room, so it may be viewed by any person entering the office. Derek Hamilton, OD, PA dba Hamilton Eye Associates will give a copy of the Notice of Privacy Practices and attempt to obtain a signed AOR At the patients first visit to the office. Signed copies of the AOR will be maintained in Scanned into the patients EHR chart.

The Notice of Privacy is available to all patents upon request. Derek Hamilton, OD, PA dba Hamilton Eye Associates will keep copies available to patients at/in At the front desk.

It is the standard of this practice to follow published HIPAA/CMS guidance regarding the content of the NPP.

Addendum to Notice of Privacy Practices

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)

Designated Record Set

This office considers the following records to be the "designated record set" for purposes of patients' right to access and amend their PHI:

1. The patient's clinical chart, hard copy or electronic:
   - Reports or screening and diagnostic tests;
   - Notes on examinations;
   - Patient demographic information, including email and photos (if applicable);
   - Consultant reports;
   - Refraction results;
   - Materials and/or supplies prescriptions;
   - History and medication reports;
   - All other clinical information;
2. The patient's billing records, hard copy or electronic:
   - Insurance claims;
   - Remittance advice from insurance companies;
   - Electronic fund deposit receipts;
   - Bills to patients;
   - Evidence of payment by patients;
   - Collection records;
   - Referrals to collection agencies or attorneys;
   - Reports to consumer credit agencies for unpaid balances;
   - All other billing, claim, payment, and collection records;
3. Materials and/or supply order and receipt forms specific to a patient, hard copy or electronic.

Addendum to Designated Record Set

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)

Patient's Access to Their PHI

- Derek Hamilton, OD, PA dba Hamilton Eye Associates will allow patients to inspect and/or copy their own PHI under the conditions stated in this policy. If the patient has an authorized personal representative the personal representative can inspect or copy the patients PHI on behalf of the patient.
- Patients are asked to send a written request to inspect or copy their PHI. If a patient calls on the telephone asking to inspect or copy their PHI, we will inform the patient of the requirement to send the request in writing.
- The Privacy Officer or other designated personnel is responsible for handling patient requests to inspect or copy their PHI.
- We will respond to a patient's request to inspect or copy their PHI (paper or electronic) within 30 days of receiving the written request. If the PHI is stored off-site it will be made available for patient review within 60 days.
- In the event of extenuating circumstances, Derek Hamilton, OD, PA dba Hamilton Eye Associates may be allowed one 30-day extension. Patient will be notified in writing of the extension before the original time period expires.
- The patient may also request to receive electronic access to their PHI. We will comply with this requirement under the following circumstances:
- The patient must accept the designated media that we have defined for our practice. We cannot accept a patient's media device.
- If the patient refuses the media device that we provide, we will provide a paper copy of the information requested.
- If the patient requests information via email, the appropriate security measures and patient consent will be in place.
- The request to inspect or receive copies of protected health information may be denied for one or more of the following circumstances:

Unreviewable **grounds for denial (45 CFR 164.524(a) (2)):**

- The request is for psychotherapy notes, or information compiled in reasonable anticipation of, or for use in, a legal proceeding.
- An inmate requests a copy of her PHI held by a covered entity that is a correctional institution, or health care provider acting under the direction of the institution, and providing the copy would jeopardize the health, safety, security, custody, or rehabilitation of the inmate or other inmates, or the safety of correctional officers, employees, or other person at the institution or responsible for the transporting of the inmate. However, in these cases, an inmate retains the right to inspect her PHI.
- The requested PHI is in a designated record set that is part of a research study that includes treatment (e.g., clinical trial) and is still in progress, provided the individual agreed to the temporary suspension of access when consenting to participate in the research. The individual’s right of access is reinstated upon completion of the research.
- The requested PHI is in Privacy Act protected records (i.e., certain records under the control of a federal agency, which may be maintained by a federal agency or a contractor to a federal agency), if the denial of access is consistent with the requirements of the Act.
- The requested PHI was obtained by someone other than a health care provider (e.g., a family member of the individual) under a promise of confidentiality and providing access to the

information would be reasonably likely to reveal the source of the information.

Reviewable **grounds for denial (45 CFR 164.524(a) (3)). A licensed health care professional has determined in the exercise of professional judgment that:**

- The access requested is reasonably likely to endanger the life or physical safety of the individual or another person. This ground for denial does not extend to concerns about psychological or emotional harm (e.g., concerns that the individual will not be able to understand the information or may be upset by it).
- The access requested is reasonably likely to cause substantial harm to a person (other than a health care provider) referenced in the PHI.
- The provision of access to a personal representative of the individual that requests such access is reasonably likely to cause substantial harm to the individual or another person.

If we deny a patient access to their PHI, we will notify the patient of our decision. The patient has a right to a request a review of our decision. The review will be handled by Derek Hamilton, OD.

- The Privacy Officer or other designated personnel will review the information as requested by the patient and decide if the denial is reviewable as outlined above.
    - If not, the patient may inspect or copy the information.
    - If so, the patient may not inspect or copy the information.
- The patient may not further question our decision. Our notice (outlined below) to the patient will include instructions about how the patient may take advantage of this review right.

When we permit a patient to inspect or copy the requested information, we will:

- Provide the information in the form or format that the patient requests, if we can reasonably produce it that way. If we cannot, we will either agree with the patient about another format or give it to the patient in hard copy.
- Allow the patient to inspect or copy the information at our office during normal business hours. Within these limits, the patient can select the date and time to inspect or copy the records.
- Charge the patient a legal and reasonable fee for copying the requested information for the patient. If the patient wants the information mailed to him or her, we will charge the patient the cost of mailing, or any special delivery method that the patient wants us to use. We will collect all charges before we make any copies.
- If the patient agrees in advance, we may summarize the requested information and give this to the patient instead of having the patient inspect all the information or copy all of it. If we do this, we will charge the patient the cost of preparing the summary. We will collect all charges before preparing the summary.
- We will notify the patient that their request to access information is granted (see Forms and Templates).

Notice of Denial of Access to PHI

Derek Hamilton, OD, PA dba Hamilton Eye Associates will utilize the following or similar template to notify the patent of the denial for access to their PHI. This will be on the Practice's letterhead. At a minimum it will contain information to file a grievance. (See Forms and Templates)

Amendment of PHI

It is the policy of this office to permit patients to request amendments to their PHI under the conditions stated in this policy. If the patient has an authorized personal representative, the personal representative may exercise this right on behalf of the patient.

We require that all requests to amend PHI be in writing. If a patient calls on the telephone to request an amendment, we will inform the patient of the requirement to submit this request in writing.

The Privacy Officer or other designated personnel is responsible for handling patient requests to amend their PHI.

- We will respond to requests for amendment within 60 days after we receive the written request.
- In the event of extenuating circumstances, Derek Hamilton, OD, PA dba Hamilton Eye Associates may be allowed one 30-day extension. Patient will be notified in writing of the extension before the original time period expires.

We can deny a requested amendment only for one or more of the following reasons:

- Was not created by the covered entity, unless the individual provides a reasonable basis to believe that the originator of protected health information is no longer available to act on the requested amendment;
- Is not part of the designated record set;
- Would not be available for inspection under *Patient Access to Their PHI* (above)
- Is accurate and complete.

If we deny a request, we will notify the patient (see below). We will inform the patient of:

- The basis for the denial, in accordance
- The individuals's right to submit a written statement disagreeing with the denial and how the individual may file such a statement

The denial letter (see Forms and Templates) will at a minimum include:

- A statement that, if the individual does not submit a statement of disagreement, the individual may request that the covered entity provide the individual's request for amendment and the denial with any future disclosures of the protected health information that is the subject of the amendment; and
- A description of how the individual may complain to the covered entity or to the Secretary. The description must include the name, or title, and telephone number of the contact person or office.

If we grant the requested amendment, the patient will receive notification (see Forms and Templates) including at a minimum:

- Append or link the corrected information to the information that we are holding.

In addition, Derek Hamilton, OD, PA dba Hamilton Eye Associates will:

- Send the corrected information to anyone who we know has previously received the incorrect information.

Send the correct information to anyone that the patient requests.

Addendum to PHI Access

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)

Accounting for Disclosures of PHI

It is the policy of this office to provide patients, upon request, an accounting of the disclosure that we have made of their PHI during the six (6) years preceding their request, subject to the terms and conditions stated in this policy.

- We will provide an accounting of all our disclosures of a patient's PHI, except the following:
    - Disclosures for treatment, payment, or health care operations;
    - Disclosures made with a signed patient authorization
    - Disclosures that are incident to a use or disclosure otherwise permitted;
    - Disclosures to the patient personally;
    - Disclosures for the facility's directory and disclosures to family or friends involved in a patient's care;
    - Disclosures occurring prior the compliance date for Derek Hamilton, OD, PA dba Hamilton Eye Associates
- Derek Hamilton, OD, PA dba Hamilton Eye Associates will keep track of all disclosures that are made of our patient's PHI, except for those disclosures listed in paragraph above. Our Privacy Officer or other designated personnel is authorized to make a disclosure of PHI that is not listed above. These disclosures will be documented in the patient file or designated storage site. Derek Hamilton, OD, PA dba Hamilton Eye Associates will keep a list of disclosures In the patient electronic record.
- Derek Hamilton, OD, PA dba Hamilton Eye Associates will keep this documentation for six (6) years. This documentation will include:
    - The date of the disclosure;
    - The name and address (if known) of the person or organization that received the PHI;
    - A description of the PHI that was disclosed;
    - A statement of the purpose or basis for the disclosure, or a copy of any request for the PHI that prompted the disclosure;
- Derek Hamilton, OD, PA dba Hamilton Eye Associates requires that all requests for an accounting be in writing. If a request is made by telephone, we will advise the caller to submit it in writing to Our Privacy Officer or other designated personnel.
- Derek Hamilton, OD, PA dba Hamilton Eye Associates will respond to a request for an accounting within 60 days from our receipt of the written request. If we are unable to provide the accounting within this 60 day period, we may have one extension of 30 days, provided that we notify the patient of this delay before the original 60 day period expires. This notice must include the reason for the delay and the date that we will have the accounting ready. Our Privacy Officer or other designated personnel is responsible for advising patients of delays.
- The accounting of disclosures will list all information outlined above. If we make repeated disclosures of PHI about a patient to the same person or organization for the same purpose, our accounting will provide all information for the first such disclosure, and then indicate the frequency or periodicity of the other disclosures, and the date of the last such disclosure. Our Privacy Officer or other designated personnel is responsible for generating requested accountings and furnishing them to the patient.
- We will provide patients with one free accounting, upon request, within any twelve (12) month period. For additional accountings within any twelve (12) month period, we will charge a legal and reasonable fee for the actual cost of preparing and mailing the accounting. Payment will be required before any subsequent disclosures are released.

Addendum to Accounting for Disclosures

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)

Restrictions on Use of PHI

It is the policy of this office to permit patients to request that we restrict the way that we use some PHI for purposes of treatment, payment, or health care operations.

- The Public Information Officer or other designated personnel will handle requests from patients for restrictions on the use PHI for treatment, payment, or health care operations.
- Generally, Derek Hamilton, OD, PA dba Hamilton Eye Associates will not agree to restrictions requested by patients. In unusual circumstances that the Public Information Officer or other designated personnel thinks are meritorious, we may agree to a requested restriction.
- If we agree to a requested restriction, the Public Information Officer or other designated personnel will document its terms and this documentation will be kept in In the patient electronic record. The Public Information Officer or other designated personnel will communicate the terms of the restriction to all staff and/or business associated as applicable.
- No previously agreed to restriction will prevent us from using any PHI in an emergency treatment situation.
- If we have agreed to a restriction but can no longer practically honor it, our Public Information Officer or other designated personnel will do one of the following:
    - Contact the patient to determine a mutually agreeable termination of the restriction. Our Public Information Officer or other designated personnel will document this agreement and keep it in patient's record.
    - Contact the patient and advise that we are no longer able to honor the restriction that was previously agreed to. This change in restriction will apply only to PHI that we obtain or generate after the notice is given.
- Restriction to health insurance company:
- If a patient presents to the office and requests that the information not be sent to their insurance company, they are required to complete the Restriction of Health Information form and make payment in full for all services. The restriction will only apply to the services for that date of service.
- If any outstanding balance exists or the patient does not pay, we have the right to send the claim and PHI to the insurance company
- Once restricted the encounter may not be billed to an insurance company without additional consent from the patient.
- In the event a restriction is in place for a date of service, a paper medication prescription should be given to the patient when applicable.

Addendum to PHI Restrictions

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)

Confidential Communication Methods with Patients

It is the policy of Derek Hamilton, OD, PA dba Hamilton Eye Associates to accommodate requests from patients to send PHI to them in a confidential way. If the patient requests that we use a specific method to communicate with them to preserve the confidentiality of their information, we will accommodate that when reasonably possible.

- We require that such requests be in writing. If a request comes in by telephone, we will advise the patient how to send the request in writing.
- We will not ask or require a patient to explain why they want the specific communication method.
- We will charge the patient the reasonable cost of complying with their request, if any.
- Our Public Information Officer or other designated personnel is responsible for receiving and acting upon patient requests for confidential communication methods.

If a patient requests confidential means of communication to be used, Derek Hamilton, OD, PA dba Hamilton Eye Associates has to use the follow methods of communication: In the patient electronic record

Addendum to Communication Method

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)

Minimum Necessary Uses and Disclosures of PHI

It is the policy of Derek Hamilton, OD, PA dba Hamilton Eye Associates to use or disclose the minimum amount of PHI necessary to accomplish the purpose for the use or disclosure, under the conditions and exceptions described in this policy.

- Access will be assigned by role:
  - All doctors and technicians who document in the record as part of their role may access any and all PHI, including the entire clinical chart, for treatment purposes.
  - Coders/billers may access Patient demographics, insurance information and chart notes. They may also access billed charges, NPI and Tax ID information.
  - Receptionist may access Patient demographics, insurance information and chart notes.
  - Physicians may access Patient demographics, insurance information and chart notes.
  - Other ancillary staff may access Practice Administrator specific to their role(s)
- Clinical charts and billing records will be kept in Stored on the server. when not in use. Only authorized staff will have access to this secure storage.
- Computers will be password screen locked or turned off when the user is away from their workstation.
- Staff are prohibited from talking about patients in public areas.
- All staff will sign a confidentiality agreement indicating their commitment to access only the minimum amount of PHI necessary for them to do their job. Violation of this agreement is grounds for employment discipline up to and including termination according to our sanctions policy.
- Requests for PHI from an authorized third party will be provided only the PHI necessary to satisfy the purpose of that disclosure. This does not apply in the following cases:
  - The patient has authorized the disclosure;
  - The disclosure is for treatment purposes.
- As appropriate, only the PHI requested will be released. The Privacy Officer or other designated personnel may determine if the PHI requested is appropriate.
- In the event Derek Hamilton, OD, PA dba Hamilton Eye Associates requests PHI about one of our patients only the minimum PHI necessary for us to accomplish the purpose will be included in the request.
- Immunization data may be released to schools without a written authorization if:
  - The verbal authorization is made by an eligible person;
  - Records are released directly to the school.

Addendum to Minimum Necessary

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)

Verification before Disclosing PHI

It is the policy of Derek Hamilton, OD, PA dba Hamilton Eye Associates to verify the authority and identity of people or organizations that request us to disclose PHI about our patients, subject to the following conditions:

- If a patient has a personal representative who seeks to sign an authorization to disclose the patient's PHI to a third party, or to exercise any of the rights that patients have regarding their PHI, following steps will be taken before we accept their signature or allow them to exercise those rights:
    - Copies of any documents that are relevant to their status as personal representative will be reviewed, i.e. a copy of the court papers appointing a legal guardian, or a healthcare power of attorney
    - Picture identification of the person serving as personal representative will be requested as applicable.
- If there are questions about the documents, our Privacy Officer or other designated party will work to resolve them. We will not disclose any PHI until all questions are answered and we have proper evidence of the authority of the person acting as personal representative.
- If we receive a request from a third party without a signed patient authorization to see or receive a copy of PHI Derek Hamilton, OD, PA dba Hamilton Eye Associates will take the following steps before allowing such access:
    - Request evidence that the requestor is affiliated with an organization or government agency that is authorized to have access to PHI without an authorization. Evidence may include an official badge or identification card, an assignment on official letterhead, or similar items.
    - Request legal picture identification.
    - Ask the requestor to specify the legal authority that the requestor believes allows access to PHI.
- The Privacy Officer or other designated personnel will review all evidence supplied by the requestor to make sure that the requestor has proper authority to access PHI with no limits or expiration dates.
- The Privacy Officer or other designated personnel is responsible for this review. If there are questions the Privacy Officer or other designated personnel will work to resolve them. We will not disclose any PHI until all questions have been resolved and we are sure that the requestor has proper authority to access the PHI.

Addendum to Disclosure Verification

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)

De-Identification of PHI

It is the policy of Derek Hamilton, OD, PA dba Hamilton Eye Associates to use de-identified information instead of PHI whenever this is feasible. None of HIPAA's Privacy Rule's restrictions on the use and disclosure of PHI apply to de-identified information, which may be used or disclosed freely. The Privacy Officer or other designated personnel is responsible for determining the feasibility of de-identifying any PHI and for performing such de-identification.

Derek Hamilton, OD, PA dba Hamilton Eye Associates will remove all the identifiers with respect to our patient, the patient's relatives, the patient's household members, and the patient's employer including:

- Names;
- All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geo-codes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:
  - The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
  - The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
- All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints; 17. Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic or code.

We will not consider information to be de-identified unless we have no actual knowledge that the remaining information can be used, either alone or in combination with other reasonably available information, to identify a patient.

If de-identified information is disclosed, we will not provide any key that we create to re-

identify the information.

An outside company may be used to assist in de-identifying PHI. If we do, we will enter into a business associate contract with this outside company. In this case the proper Business Associate Agreement will be in place.

Addendum to De-indentification

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)

Limited Data Sets

It is the policy of Derek Hamilton, OD, PA dba Hamilton Eye Associates to use a limited data set for certain disclosures of PHI, whenever this is appropriate and feasible.

We will use a limited data set for disclosures that are for research, public health purposes, or health care operations.

A limited data set is PHI from which all of the following identifiers for the patient, patient's relatives and members of the patient's household have been removed:

- Names;
- Postal address information, other than town or city, State, and zip code;
- Telephone numbers;
- Employer Information
- Fax numbers;
- Electronic mail addresses;
- Social security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints; and 16. Full face photographic images and any comparable images.

The Privacy Officer or other designated personnel is responsible for determining whether to release a limited data set.

When a limited data set is disclosed, the recipient will be required to enter into a data use agreement. The data use agreement (see Forms and Templates) restricts the ways in which the recipient can use the limited data set.

Addendum to Limited Data Set

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)

HIPAA Security Policies

Risk Analysis

Purpose: Implement policies and procedures to assure prevention, detection, containment, and correction of any potential security violations. Evaluation of potential threats, vulnerabilities and risks to the organization.

Policy: Derek Hamilton, OD, PA dba Hamilton Eye Associates will conduct regular assessments of risks and vulnerabilities to PHI created and managed in all media. The regular reviews will help protect the confidentiality, integrity, and availability of PHI.

Procedure: A regular risk analysis will be conducted in accordance with the HIPAA Security review. All documentation of identified risks and mitigation to the risks will be maintained by Derek Hamilton, OD, PA dba Hamilton Eye Associates for six (6) years past the completion of the assessment.

The Risk Analysis will include, but not limited to the following:

1. A physical review of all clinic locations and other areas where PHI will be kept and maintained.
2. Information System Inventory List, including location of systems (maintained by Derek Hamilton, OD, PA dba Hamilton Eye Associates or designated vendor)
3. Information Security analysis review.
4. Creation of a Risk Analysis Report as well as a Risk Mitigation Report to be used as a working document when working to resolve identified threats.
5. Follow-up documentation on the mitigation or the risks (maintained by Derek Hamilton, OD, PA dba Hamilton Eye Associates).
6. The HIPAA Security Officer, or other designated personnel, will be responsible for the completion and maintenance of this documentation.

Formal Risk Analysis will be completed on an annual basis.

Risk Management

Purpose: The management and oversight of risks and vulnerabilities to PHI and ePHI.

Policy: Derek Hamilton, OD, PA dba Hamilton Eye Associates will implement and manage the proper administrative, physical, and technical security safeguards that are reasonable and appropriate to Derek Hamilton, OD, PA dba Hamilton Eye Associates in efforts to maintain the confidentiality, integrity and availability of the ePHI and PHI.

The following measures will be implemented to manage risks and vulnerabilities identified:

1. A regular review of the risk analysis and mitigation report to evaluate the current state of all the identified risks and vulnerabilities to the organization.
2. Ad-hoc meetings as needed with information technology, administration, and other appropriate people in order to review the current state of mitigation plans for identified risks.

3. Regular HIPAA Privacy and Security Compliance training for all staff and volunteers at Derek Hamilton, OD, PA dba Hamilton Eye Associates.
4. Regular review of existing policies and procedures to assure compliance with regulations and effectiveness in the organization.

Addendum to Risk Analysis/Management

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)

Sanctions -164.308(a) (1) (ii) (C)

Purpose: All members of the workforce at [Organization] will be responsible for compliance of all privacy and security policies and procedure. Workforce members who fail to comply with the policies and procedures will be subject to possible sanctions.

Policy: [Organization] will apply the proper sanctions for all workforce members who fail to comply with the Privacy and Security Policies and Procedures for (Derek Hamilton, OD, PA dba Hamilton Eye Associates).

All potential violations to the Privacy and Security Policies will be evaluated by the Security Officer or other designated personnel. Based on the results of that evaluation, a level of violation will be assigned. The appropriate disciplinary action, based on the level of violation, will be assigned and documented.

Violation Level	**Violation Type**	**Examples (not all inclusive)**	**Disciple Recommendations**
Level 1	Accidental disclosure or violation	Faxing to incorrect recipient, mailing to incorrect patient, forgetting to log out of electronic health record	Coaching or verbal discipline
Level 2	Failure to follow policies and procedures, carelessness or lack of proper job performance	Repeated level I violations, not properly safeguarding usernames and passwords, improper disposal of protected health information, ending email with proper security measures	Verbal or written warning
Level 3	Deliberate and purposeful violation without intent to harm	Repeated level 1 and/or 2 violations, accessing protected health information without a business need, posting protected information on social media without the intent to harm	Final written warning or suspension

Level 4	Willful and malicious violation with intent to harm	Repeated level 1, 2 and/or 3 violations. Purposefully disclosing information to individuals, posting information on social medical with intend to harm, other violations of the privacy and security policies with intent to harm.	Termination of contract and/or employment

Addendum to Sanctions

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)

Transfer Methods for Protected Health Information

Purpose: Transfer of protected health information (PHI) will be performed in a way the privacy and security of the information can be protected.

Policy: The following are deemed acceptable methods of transfer of PHI. Per the published regulations, HIPAA allows you to use email, telephone, or fax machines to communicate with patients and other health care professionals using appropriate safeguards to protect patient privacy.

- Client Systems: (such as EHR portal)
- Secure Messenger/Secure Email

In the event other methods of transfer are utilized the workforce of Derek Hamilton, OD, PA dba Hamilton Eye Associates will ensure that the information is being directed to the correct person. Security measures may include but are not limited to:

Fax:

- Confirm number that fax is being sent to
- Included a confidentiality clause on the cover sheet
- Verify correct number was used on fax reporting

Email:

- Ask the recipient to email you so you can respond with the requested information
- Verify verbally the email address to use
- Follow up with recipient to ensure receipt
- Recipient should be advised this is not considered a HIPAA secure transfer of data

Mobile Devices:

- Use a password or other authentication
- Enable encryption
- Disable file sharing applications
- Install security software
- Maintain physical control of the device
- Follow media destruction and re-use guidelines

Addendum to PHI Transfer Methods

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)

Information System Activity Review

Purpose: Access to protected health information, when applicable, for the staff of Derek Hamilton, OD, PA dba Hamilton Eye Associates workforce will be reviewed to assure appropriate use.

Policy: Derek Hamilton, OD, PA dba Hamilton Eye Associates will conduct regular audits of system activity to ensure that patient information is accessed only when there is a legitimate business reason to do so. Reviews may be conducted using audit logs, access log, and security incident reports; however, this review is not limited to these reports.

Procedure:

When/if applicable:

- Derek Hamilton, OD, PA dba Hamilton Eye Associates will review access to patient information on the end of the day for each quarter in the calendar year (March 31, June 30, September 30, and December 31).
- Information system activity documents will be run and reviewed for the appropriateness of access. Systems reviewed may include, but are not limited to, electronic medical record software, practice management software/financial software, network access, and internet usage.
- The review logs will be dated and stored by the HIPAA Security Officer or other designated personnel.
- If a violation is suspected, an investigation will open in accordance with the Breach Notification Policy.
- All suspected violations will be documented and maintained in the employee’s personnel file.
- All information system activity review logs will be kept and maintained for 6 years past the date of the audit.

Addendum to System Activity Review

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)

Information Access Management

Access Authorization, Establishment, Modification, and Termination

Purpose: To ensure that adequate authorization is granted prior to the workforce member getting access to electronic PHI.

Policy: Derek Hamilton, OD, PA dba Hamilton Eye Associates will ensure that a process exists for granting access to PHI to all workforce members. Access will be granted to each individual or workstation based on the minimum necessary standard for fulfillment of their job.

Procedure:

1. All workforce members who need electronic access to information for the purpose of their job will be sent to the HIPAA Security Officer or other designated personnel and recommended by their immediate supervisor.
2. The HIPAA Security Officer or other designated personnel will grant access based on the minimum necessary standard for fulfillment of job duties.
3. The HIPAA Security Officer or other designated personnel will be responsible for assuring access that is granted is appropriate and proper and will maintain a log of workforce member who have been granted access to information systems with electronic PHI.
4. If a change is needed for job duty fulfillment, the direct supervisor of the workforce member will contact the HIPAA Security Officer or other designated personnel and inform them of the changes needed.
5. The HIPAA Security Officer or other designated personnel will review and approved the changes to access as needed.
6. The access of the employee will be updated to reflect the new job requirements.
7. If an employee is terminated or no longer needs access to the systems with electronic PHI, a request to terminate access will be made to the HIPAA Security Officer or other designated personnel.
8. The HIPAA Security Officer or other designated personnel will assure that the workforce member is removed from the system timely.
9. Documentation will be maintained on the date of termination from the system.
10. On a quarterly basis, the HIPAA security officer or other designated personnel will review all current and active workforce members in the systems with electronic PHI to assure appropriate access to the system.
11. If necessary, the HIPAA Security Officer or other designated personnel will remove all inactive members of the workforce.

Addendum to Information Access

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)

Security Awareness and Training

Security Reminders and Training

Purpose: To insure information regarding HIPAA Privacy and Security is provided to the workforce regularly.

Policy: Derek Hamilton, OD, PA dba Hamilton Eye Associates will ensure that information is provided to all members of the workforce to keep them up and aware of current trends and issues. Each employee is required to understand and comply with all aspects of organization's privacy and security policies and procedures.

Procedure:

1. HIPAA Privacy and Security training for all new hires of Derek Hamilton, OD, PA dba Hamilton Eye Associates will be conducted within 30 days of the start of their employment.
2. All employees will sign a confidentiality form at the commencement of their employment.
3. Training will be conducted on an annual basis for all workforce members of Derek Hamilton, OD, PA dba Hamilton Eye Associates and the focus will be on aspects of the Privacy and Security Policies and Procedures.
4. Documentation of the trainings will be kept in the employee files that Derek Hamilton, OD, PA dba Hamilton Eye Associates maintain.
5. The HIPAA Security will send out updates on HIPAA Privacy and Security on a regular basis and in-between annual trainings. Updates may be done, but are not limited to, verbal discussions, printed materials, e-mails, videos, or other training seminars.
6. Documentation of trainings will be maintained for a minimum of six (6) years.

Addendum to Security Training

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)

Malicious Software Protection

Purpose: To ensure all workstations and servers at Derek Hamilton, OD, PA dba Hamilton Eye Associates operate with the appropriate security measures in place to protect the confidentiality, integrity and accessibility of PHI.

Policy: This policy outlines Organization's process for assuring that all hardware, software, and other network devices are kept up to date with the proper security safeguards. This includes assuring the proper security safeguards are in place to guard again, detect, and report any potential malicious software.

Procedure:

1. Derek Hamilton, OD, PA dba Hamilton Eye Associates shall assure that all hardware, including computers, servers, and other network equipment is kept up to date with patches and security updates as they are released.
2. All attachments to emails that may be received as well as downloads will be scanned for viruses prior to downloading them
3. Regular scans of the systems and firewalls will be conducted to assure no malware or viruses are present in the network.
4. All hardware being plugged into the Organization's network system will be tested by the HIPAA Security Officer or other designated personnel prior to installing to assure that no inappropriate and/or harmful software is on the hardware that could cause risks and vulnerabilities to the network system.
5. All employees of Derek Hamilton, OD, PA dba Hamilton Eye Associates will be trained on viruses and malware and will report any concerns to the HIPAA Security Officer or other designated personnel immediately.

Addendum to Malicious Software

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)

Log in Monitoring

Purpose: To ensure appropriate measures are implemented to verify access to systems with PHI is appropriate and report any areas of concern and discrepancies to the HIPAA Security Officer or other designated personnel.

Policy: Derek Hamilton, OD, PA dba Hamilton Eye Associates will evaluate and monitor log-in attempts and documented log-in discrepancies.

Procedure:

1. An audit trail of failed log-ins will be generated and reviewed on a regular basis by the HIPAA Security Officer or other designated personnel.
2. Any concerns with the failed log-ins will be investigated and evaluated by the HIPAA Security Officer or other designated personnel.
3. All workforce members who fail a log-in attempt a minimum of three (3) and a maximum of five (5) times will be locked out of the system and will need to contact the HIPAA Security Officer or designated individual(s) to reset the password.
4. Any other suspicious log in activity will be reviewed by the HIPAA Security Officer or other designated personnel.

Addendum to Log in Monitoring

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)

Password Management

Purpose: Derek Hamilton, OD, PA dba Hamilton Eye Associates will ensure that each workforce member uses proper password set up and safeguards.

Policy: All workforce members of Derek Hamilton, OD, PA dba Hamilton Eye Associates will be required to follow the password guidelines to assure that adequate safeguards are made with protecting patient information. All workforce members are solely responsible for the protection and safeguards of passwords.

Procedure:

1. Employees will be given a temporary password on initial log in to the system, which needs to be changed after the initial log in.
2. All passwords will be created using a minimum of two (2) of the following security features; however, it is recommended that three (3) out of four (4) are used.
    1. Upper case letter;
    2. Lower case letter;
    3. Number;
    4. Symbol;
3. Passwords must be a minimum of six (6) characters in length.
4. Old passwords will not be able to be reused for a minimum of the last five (5) attempts.
5. Passwords will expire every 180 days.
6. Employees are not allowed to write down passwords, share passwords, or any other action that may compromise the security of their password.

Addendum to Password Management

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)

Security Incident

Purpose: Derek Hamilton, OD, PA dba Hamilton Eye Associates will investigate any potential security risks identified to the organization.

Policy: Derek Hamilton, OD, PA dba Hamilton Eye Associates will identify and respond to any security incidents that the have been identified through the work of the organization. Each security risk will be investigated, mitigated, and documented appropriately. If needed, proper notification will happen in accordance with the Breach Notification Policy and Procedure.

Procedure:

1. The HIPAA Security Officer or other designated personnel will be the person responsible for leading all responses to security incidents within the organization.
2. Security incidents or potential incidents will be reported to the HIPAA Security Officer or other designated personnel as soon as they are known to anyone within the organization.
3. The HIPAA Security Officer or other designated personnel will lead the investigation into the security incidents or potential security incidents.
4. Periodic evaluation and monitoring of any user activity, failed log in attempts, virus scans, audit trails, and firewall functionality will be complete.
5. Once alerted to a potential security incident, the incident will be immediately investigated.
6. Immediate and reasonable steps to be taken to address the identified issue. The incident will be resolved as soon as possible.
7. If the issue is causing major disruptions or risks, components of the contingency plan will be implemented and communicated to all staff.
8. Once the incident is fully resolved, it will be properly communicated throughout the organization.
9. If during the investigation, it is determined that a security incident has not happened, it will just be documented.
10. All information will be immediately documented and will include at a minimum the security incidents, date notified, investigation notes and findings, mitigations, and any education that was done.

Addendum to Security Incident

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)

Facility Access Controls

Facility Access Controls

Purpose: Derek Hamilton, OD, PA dba Hamilton Eye Associates will ensure proper facility access controls are implemented.

Policy: Derek Hamilton, OD, PA dba Hamilton Eye Associates will implement policies and procedures to assure limited physical access to the facility (facilities) and electronic information systems such as servers, routers, computers, and other hardware. Proper access controls will be put in place to assure that only the authorized individuals will access the electronic information systems:

Procedure:

1. Derek Hamilton, OD, PA dba Hamilton Eye Associates will evaluate the physical security of the organization and identify areas where access controls need to be implemented.
2. All areas that contain protected hardware such as servers and routers will be properly secured with limited individuals that have access.
3. Facility access controls will be regularly evaluated and updated as necessary.

Addendum to Facility Access Controls

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)

Contingency Operations

Purpose: Derek Hamilton, OD, PA dba Hamilton Eye Associateswill ensure that contingency operations are defined to maintain the confidentiality, integrity, and accessibility of health information.

Policy: Derek Hamilton, OD, PA dba Hamilton Eye Associateswill establish and implement, as necessary, policies and procedures that allow the facility access to PHI in the event of an emergency. In the event of a disaster or emergency, proper personnel will be used to monitor and restrict access to the facilities where PHI is stored.

Procedure:

1. In the event of an emergency, Derek Hamilton, OD, PA dba Hamilton Eye Associates will implement contingency operations to maintain proper business support and patient care.
2. Operations will be based on the defined contingency plan, which includes disaster recovery and emergency mode operations.
3. The contingency operations will be evaluated regularly for needed updates.

6c. Facility Security Plan and Access Control and Validation - 164.310(a) (2) (ii) & 164.310(a) (2) (iii)

Purpose: Derek Hamilton, OD, PA dba Hamilton Eye Associates will ensure proper steps are taken to assure security in the facility or facilities hosting PHI.

Policy: Derek Hamilton, OD, PA dba Hamilton Eye Associates will implement necessary policies and procedures to assist in safeguarding any hardware or software that contains PHI, in all media formats. Derek Hamilton, OD, PA dba Hamilton Eye Associates will be responsible for assuring that all hardware and software that contains PHI will be free from unauthorized access, tampering, and theft.

Procedure:

1. All staff members are responsible for assisting and helping with the safeguards of PHI.
2. Only the individuals that need access to restricted areas will be granted access, and a limited number of keys or access badges will be provided. To be granted access to these areas, staff members must go through proper training and sign off understanding the safeguard requirements.
3. If a key or access badge is lost, it must immediately be reported to the HIPAA Security Officer or other designated personnel.
4. All employees will be responsible for a safe and secure workplace by doing such items as logging off the system when leaving the computer, assuring that faxes and prints are promptly retrieved from the fax machine, do not write down user names and passwords, and all other safeguards that may be implemented.
5. Non-employees will not be allowed in areas where PHI is maintained unless it is for patient care and they are escorted by a staff member.
6. If maintenance is required in an area with PHI, it will take place during business hours with a staff member present in the area.
7. Regular education will be provided to help assure that proper security safeguards are in place.

Addendum to Contingency Operations

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)

Maintenance Records

Purpose: Derek Hamilton, OD, PA dba Hamilton Eye Associates will maintain records of any maintenance that occurs in areas where PHI is present.

Policy: Derek Hamilton, OD, PA dba Hamilton Eye Associates will implement adequate policies and procedures to assure that all changes, which includes but is not limited to modifications, repairs, and updates to the physical location of an area containing PHI will be documented adequately.

Procedure:

1. Documentation of any altering to physical locations containing PHI will be documented in the maintenance log immediately after the alterations take place.
2. The logs will be maintained for six (6) years.
3. The HIPAA Security Officer or other designated personnel will be responsible for maintaining the maintenance records for the entire facility in conjunction with the proper individual responsible for the physical plant.

Addendum to Maintenance Records

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)

Workstation Use and Security

Purpose: Derek Hamilton, OD, PA dba Hamilton Eye Associates will be responsible for assure proper workstation use and workstation security to all equipment owned by the company.

Policy: Derek Hamilton, OD, PA dba Hamilton Eye Associates will implement policies and procedures that assure proper functions to be performed, the way the functions are performs, and the proper attributes of the surrounding of a specific workstation for use and security purposes. All workforce of Derek Hamilton, OD, PA dba Hamilton Eye Associates will be granted access and use of the workstations and will be trained on the requirements of proper use and security. The proper use and security is described in this policy.

Procedure:

1. Organization’s owned hardware will only be used for business purposes related to the business operations.
2. Every user must log onto the computer using the credential provided to them by the company.
3. When leaving a computer, all users are required to log out of the system to protect the information in the EHR and on the computer's drive.
4. When left idle, all computers in the active directly will implement a screen saver after a minimum of two (2) and a maximum of five (5) minutes.
5. Doors leading into offices with computers (desktops or laptops) are adequately secured.
6. All removal or change in hardware, software, and other media will require a receipt of removal of hardware.
7. If an issue arises or potential virus is detected, workforce will report the incident immediately.
8. No software will be downloaded onto the computer without proper permissions.
9. No outside portable media will be inserted into the computer without prior evaluation.
10. Workstations are unable to be moved without prior approval.
11. Any theft or loss of a workstation will immediately be reported to the HIPAA Security Officer or other designated personnel.
12. Adequate training will take place to ensure protection and proper use.

Addendum to Worstation Use

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)

Device and Media Controls

Electronic Media Disposal and Re-Use

Purpose: Derek Hamilton, OD, PA dba Hamilton Eye Associates will ensure the appropriateness of disposal and reuse of all media devices that deal with PHI.

Policy: Derek Hamilton, OD, PA dba Hamilton Eye Associates will implement policies and procedures to adequately dispose of and re-use any media that encounters PHI. This could include, but is not limited to, computers, servers, USB drives, copy machines, faxes, paper, external hard drives, and all other media.

Procedure:

- When media that encounters PHI is ready to be disposed of or re-deployed, the proper steps will be taken to remove the all PHI from media devices (see below).
- The following table describes the media and the proper steps for re-use or destruction of the media and the individual responsible.
- The HIPAA Security Officer or other designated personnel is responsible for ensuring the proper disposal and reuse of the media.
- A log will be kept and maintained that will include the following information:
  - Medium type;
  - Model name/serial number;
  - Date received;
  - Date moved;
  - Date destroyed;
  - Department/location assigned to;
  - Department/location moved to;
  - Final disposal location;
  - Approval party;
- Logs will be maintained for six (6) years.

Addendum to Device and Media

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)

Media Type	Responsible Party	Media Disposal Process	Media Re-Use Process
Computers/Laptops	HIPAA Security Officer	Computers and laptops will be destroyed by an authorized computer destruction service. A certificate of destruction will be obtained for each computer or laptop. Certificates will be maintained for six years.	The computer or laptop will not be re-used.
Paper	HIPAA Security Officer	Paper will be cross-shredded and properly disposed of or will be destroyed by a HIPAA compliant confidential service. A BAA must be on file.	Once shredded this is not applicable.
External Hard Drive	HIPAA Security Officer	External hard drives will be destroyed by an authorized computer destruction service. A certificate of destruction will be obtained for each computer or lap top. Certificates will be maintained for six years.	The external hard drive will not be re-used.
Media Type	Responsible Party	Media Disposal Process	Media Re-Use Process

USB/Flash Drive	HIPAA Security Officer	USB/flash drives will be destroyed by an authorized computer destruction service. A certificate of destruction will be obtained for each USB/flash drive. Certificates will be maintained for six years.	The USB or flash drive will not be re-sued.
Server	HIPAA Security Officer	The server will be cleared of all information, including protected health information, by an authorized company. A certificate of clearing of data will be obtained for each server. Certificates will be maintained for six years.	The server will not be re-used.
Copy Machines/ Multifunction Printer (MFP)	HIPAA Security Officer	Hard drives will be removed from all MFPs prior to replacement of the machine. The hard drive will be destroyed by an authorized computer destruction service. A certificate of destruction will be obtained for each MFP hard drive. Certificates will be maintained for six years.	Once the hard drive has been replaced the machine may be sold or leased to another customer.

Data Back-up and Storage

Derek Hamilton, OD, PA dba Hamilton Eye Associates will ensure electronic patient data is backed up on a regularly scheduled basis to prevent an inadvertent loss of information. This will include all diagnostic equipment in which patient information is stored. Backups may be performed remotely or locally. Derek Hamilton, OD, PA dba Hamilton Eye Associates will ensure the security of backed up data. Local back-ups will be stored in a secure location off-site (recommended) or, at a minimum, in a locked, fireproof container located within the Practice. Data included in the back-ups should be periodically reviewed to ensure data is not corrupted or missing.

Addendum to Data Back-up and Storage

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)

Access Control (Password)

Unique user identification

Purpose: Derek Hamilton, OD, PA dba Hamilton Eye Associates will ensure access to protected health information can be monitored via unique password assignments.

Policy: Derek Hamilton, OD, PA dba Hamilton Eye Associates will assign a unique username for each workforce member who has electronic access to protected health information.

Procedure:

- When a workforce member has been approved for access to protected health information a unique username will be assigned for identifying and tracking user identity.
- Passwords will remain confidential and will not be shared with any other user under any circumstances.
- In the event a user feels their password has been compromised, it will be immediately changed.
- The HIPAA Security Officer or other designated personnel will be responsible for managing and monitoring electronic access to PHI.

Addendum to Access Control (Password)

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC

Auto Log-Off

Purpose: Derek Hamilton, OD, PA dba Hamilton Eye Associates will ensure that the system automatically logs off when idle for a specified amount of time. Auto log off is an effective way to prevent unauthorized access to electronic protected health information.

Policy: Derek Hamilton, OD, PA dba Hamilton Eye Associates will implement electronic solutions that will terminate an electronic session after a predetermined time of inactivity.

Procedure:

- Systems will be automatically set to auto log off after a predetermined time of inactivity.
- All systems will be consistent with the time of inactivity.

It is the expectation of staff to log off or lock all unattended workstations.

Addendum to Auto Log-off

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)

Audit Control

Purpose: Derek Hamilton, OD, PA dba Hamilton Eye Associates will implement mechanisms that record and examine ePHI activity.

Policy: Derek Hamilton, OD, PA dba Hamilton Eye Associates will implement appropriate control mechanisms to ensure appropriate access and use of ePHI.

Procedure: Derek Hamilton, OD, PA dba Hamilton Eye Associates will review the following logs on a regular basis. Documentation of the review of logs will be maintained for six (6) years.

- Firewall logs for the server;
- Server logs for access by users and administrators;
- Logs for all software containing electronic PHI, which may include but is not limited to practice management software, electronic medical record software, transcription software, imaging system software, and other required software;
- Logs of any other hardware, software, or other medium that contain electronic PHI;

If issues or concerns are detected additional research will be done. The Security Officer or other designated personnel is responsible for ensuring this policy is followed.

Addendum to Audit Control

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)

Integrity

Purpose: Derek Hamilton, OD, PA dba Hamilton Eye Associates will take appropriate measures to PHI information from improper alteration or destruction.

Policy: Derek Hamilton, OD, PA dba Hamilton Eye Associates will implement mechanisms and safeguards to ensure that PHI has not been altered or destroyed in an unauthorized manner. All workforce members will be responsible for the protection and safeguarding of PHI.

Procedure:

- Derek Hamilton, OD, PA dba Hamilton Eye Associates will use and adopt mechanisms such as RAID disk arrays, HL7 standards, and/or error correcting memory to protect data from alteration or being destroyed erroneously.
- For data integrity during transmission, security measures will be taken such as encryption or HTTPS to ensure that PHI is not altered or destroyed erroneously.
- All server communication will be kept in a controlled internal environment.
- Reports from applications will be reviewed on a regular basis to ensure data integrity and verify changes where legitimate.
- No PHI will be stored on the local drive on the computers by staff. All PHI will reside within the server files or EHR database to ensure integrity.
- Electronic health records will only be accessed by a username and password. All information is directly linked to the specific user.
- Any deletion of information in the HER may be reviewed to ensure the change was legitimate.

Addendum to Integrity

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)

Person or Entity Authentication

Purpose: Derek Hamilton, OD, PA dba Hamilton Eye Associates will implement procedures to verify that a person or entity seeking access to PHI is the one claimed.

Policy: The following measures are in place to ensure only authorized persons are accessing protected health information:

Procedure:

- Unique user passwords are required for access to workstation, system network, or software application that contains protected health information.
- User will not share or use other usernames and passwords to access PHI.
- Users will not access PHI for another person.
- When PHI is requested, Derek Hamilton, OD, PA dba Hamilton Eye Associates will take precautionary steps to verify the requestor is who they are state that they are.
- Regular education will be held to discuss the important or verification of identity and protection or username and passwords.

Addendum to Authentication

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)

Transmission Security

Integrity Controls

Purpose: Derek Hamilton, OD, PA dba Hamilton Eye Associates will implement necessary safeguards to guard against unauthorized access to protected health information that is being transmitted over an electronic communications network.

Policy: Derek Hamilton, OD, PA dba Hamilton Eye Associates will implement the following measures to ensure the security of transmitted PHI:

Procedure:

1. All information being transferred by removal hardware (CDROM, USB Drive, disks, etc.) will have a minimum safeguard of passwords in place. For adequate protection, the removal hardware may be encrypted.
2. Prior to sending electronic PHI, staff will verify the receiver's information to ensure the PHI is sent to the correct person/entity.
3. All transfers of information will follow the minimum necessary policy.
4. Electronic PHI received by Derek Hamilton, OD, PA dba Hamilton Eye Associates will be secured in the patient record or other designated area as soon as possible after receipt.
5. Staff of Derek Hamilton, OD, PA dba Hamilton Eye Associates are educated on this process.

Addendum to Tramsmission Security

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)

Encryption

Purpose: Derek Hamilton, OD, PA dba Hamilton Eye Associates will review the need to encryption on a regular basis and for all newly purchased computer equipment.

Policy: To ensure the highest security for Derek Hamilton, OD, PA dba Hamilton Eye Associates's protected health information, the Practice will:

Procedure:

- Derek Hamilton, OD, PA dba Hamilton Eye Associates will consider the use of encryption for transmitting EPHI, particularly over the Internet. As business practices and technology change, situations may arise where EPHI being transmitted from a covered entity would be at significant risk of being accessed by unauthorized entities.
- Encryption will be considered for all workstations, laptops, iPad and other electronic devices housing PHI
- A listing of encrypted devices can be found in Derek Hamilton, OD, PA dba Hamilton Eye Associates Specific Notes area below.

Addendum to Encryption

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)

Organizational Reminders

To ensure ongoing compliance and HIPPA security:

- The HIPAA Security officer or other designated personnel will perform a review of all physical and technical safeguards on a regular basis.
  - The review may consist of, but is not limited to security incidents, data breaches, policies and procedure, review, observation of the workplace and workforce members, and other activities that may be fit.
- Derek Hamilton, OD, PA dba Hamilton Eye Associates will:
  - Create policies and procedure in accordance with state and federal privacy and security requirements.
  - Update all privacy and security policies and procedures as needed within the organization.
  - Ensure adequate access to all privacy and security policies and procedures to all workforce members.
  - Ensure that impacted individuals are properly informed of all updates
  - Review policies and procedures on a minimum of a bi-annual basis, or as regulations change. If there are any major changes in administrative, physical or technical aspects of the company, privacy and security policies and procedures will be reviewed.
  - Maintain all documentation regarding privacy and security policies and procedures for six (6) years post the last day it was active or used.

Addendum to Organizational Reminders

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)

Breach Notification

Purpose: Derek Hamilton, OD, PA dba Hamilton Eye Associates will ensure that all reported unauthorized use of PHI are researched in a timely and compliant manner no later than 60 days following discovery of the breach. Unauthorized uses of PHI will be presumed a breach until it is determined otherwise.

Policy: Derek Hamilton, OD, PA dba Hamilton Eye Associates will assure that breach notification will be carried out in compliance with all state and federal guidelines including, providing notice, as indicated by the findings in the breach risk assessment. Notices will be sent to:

- Individuals
- Media if required
- Federal and State governments as required by law

Procedure: Upon notification of a potential breach, the following steps will be implemented:

Discovery:

  - A breach of PHI will be deemed “discovered” as of the first day Derek Hamilton, OD, PA dba Hamilton Eye Associates is notified regarding the potential breach. This excludes the person committing the breach.
  - The investigation is time sensitive and must be immediately reported to start the investigation in a timely fashion.

Investigation:

  - Upon receipt of notification the potential breach will promptly be investigated.
  - The investigation will include interviewing individuals involved, collecting written documentation, and completing all appropriate documentation.
  - If the breach falls into one of the three listed exceptions, it will be documented, and the investigation will be concluded. Exceptions include:

- Unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or business associate.
- Inadvertent disclosure of protected health information by a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the covered entity or business associate, or organized health care arrangement in which the covered entity participates.
- The covered entity or business associate has a good faith belief that the unauthorized person to whom the impermissible disclosure was made, would not have been able to retain the information.

  - A breach risk assessment will be completed for each investigation. This assessment will include:

    - The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
    - The unauthorized person who used the PHI or to the disclosure was made;
    - Whether the PHI was acquired or viewed; and 4. The extent to which the risk to the PHI has been mitigated.

- All documentation related to potential breach investigations will be retained for a minimum of six years.

Notification:

Notice to Individual(s): Notice will be provided promptly and in the following form:

- Written notification by first-class mail to the individual at the last known address of the individual. The notification will be provided in one or more mailings as information is available. If Derek Hamilton, OD, PA dba Hamilton Eye Associates knows that the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification by first-class mail to the next of kin or person representative will be carried out.
- Substitute Notice: In the case where there is insufficient or out-of-date contact information (including a phone number, email address, etc.) that precludes direct written or electronic notification, a substitute form of notice reasonably calculated to reach the individual will be provided. A substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative.
- In a case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, then the substitute notice may be provided by an alternative form of written notice, telephone, or other means.
- In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then the substitute notice will be in the form of a conspicuous notice in a major print or broadcast media in Derek Hamilton, OD, PA dba Hamilton Eye Associates's geographic area where the individuals affected by the breach likely reside. The notice will include a toll-free number that remains active or at least 90 days where an individual can learn whether his or her PHI may be included in the breach.
- If Derek Hamilton, OD, PA dba Hamilton Eye Associates determines that notification requires urgency because of possible imminent misuse of unsecured PHI, notification may be provided by telephone or other means, as appropriate in addition to the methods noted above.
    - Notification to media - Notice will be provided to prominent media outlets serving the state and regional area when the breach of unsecured PHI affects 500 or more patients. The Notice will be provided in the form of a press release.
    - Notification to the Secretary of the Department of Health and Human Resource (DHHS) Notice will be provided to the Secretary of HHS as follows below. The Secretary will make available to the public on the HHS Internet website a list identifying covered entities involved in all breaches in which the unsecured PHI of more than 500 patients is accessed, acquired, used, or disclosed.
        - For breaches involving 500 or more individuals, the organization will notify the Secretary of HHS as instructed at www.hhs.gov at the same time notice is made to the individuals.
        - For breaches involving less than 500 individuals, the organization will maintain a log of the breaches and annually submit the log to the Secretary of HHS during the year involved (logged breaches occurring during the preceding calendar year to be submitted no later than 60 days after the end of the calendar year). Instructions for submitting the log are provided at www.hhs.gov.
- Derek Hamilton, OD, PA dba Hamilton Eye Associates will verify state specific breach notification requirements.
- Content of the notice: The substance of the notice should be written in clear, concise, and easy-to-

understand language. The notice should avoid the use of technical jargon and include, at a minimum, the following elements:

  - A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
  - A description of the types of unsecured PHI that were involved in the breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
  - Steps the individual should take to protect themselves from potential harm resulting from the breach;
  - A brief description of what the organization is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches;
  - Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, website, or postal address;

- Additional content areas may include:
  - Information about steps the covered entity is taking to retrieve the breached information such as filing a police report (if a suspected theft of unsecured PHI occurred);
    - Recommendations that the individual contact his or her credit card company and information about how to contact the credit bureaus and obtain credit monitoring services (if credit card information was breached);
    - Information about steps the covered entity is taking to improve security to prevent future similar breaches;
    - Information about sanctions the covered entity imposed on workforce members involved in the breach;

- Maintenance of Breach Information Log – As described above and in addition to the reports created for each incident, Derek Hamilton, OD, PA dba Hamilton Eye Associates will maintain a process to record or log all potential breaches and breaches of unsecured PHI regardless of the number of patients affected.

The following information should be collected/logged for each breach:

- Date of Discovery;
- Date(s) of breach/potential breach;
- Breach exceptions that apply;
- Approximate number of individuals impacted;
- Type of Breach (theft, loss, hacking, employee issue);
- Location of Breach (paper, phone, electronic)
- Type of Information Involved;
- Summary of the Breach;
- Safeguards in Place Prior to Breach (firewalls, passwords)
- Date(s) Notice Provided to impacted individual(s) & Types of notices
- Actions taken in response to breach.

This policy and procedure will be regularly reviewed.

Addendum to Breach Notification

(Any information contained in this addendum is content provided solely by the client and not that of

Compliance Specialists, LLC)

Contingency Plan

(Place practice Contingency Plan in this section)

Additional Addendum to Policy IV

Policy V

Auditing, Benchmarking and

Monitoring of Charts and Claims

Monitoring and Auditing

Monitoring and Internal Audits

The Compliance Officer or other designated personnel will periodically review Derek Hamilton, OD, PA dba Hamilton Eye Associates's procedures to determine if the Practice is utilizing the complete and most current information contained in the government regulations. The Compliance Officer or other designated personnel will at least quarterly verify that there have not been changes in the Current Procedural Terminology (CPT) and ICD-10-CM Codes. In the event of a change in codes or procedures, the Compliance Officer or other designated personnel shall maintain an archival copy of the former codes under the Practice's records retention plan.

Internal monitoring may include, but is not limited to:

- Review of submitted claims
- Review of claims prior to submission
- Review of provider documentation

The internal audits are conducted to determine:

1. Whether charges for services are consistent with services delivered regardless of who is paying the bill;
2. Whether bills are accurately coded and reflect the services provided;
3. That the documentation in the medical record supports the coding;
4. That the documentation is completed correctly;
5. That the documentation explains why the services or items provided were reasonable and necessary for the patient;
6. Verification that no incentives existed for unnecessary services.

Procedures for Corrective Action

In the event a periodic audit, or a review of claim rejections indicates that an overpayment has been received, the Compliance Officer or other designated personnel will immediately internally report the findings and determine additional steps needed. When appropriate, the Compliance Officer or other designated personnel will follow CMS/OIG written guidance to arrange repayment or other financial adjustments as appropriate. In the event the matter is of greater significance, the Compliance Officer or other designated personnel will contact legal counsel for the Practice.

Addendum to Policy V

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)

Policy VI

Training and Education

Derek Hamilton, OD, PA dba Hamilton Eye Associates is responsible for the training of its workforce:

Workforce includes:

- Qualified Health Care Professionals (QHCP);
- All W2 employees;
- Students (all kinds);
- Volunteers;
- Any independent contractor working on-site, under your direct control that [Organization] has not treated as a business associate.

Training may be in many forms:

- Live lectures;
- Purchased on-line training modules;
- Review of policies/procedures;
- Workbooks;
- Other methods devised by the Practice

- Training will be job specific.
- All existing workforce members will receive ongoing training.
- Any new workforce member must be trained within a reasonable time after joining and will receive ongoing training.
- All members must be trained within a reasonable time after any change in policy or procedures affecting all health care laws and regulations.

Training and Education

Derek Hamilton, OD, PA dba Hamilton Eye Associates believes that it is important for all employees to participate in ongoing training programs including training related to compliance.

Initial Compliance Training

In conjunction with the Compliance Officer or other designated personnel and/or Practice leadership, all employees will be trained concerning the commitment of the Practice to compliance, including the importance of compliance, the role of each employee in compliance, and consequences for violating standards and procedures.

All employees hired subsequent to the initial training program will go through an individualized training program with the focus on the importance of compliance within the first thirty (30) days of employment. The Compliance Officer or other designated personnel will conduct annual compliance training for all employees, as well as other trainings as may be necessary or appropriate.

Training courses may be conducted in house or may be offered by outside sponsors or through online training programs such as those offered by CMS MedLearn Matters, the OIG's HEAT videos, and/or Medicare Contractors. Upon completion of web-based training, the certificate of completion should be recorded on the education log.

All staff will complete:

- Fraud, Waste and Abuse
- HIPAA and Compliance Overview
- Cybersecurity
- Cultural Awareness

Training specific to one’s job duties will be determined by the Practice.

Corrective Action

The goal of this Compliance Program is to have zero errors, however if an occasional human mistake may occur. In the event there is suspected non-compliance discovered by any employee, the employee should immediately report the discovery to the Compliance Officer or other designated personnel. As soon as possible, the Compliance Officer or other designated personnel will investigate the error and take the following actions as appropriate:

- Verify whether an error has occurred on behalf of the Practice or another party;
- Log the error in a log book identifying the date, description and the person noting the entry;
- Correct and note the error in the log book identifying what corrective action was taken;
- Other actions necessary to gain compliance.

Refunds to government and other insurance programs will be completed in a timely manner.

Addendum to Policy VI

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)

Policy VII

Communication and Compliance Reporting

Reporting Guidelines

All employees are responsible for monitoring and reporting concerns that may arise. If an employee should become aware of an error (i.e. billing, documentation, fraud or any other suspected violation) the employee must immediately report those concerns to his supervisor. If the employee is uncomfortable with reporting a concern to his supervisor or if his supervisor is unresponsive towards the concern, the employee may report the concern to the Compliance Officer or other designated personnel. If the employee desires, reports can also be submitted anonymously or to Derek Hamilton, OD, PA dba Hamilton Eye Associates's legal counsel as indicated below. At the time a concern is brought forward appropriate research will be done to determine if a compliance or HIPAA violation exists.

If the concern involves a Business Associate appropriate research will be completed to determine the extent, of any, of the violation.

An employee may anonymously report concerns to legal counsel for Derek Hamilton, OD, PA dba Hamilton Eye Associates. Employees may contact:

0

Whistleblower Protection

Errors or violations which are reported in good faith with a sincere belief that the conduct is erroneous or potentially fraudulent will result in no retribution or adverse job action to the employee making the report. Under no circumstances will the good faith reporting of any concerns or possible impropriety serve as a basis for any retaliatory action(s) against any employee reporting such concerns.

Addendum to Compliance Reporting

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)

Handling Patient Complaints about Privacy Violations

It is the policy of Derek Hamilton, OD, PA dba Hamilton Eye Associates to accept, investigate and resolve to the best of our ability complaints from patients who believe that their privacy was not properly protected.

Complaints must be in writing and will be handled by the Public Information Officer or other designated personnel. If a complaint comes over the telephone, the PIO will inform the patient to send it in writing. Concerns can be submitted via hard copy or electronic, as the patient wishes. If a patient wishes to remain anonymous, we will accommodate that to the extent practical.

- The Public Information Office will keep all patient complaints for at least six (6) years. These will be stored, along with information about the investigation and resolution of the complaint.
- Upon receiving a patient complaint about privacy, the Public Information Officer or other designated personnel will investigate. The Public Information Office or other designated personnel has discretion to conduct the investigation in the manner considered reasonable and logical based on the nature of the complaint. Generally, a complaint investigation includes:
  - Discussion with the person in the office whom the patient believes violated their privacy
  - Review the patient's clinical chart (as needed)
  - Discussion with other staff who may have knowledge of the patient and/or complaint
  - Discussion with the patient
  - Review of any information or evidence that the patient presents in support of the perceived privacy violation
- Based upon the results of the investigation, the Public Information Officer or other designated personnel will determine if the patient's complaint is substantiated or not. If the complaint is not substantiated, the Public Information Officer or other designated personnel will notify the patient in writing. If it is substantiated, the Public Information Officer or other designated personnel will determine what steps are necessary to resolve the issue so that it does not recur.
- In determining what steps are necessary to resolve a substantiated complaint of a violation of privacy, the Public Information Officer or other designated personnel will generally consider:
  - Review the cause of the violation
  - If the violation was caused by a failure to comply with existing policy, the Public Information Officer or other designated personnel will report the issue for formal disciplinary action (see Sanctions)
  - If the problem was caused by a lack of an appropriate policy, or an inadequate policy, the Public Information Officer or other designated personnel will consult with the Privacy Officer or other designated personnel to determine how the policy should be changed, or developed
  - If a Business Associate was involved in the violation, a procedure to ensure the issue will not recur will be required. In the event this cannot be provided the Business Associate contract will be considered for termination.
  - If the privacy violation caused harm the Public Information Officer or other designated personnel will consult with the Privacy Officer or other designated personnel to outline the steps toward resolution. Other Derek Hamilton, OD, PA dba Hamilton Eye Associates leaders will be asked to intervene as needed.
- Once a resolution of a complaint is determined, the Public Information Officer and the Privacy Officer or other designated personnel will work cooperatively to take the steps identified as necessary for the resolution.
- If new policies or procedures are put into place as part of the resolution, the Privacy Officer or other designated personnel will conduct mandatory training for our workforce regarding them.

- The Public Information Officer or other designated personnel will develop monitoring to ensure the resolution is working to improve our privacy protections. The Public Information Officer or other designated personnel will report to the Privacy Officer or other designated personnel on the results of the monitoring. If the PIO discovers continued problems through monitoring, the Public Information Officer and the Privacy Officer or other designated personnel will work cooperatively to resolve the issue(s).
- All documentation will be kept In the H drive on the server.

Addendum to Patient Complaints

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)

Mitigation of Known Harm Due to an Improper Disclosure of PHI

It is the policy of Derek Hamilton, OD, PA dba Hamilton Eye Associates to mitigate known harm from an improper disclosure of PHI, when it is practicable to do so.

- Reasonable steps will be taken to mitigate harm due to an unauthorized disclosure of PHI by [Organization]'s staff or business associated.
- The Privacy Officer and Public Information Officer or other designated personnel will determine what specific steps are appropriate on a case by case basis as it is our policy to determine mitigation based on the individual situation. Examples of mitigation may include:
  - Getting back PHI that was improperly disclosed
  - Preventing further disclosure through agreements with the recipient
- Derek Hamilton, OD, PA dba Hamilton Eye Associates does not consider money reparations to be appropriate mitigation.
- If a Business Associate has made the improper disclosure, the Business Associate will be required to cure the problem to our satisfaction, or the Business Associate contract may be terminated.

Addendum to Improper Disclosure of PHI

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)

Policy VIII

Enforcement Employment and Employee Discipline

Hiring and Background Checks

On an annual basis, Derek Hamilton, OD, PA dba Hamilton Eye Associates or a designated vendor/contractor will verify that its employees are not excluded from participation in government reimbursement programs. (https://exclusions.oig.hhs.gov).

The following steps will be taken prior to hiring any individual:

- The applicant must complete an application which includes signatures, dates and references
- The applicant must produce a valid driver's license and social security card
- The Compliance Officer or other designated personnel will verify that the person is not included on the OIG's Cumulative Sanctions Report (https://exclusions.oig.hhs.gov)
- Derek Hamilton, OD, PA dba Hamilton Eye Associates will verify the applicant's references
- Derek Hamilton, OD, PA dba Hamilton Eye Associates will provide an overview of the Compliance Program Manual and indicate that compliance with this procedure is an ongoing condition of employment

Addendum to Hiring

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)

Ongoing Training

As noted above, all employees of [Organization] will be required to participate in training and continued education concerning compliance issues.

Addendum to Training

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)

Disciplinary Action

Derek Hamilton, OD, PA dba Hamilton Eye Associates is committed to full and complete compliance with the law, including the terms of this compliance plan. Any illegal or unethical conduct by any employee will result in immediate and appropriate disciplinary action, including the potential for termination of employment. Beyond employment termination, however, Derek Hamilton, OD, PA dba

Hamilton Eye Associates may in appropriate circumstances refer former employees to appropriate authorities for criminal prosecution and seek restitution of damages if applicable. All employees remain "at will" employees.

Addendum to Disciplinary Action

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)

Policy IX

Outside Inquiry

In the event any employee of Derek Hamilton, OD, PA dba Hamilton Eye Associates is contacted by any outside agency or payer concerning an audit, the employee must immediately notify the Compliance Officer or other designated party.

The Compliance Officer or other designated personnel will use the following procedure in the event of such inquiries:

- If the inquiry is in writing, the Compliance Officer or other designated personnel will immediately advise legal counsel of the inquiry. The Compliance Officer or other designated personnel will review any requested information and confer with legal counsel prior to any response;
- If the visit is in person, the Compliance Officer or other designated personnel will take the following steps:
  - Verify the identity of the government agency;
  - Determine the exact nature of the inquiry of the agent;
  - Determine that any requested documents will be reviewed by the Compliance Officer or other designated personnel and legal counsel prior to or at the time of release to the agent.

To avoid any confusion or misunderstanding all communication will be handled by the Compliance Officer or other designated personnel. No other employee should have discussions or release information without the prior consent of Compliance Officer or other designated personnel or legal counsel. Once it is determined what staff, if any, will be needed for the inquiry they will be notified by the Compliance Officer or other designated personnel.

Unscheduled On-site Visit by DME NSC Representative

42 CFR section 424.57(e) requires the National Supplier Clearinghouse (NSC) to revalidate suppliers every three (3) years. The NSC, acting for the Centers for Medicare & Medicaid Services (CMS), is the central entity responsible for maintaining supplier identification and ownership data, as well as other business data. Part of that responsibility requires the NSC to share this information with the Durable Medical Equipment Medicare Administrative Contractors (DME MACs) for provider relations and claims processing.

Therefore, it is imperative the NSC have the most accurate information on file. Further, the revalidation process also allows the NSC to determine if the supplier is in compliance with the supplier standards. Suppliers may revalidate via Internet-based PECOS or by downloading a CMS855S enrollment application.

The revalidation process includes a site visit, if required. Also, workload and the time spent requesting any additional information required to complete the revalidation play a part in determining the processing time. Be sure to respond to requests for information from the NSC timely to avoid having your supplier number deactivated and having to begin the process again.

An authorized site inspector, whether an NSC employee or a contractor, will have a photo

identification card and a signed letter on CMS letterhead authorizing the individual to conduct the visit with them. Please note, the inspector will have a camera to take various pictures of the facility, sign, inventory, etc. The inspector will also have a questionnaire to complete based on the supplier standards.

The inspector will ask to review your files to determine if you are in compliance with certain requirements of the supplier standards. However, the site inspector should not take the files, make copies or take pictures of the information contained in the files.

Please notify the NSC immediately if the site inspector requests to take the original or make copies of the beneficiary files, fails to present the photo ID or fails to present the signed authorization letter. You should not give any information to an individual that is not properly credentialed. Please call (866) 238-9652 to report any concerns.

Addendum to Policy IX

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)

Policy X

Electronic Health Records and Health Information Exchange

Purpose

The purpose of this policy is to identify the health record for business and legal purposes during and after the transition to electronic health records and to ensure that the integrity of health records is maintained so that it can support business and legal needs.

Scope

This policy applies to all uses and disclosures of the health record for administrative, business or evidentiary purposes. It encompasses records that may be kept in a variety of media including, but not limited to, electronic, paper, digital images, video and audio. It excludes those health records not normally made and kept in the regular course of the business.

Policy

It is the policy of Derek Hamilton, OD, PA dba Hamilton Eye Associates to create and maintain health records that, in addition to their primary intended purpose of clinical and patient care use, will also serve business and legal needs.

Derek Hamilton, OD, PA dba Hamilton Eye Associates will document:

- Information comprises the health record for legal and business purposes.
- The various sources and location of the information.
- The media in which the information is maintained.

This document will be used to identify what information will be disclosed upon receipt of an authorized request for health records.

It is the policy of Derek Hamilton, OD, PA dba Hamilton Eye Associates yo maintain health records such that their integrity will not be compromised, and the records will support the business and legal needs of the practice.

Procedure

Accurate Patient Identification

It is the responsibility of Derek Hamilton, OD, PA dba Hamilton Eye Associates to:

- Work in conjunction with information services, legal services and others, to create and maintain a matrix or other document that tracks the source, location and media of each component of the health records;
- Identify any informational content that may be used in decision-making and care of the patient that may be external to the organization (outside records and reports, PHRs, email, etc.) that is not

included as part of the legal record because it was not made or kept in the regular course of business;
- Develop, coordinate and administer a plan that manages all information content, regardless of location or form, that comprises the legal health record of;
- Develop, coordinate and administer the process of disclosure of health information;
- Devise and administer a health records retention schedule that complies with applicable regulatory and business needs.

Information Services and Technology

Actions:

It is the responsibility of Information Services to:

- Ensure appropriate access to information systems containing components of the health record;
- Execute the archiving and retention schedule pursuant to the established retention schedule.
- Other duties include None.

Addendum to EHR

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)

Definitions

Business Record - a recording/record made or received in conjunction with a business purpose and preserved as evidence or because the information has value. Because this information created, received and maintained as evidence and information by an organization or person, in pursuance of legal obligation or in the transaction of business, it must consistently deliver a full and accurate record with no gaps or additions.

Data - basic facts about people, processes, measurements, and conditions represented in dates, numerical statistics, images and symbols. An unprocessed collection or representation of raw facts, concepts, or instructions in a manner suitable for communication, interpretation or processing by humans or automatic means.

Data Element - a combination of one or more data entities that forms a unit or piece of information, such as patient identifier, a diagnosis or treatment.

Electronic Health Record - medical information compiled in a data gathering format for retention and transferal of protected information via secured, encrypted communication line. The information can be readily stored onto an acceptable storage medium such as compact disk.

Evidence - information that a fact finder may use to decide an issue. Information that makes a fact or issue before court or other hearing more or less probable.

Legal Health Record - AHIMA defines the legal health record as "generated at or for a healthcare organization as its business record and is the record that would be released upon request." It does not affect the discoverability of other information held by the organization. The custodian of the legal health record is the health information manager in collaboration with information technology personnel. HIM professionals oversee the operational functions related to collecting, protecting, and archiving the legal health record, while information technology staff manage the technical infrastructure of the electronic health record.

The legal health record is a formally defined legal business record for a healthcare organization. It includes documentation of healthcare services provided to an individual in any aspect of healthcare delivery by a healthcare provider organization. The health record is individually identifiable data in any medium, collected and directly used in documenting healthcare or health status. The term also includes records of care in any health-related setting used by healthcare professionals while providing patient care services, reviewing patient data, or documenting observations, actions, or instructions.

Metadata - descriptive data that characterize other data to create a clearer understanding of their meaning and to achieve greater reliability and quality of information. Metadata consists of both indexing terms and attributes.

Original Document - an authentic writing as opposed to a copy.

Personal Health Records (PHR) - is an electronic, universally available, lifelong resource of health information needed by individuals to make health decisions. Individuals own and manage the information in the PHR, which comes from healthcare providers and the individual. The PHR is maintained in a secure private environment, with the individual determining rights of access. The PHR is separate form and does not replace the legal health record of any provider.

Regular Course of Business - doing business in accordance with your normal practice and custom,

as opposed to doing it differently because you may be or are being sued.

Source Systems - where the data was originally created.

Primary Source System - an information system that is part of the overall clinical information system in which documentation is most commonly first entered or generated.

Source of Legal Health Record - the permanent storage system where the documentation for the legal health record is held.

Other terms and their definitions which are used by Derek Hamilton, OD, PA dba Hamilton Eye Associates in written policies will be listed here:

None

Addendum to Practice Added Definitions

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)

Additional Addendum to Policy X

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)

Policy XI

Conclusion

Derek Hamilton, OD, PA dba Hamilton Eye Associates is committed to fully complying with government rules and regulations and assisting its employees to achieve their goal of 100% compliance.

If there are suggestions to improve the Practice's Compliance Program or reports of a situation(s) that may be a violation of the Program, staff should contact the Compliance Officer, Privacy Officer or Security Officer or other designated personnel to complete the necessary additions, changes and/or research needed to achieve resolution

References and Resources

- Relevant State & Federal Laws & Regulations References
- Applied Discovery http://www.lexisnexis.com/applieddiscovery/lawLibrary/default.asp
- Discovery Resources http://www.discoveryresources.org/
- Federal Judiciary. "Summary of the Report of the Judicial Conference Committee on Rules of Practice and Procedure." - Page 177
- http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Reports/ST09-2005.pdf
- Findlaw http://findlaw.com
- National Conference of State Legislatures http://www.ncsl.org
- "Thomas"-federal bill tracking http://thomas.loc.gov
- US Courts http://www.uscourts.gov/RulesAndPolicies.aspx

Addendum to Policy XI

(Any information contained in this addendum is content provided solely by the client and not that of Compliance Specialists, LLC)