HIPAA COMPLIANCE PLAN

FOR

OHIO EYE SURGEONS, INC.

Adopted August 2016

PREPARED BY STACEY A. BOROWICZ, ESQ.
DINSMORE & SHOHL LLP
614-227-4212
STACEY.BOROWICZ@DINSMORE.COM

OHIO EYE SURGEONS, INC.
CORPORATE RESOLUTION FROM SHAREHOLDER MEETING

Effective August 22, 2016, Ohio Eye Surgeons, Inc. ("Provider") adopted this HIPAA Compliance Plan to ensure the privacy, security and proper Use and Disclosure of Protected Health Information, in compliance with applicable federal and state law, including the HIPAA Privacy Rule (45 CFR Parts 160 and 164, Subparts A and E) and the HIPAA Security Rule (45 CFR Parts 160 and 164, Subparts A and C) and to satisfy the provisions of the Health Information Technology for Economic and Clinical Health Act, set forth in Division A, Title XIII, of the American Recovery and Reinvestment Act of 2009, and its implementing regulations and guidance (collectively, "HITECH"), including the Final Omnibus Rule.

Jori Hollenbeck will serve as the HIPAA Privacy Officer and the HIPAA Security Officer until replaced by the Shareholders.

HIPAA COMPLIANCE PLAN

Table of Contents

DEFINITIONS AND HIPAA OFFICER JOB DESCRIPTIONS

I. HIPAA DEFINITIONS

Access: The ability or the means necessary to read, write, modify, or communicate data or information or otherwise use any system resource.

Addressable (A): Refers to an "Implementation Specification" that the Provider may need to comply with to meet a standard under the Security Rule. To determine whether the Provider needs to comply with an "addressable" requirement, the Provider must (1) Assess whether the Implementation Specification is a reasonable and appropriate safeguard to the Provider's particular environment, when analyzed with reference to its likely contribution to safeguarding Electronic Protective Health Information (ePHI); (2) Initiate the Implementation Specification if reasonable and appropriate; (3) If the Implementation Specification is not reasonable and appropriate, document why the Provider cannot comply and maintain such documentation in the Provider's HIPAA Security Rule compliance records; and (4) If an equivalent alternative measure to comply with the Implementation Specification is reasonable and appropriate, the Provider should implement such measure.

Administrative Safeguards: Administrative actions, including policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect ePHI and to manage the conduct of the Provider's workforce as relating to the protection of ePHI.

ARRA: American Recovery and Reinvestment Act of 2009.

Authentication: The corroboration that a person is the one claimed.

Authorization: A written form containing the core elements and required statements set forth in the Privacy Rule, which is written in plain language and signed by an Individual to allow the Provider to Use or Disclose Protected Health Information for purposes other than Treatment, payment, and Health Care Operations.

Availability: Data or information is accessible and useable upon demand by an authorized person.

Breach: For purposes of the breach notification provisions of HITECH/ARRA, "Breach" means the acquisition, access, Use or Disclosure of Protected Health Information in a manner not permitted, which compromises the security or privacy of the Protected Health Information. For purposes of this definition, "compromises the security or privacy of the Protected Health Information" means "poses a significant risk of financial, reputation or other harm to the Individual."

Business Associate: A person or organization that performs a function or activity on behalf of the Provider, any subcontractor of a Business Associate of the Provider, involving the Use or Disclosure of Protected Health Information, such as claims processing, claims administration, data analysis, utilization review, quality assurance, billing, practice management, legal counsel, benefits management, or information technology consultants.

Business Associate Agreement: A written agreement between the Provider and a Business Associate or between a Business Associate and its subcontractor that guides how the parties will Use and Disclose Protected Health Information to perform the functions and activities of the business relationship in compliance with HIPAA.

Confidentiality: Data or information is not made available or Disclosed to unauthorized persons or processes.

Covered Entity: A Health Plan, Health Care Clearinghouse, or a Health Care Provider that transmits any health information in electronic form in connection with a transaction covered by the HIPAA regulations.

Designated Record Set: A group of records created and/or maintained by the Provider that include medical, billing, and health plan records that may be used in whole or in part to make decisions about Individuals, as defined in the Privacy Rule.

Disclosure: The release, transfer, provision of access to, or divulging in any manner of Health Information to any person or entity outside of the Provider.

EHR: Electronic Health Record

Electronic Media: Refers to electronic storage media, such as computer memory devices (hard drives) and any removable or transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card. Also refers to transmission media used to exchange information contained in electronic storage media, such as internet, extranet, leased lines, dial-up lines, private networks, and the physical movement of removable or transportable electronic storage media. Transmissions involving paper or voice, such as by fax or telephone, are not electronic media because the information being exchanged did not exist in electronic form before transmission.

Electronic Protected Health Information (ePHI): Protected Health Information that exists or is stored in Electronic Media.

Encryption: The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key, as defined in the Security Rule, as amended by HITECH/ARRA.

Facility: The physical premises, including the interior and exterior of a building.

Health Care: Care, services or supplies related to the health of an Individual, including preventive, diagnostic, therapeutic, rehabilitative, maintenance, palliative, and counseling care and services, or the sale of drugs, devices, equipment and other items in accordance with a prescription.

Health Care Clearinghouse: A public or private entity such as a billing service, a re-pricing company, or management and information systems that processes Health Information received from another entity into a HIPAA-compliant transaction for the electronic transmission of that Health Information.

Health Care Operations: Any activities of the Provider related to activities necessary to carry on business activities associated with the provision or administration of Health Care, including but not limited to activities associated with quality assurance and improvement, credentialing and license verification, practitioner and provider evaluations, insurance contracting and underwriting, audits and surveys, legal services, compliance programs, business planning and development, management and general administration.

Health Care Provider: A provider of medical or health services and any other person or organization that furnishes, bills, or is paid for health care in the normal course of business.

Health Information: Any information, oral or written and maintained in any form or medium, that relates to an Individual's past, present or future health conditions, treatments or payments, and is created or received by a Health Care Provider, Health Plan, Health Care Clearinghouse, public health authority, employer, life insurer, and school or university.

Health Oversight Agency: An agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person acting under a grant of authority from or contract with such a public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has been granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which Health Information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which Health Information is relevant.

Health Plan: An Individual or group health plan that provides for or pays the cost of medical care. Health plans include group health plans, health insurance issuers, HMOs, and most federally-funded health benefits programs.

HIPAA: Health Insurance Portability and Accountability Act of 1996. The Privacy Rule, Security Rule, ARA, HITECH and Final Omnibus Rule will collectively be referred to in this Plan as HIPAA.

HITECH: Health Information Technology for Economic and Clinical Health Act.

Implementation Specification: Means the specific requirements or instructions for implementing a standard under the Security Rule.

Incidental Disclosures: Unintended Disclosures that occur after reasonable safeguards have been taken to protect against unauthorized persons hearing or viewing an Individual's Protected Health Information.

Individual: A person who is the subject of Protected Health Information.

Individually Identifiable Health Information: A subset of Health Information, Individually Identifiable Health Information means demographic information collected from a Individual relating to past, present or future physical or mental conditions and treatments, or payments for treatment, that identifies the Individual or from which there is a reasonable basis to believe that the information can be used to identify the Individual.

Integrity: The property that data and information have not been altered or destroyed in an unauthorized manner.

Malicious Software: Refers to software designed to damage or disrupt a system, such as a computer virus.

Marketing: Any communications made about products or services with the intent to encourage Individuals to use or purchase the products or services, with certain exceptions as stated in the Privacy Rule.

Notice of Privacy Practices (NPP): A written notice provided to an Individual by the Provider describing the Uses and Disclosures of Protected Health Information that may be made by the Provider, the Individual's privacy rights, the Provider's legal duties with respect to the Individual's Protected Health Information, and the Individual's right to file a complaint upon belief that his/her privacy rights have been violated, prepared and distributed in accordance with the requirements set forth in the HIPAA Privacy Rule.

Password: The confidential authentication information composed of a string of characters permitting a person to access ePHI.

Personal Representative: A person with the legal capacity to make health care-related decisions on behalf of the Individual (*i.e.* parent, spouse, guardian, executor, power of attorney).

Physical Safeguards: Physical measures, policies, and procedures designed to protect a covered entity's electronic information systems and related buildings and equipment from natural hazards, environmental hazards, and unauthorized intrusion.

Provider: Ohio Eye Surgeons, Inc.

Privacy Rule: The Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164, Subparts A and E.

Protected Health Information (PHI): Individually Identifiable Health Information that is transmitted by electronic means, or transmitted or maintained in any other form or medium.

Privacy Officer: A person appointed by the Provider to be responsible for ensuring compliance with Privacy Rule and Security Rule through appropriate HIPAA policies and procedures.

Required (R): Refers to an "Implementation Specification" that the Provider must comply with to meet a standard under the Security Rule. The Provider must implement a policy and procedure if it is "required" under the Security Rule.

Responsible Person: Employee or other person responsible for carrying out a particular duty regarding the Use or Disclosure of an Individual's Protected Health Information by the Provider.

Security (Security Measures): Refers to all administrative, physical, and technical safeguards taken to protect an information system.

Security Incident: The attempted or successful unauthorized Access, Use, Disclosure, modification, or destruction of information or interference with system operations in an information system.

Security Officer: Individual responsible for compliance with the Security Rule.

Security Rule: The Standards for the Protection of Electronic Protected Health Information, 45 CFR Parts 160 and 164, Subparts A and C.

Standard: A rule, condition, or requirement relating to operational or informational services, procedures, and performance with respect to the privacy and security of Protected Health Information.

Technical Safeguards: The technology and the policy and procedures for its use that protect ePHI and control access to it.

TPO: Treatment, Payment and Health Care Operations.

Transaction: The transmission of information between two parties for financial or administrative activities that is related to health care.

Treatment: The provision, coordination, or management of an Individual's Health Care and related services by one or more Health Care Providers, including the coordination or management of Health Care by a Health Care Provider with a third party; consultation between Health Care Providers relating to an Individual; or the referral of an Individual for Health Care from one Health Care Provider to another.

Unsecured Protected Health Information: Protected Health Information that is not rendered unusable, unreadable, or indecipherable to unauthorized Individuals through the use of a technology or methodology specified by the Secretary in guidance issued and posted on the HHS website (i.e., encryption and destruction),

Use: The sharing, employment, application, utilization, examination, and analysis of Individually Identifiable Health Information by an entity, such as the Provider, maintaining such information.

User: A person or entity with authorized access to a system, such as a computer.

Workforce: Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a Covered Entity, is under the direct control of the Covered Entity.

Workstation: An electronic computing device, such as a laptop or desktop computer, or any other device that performs similar functions, and the Electronic Media stored within it and in its immediate environment.

II. HIPAA OFFICER'S JOB DESCRIPTION

Privacy Officer:

The Privacy Officer is responsible for overseeing and assuring proper Access, Use, and Disclosure of Protected Health Information that is generated or maintained by Ohio Eye Surgeons, Inc. (the "Provider") according to the Privacy Rule. If the Provider ever uses more than one person for all compliance functions, the Privacy Officer works in conjunction with the Security Officer and reports to the Compliance Officer for HIPAA-related matters.

The Privacy Officer's primary duties and responsibilities under the Privacy Rule include:

1. Compliance with the Privacy Rule by the Provider and all Workforce,

2. Overseeing the implementation, distribution, and enforcement by each region of the Provider's:

   - Privacy Policies and Procedures
   - Notice of Privacy Practices
   - Authorization for Disclosure of Protected Health Information

3. Assuring, in conjunction with the Security Officer that reasonable safeguards, security measures, and "firewalls" exist, so that Protected Health Information that is maintained by the Provider is not improperly Used or Disclosed.

4. Assuring, in conjunction with designated Workforce that reasonable safeguards are maintained and that Protected Health Information that is maintained by the Provider is not improperly Used or Disclosed.

5. Arranging for third-party administrators and other Business Associates of the Provider to enter into HIPAA-compliant Business Associate Agreements. Ensuring that the Business Associate Agreements utilized by the Provider are sufficient to address the safeguarding of Protected Health Information.

6. Receiving questions and complaints by Individuals who believe the Provider may have violated their privacy rights under the Privacy Rule and collaborating with the Compliance Officer in overseeing the Provider's internal complaint resolution process.

7. Overseeing appropriate mitigation and corrective action and recommending disciplinary action (if warranted) if violations of the Privacy Rule occur.

8. Acting as the contact person to respond to questions by the Department of Health and Human Services' Office for Civil Rights if an agency investigation is initiated, based on an Individual's complaint or otherwise.

9. Arranging by each region for Privacy Rule training for members of the Workforce, when and as required by the Privacy Rule, including maintaining appropriate documentation of such training.

10. Making periodic reports to the Board of Directors and the Workforce about privacy practices and ways to improve them.

11. The Privacy Officer is responsible for training, documentation, and investigation, as well as understanding the relevant state regulations.

Security Officer

The Security Officer is responsible for the development and implementation of procedures which prevent, detect, contain, and correct security violations, as required by the Security Rule. If the Provider ever uses more than one person for all compliance functions, the Security Officer works in conjunction with the Privacy Officer and reports to the Privacy Officer for Security Rule-related matters.

The Security Officer's primary duties and responsibilities under the Security Rule include:

1. Developing and implementing policies and procedures necessary for compliance with the Security Rule.

    - *Administrative Safeguards:* Implementing policies and procedures to prevent, detect, contain, and correct Security violations (i.e., required safeguards include risk analysis, risk assessment, sanction policy, and information system activity review).
    - *Physical Safeguards*: Implementing policies and procedures to limit physical Access to electronic information systems and the facility in which they are housed while ensuring that properly authorized Access is allowed.
    - *Technical Safeguards:* Implementing technical policies and procedures for electronic information systems that maintain electronic protected health information to allow Access to only those persons or software programs that have been granted access rights.

2. Performing periodic risk analysis and review of the Provider's Security and sanctions policies.

3. Ensuring that all members of the Provider's Workforce have appropriate Access to ePHI and preventing those Workforce members who do not have Access from obtaining Access to ePHI.

4. Receiving questions and complaints by Individuals who believe the Provider may have violated their Security rights, and in collaboration with the Privacy Officer, overseeing the Provider's internal complaint resolution process.

5. Identifying and responding to suspected or known Security Incidents and mitigating, to the extent practicable, harmful effects resulting from Security Incidents that are known to the Covered Entity.

6. Documenting Security Incidents, risk assessment of Security Incidents, investigation, mitigation, and outcomes.

7. Establishing and implementing a contingency plan for responding to an emergency or other occurrence (e.g., fire, vandalism, system failure and natural disaster) that damages systems that contain ePHI.

8. Implementing, overseeing, and reviewing the Provider's data back-up process, the disaster recovery plan, and the emergency mode operation plan.

9. Addressing whether the Provider should implement procedures for periodic testing and revision of contingency plan and assess the relative criticality of specific applications and data in support of other contingency plan components.

10. Performing a periodic technical and non-technical evaluation, based initially upon the standards implemented under the Security Rule and subsequently, in response to environmental or operational changes affecting the Security of ePHI that establishes the extent to which the Provider's security policies and procedures meet the requirements of the Security Rule.

11. Providing the Provider's Workforce with training, information, and updates about security and threats to Security. Arranging for Security awareness and training for appropriate members of the workforce, considering the following addressable standards:

    - Providing periodic Security updates and reminders to Workforce and vendors of the Provider.
    - Maintaining procedures for guarding against, detecting, and reporting malicious software (i.e. a virus designed to damage or disrupt a system).
    - Maintaining procedures for monitoring log-in attempts and reporting discrepancies.
    - Maintaining procedures for creating, changing, and safeguarding passwords.

12. Managing access and privileges for all system applications, devices that access the system and system users.

13. Maintaining and reviewing physical safeguards, including addressing whether the Provider should establish policies regarding facility access in case of emergency, implement a facility security plan, access control and validation procedures, and maintenance procedures.

14. Overseeing appropriate Workstation Use and Security by the Provider's Workforce,

15. Implementing device and media controls, disposal procedures, and Electronic Media re-use and accountability procedures.

16. Along with the Privacy Officer, ensuring that the Business Associate Agreements utilized by the Provider contain satisfactory assurances to address the safeguarding of electronic Protected Health Information.

17. Working with external vendors and Business Associates to ensure that new hardware and software connected to the existing computer and, if applicable, network system conforms to Security Rule standards and implementation specifications, such as unique user identification, emergency access procedures, automatic logoff, encryption and decryption, audit controls, integrity controls, authentication, and transmission security.

18. Overseeing appropriate corrective action and recommending disciplinary action (if warranted) if violations of the Security Rule occur.

19. Acting as a contact person along with the Privacy Officer to respond to questions by the Department of Health and Human Services' Office for Civil Rights if an agency investigation is initiated, based on an Individual's complaint.

20. Making periodic reports to the Provider's Senior Management, Privacy Officer and other appropriate Workforce about security practices and ways to improve them.

PRIVACY RULE POLICIES

III. NOTICE OF PRIVACY PRACTICES AND OBTAINING ACKNOWLEDGMENT OF RECEIPT OF NOTICE OF PRIVACY PRACTICES PROVIDER POLICY:

Provider has developed a NPP that complies with the current HIPAA requirements. Such NPP will be available and distributed as detailed below.

A. NPP Availability

- The NPP will be displayed at the registration window.
- The NPP will be posted on and downloadable from the Provider website(s).
- The NPP will be made available upon request in larger print for Individuals with vision impairments.
- The NPP will be communicated orally upon request for Individuals with vision or reading impairments.

B. NPP Distribution

The Provider must provide:

- All current patients/Individuals with a copy of the revised NPP upon request.
- All new patients/Individuals with a copy of a revised NPP.

C. Hard Copy Distribution of NPP

- A copy of the NPP will be provided by the front office staff upon registration to every new Individual and to any other Individual requesting a copy.
- The signed and dated Acknowledgment Form should be placed in the Individual's file.
- If the Individual refuses, for any reason, to sign the Acknowledgment Form (Form No. 1), the front office assistant should complete the bottom portion of the form and place it in the Individual's file. The receptionist may also indicate the Individual's refusal to sign on the bottom portion of the Acknowledgment Form.
- If the Provider knows transmission has failed, a paper copy must be provided to the Individual.

IV. USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION FOR TREATMENT, PAYMENT AND HEALTH CARE OPERATIONS

Provider Policy:

It is the policy of the Provider to comply with HIPAA and to Use or Disclose Protected Health Information for Treatment, Payment and Health Care Operations only as permitted by the Privacy Rule. Under the HIPAA Privacy Rule, the Provider and its Workforce may Use or

Disclose an Individual's Protected Health Information (PHI) for Treatment, Payment and Health Care Operations without obtaining a separate HIPAA-compliant Authorization from the Individual.

State law, however, still requires the Provider to obtain informed consent from an Individual prior to any treatment, diagnostic test or procedure.

PHI may be Used and Disclosed by the Provider for:

- Providing medical **Treatment** to Individuals for all activities relating to a Individual's health care, including consultations, counseling, referrals to another physician, hospital or health care provider, calling in prescriptions or orders, ordering laboratory tests, receiving laboratory and diagnostic test results, completing certificates of medical necessity, and sending medical records to other physicians and Health Care Providers involved with the Individual's treatment; etc.

- Obtaining **Payment** for services provided to Individuals, which includes all activities relating to the Provider obtaining payment for services from Medicare, Medicaid, private insurers, HMOs, managed care organizations, etc.

- Conducting the Provider's **Health Care Operations**, which may involve the use of an Individual's Protected Health Information for activities related to business and financial management, quality assurance reviews, compliance, audits, surveys, legal assistance, training, development of clinical guidelines, performance evaluations, etc.

V. USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION BY AUTHORIZATION PROVIDER POLICY:

The Provider has developed a HIPAA-compliant Authorization form (Form No. 2) for Individuals to use when they request their Protected Health Information be Disclosed to another person or entity for purposes not related to Treatment, Payment or Health Care Operations.

Any questions regarding the use of Authorizations should be directed to the Privacy Officer.

A. Use of an Authorization

Generally, an Authorization must be signed before an Individual's Protected Health Information can be used for:

- Marketing
- Fundraising
- Employment-related purposes
- Purposes not related to Treatment, Payment and Health Care Operations
- Research

- Schools
- Insurance companies (for enrollment purposes). (Note, Individuals may provide a written directive that Protected Health Information not be provided to their insurance company.)
- Persons or entities not involved in Treatment, Payment or Health Care Operations.

A copy of the Authorization is to be placed in the Individual's file and given to the Individual.

B. Required Statements

- The Individual's right to revoke the Authorization in writing, and either: (a) the exceptions to the right to revoke and a description of how the Individual may revoke the Authorization; or (b) to the extent that the information is included in the Notice of Privacy Practices, a reference to the Provider's Notice.
- The ability or inability to condition Treatment, Payment, Enrollment or Eligibility for benefits on the Authorization, by stating either: (a) the Provider may not condition Treatment, Payment, Enrollment or Eligibility for benefits on whether the Individual signs the Authorization when the prohibition on conditioning of Authorizations applies; or (b) the consequences to the Individual of a refusal to sign the Authorization when the Provider can condition Treatment, Enrollment in the Health Plan, or Eligibility for benefits on failure to obtain such Authorization.
- The potential for information Disclosed pursuant to the Authorization to be subject to re-disclosure by the recipient and no longer be protected by the Privacy Rule.

C. Defective Authorizations

Never Use, Disclose or release an Individual's PHI or medical record if an Authorization is defective. A defective Authorization is one that:

- Does not contain all of the core elements and required statements described above.
- Is expired or revoked.
- Combines a request for general medical information with a request for Psychotherapy Notes.
- Contains any information known by the Provider, or any of its Workforce, to be false.
- Does not contain any requirements of State law.

D. Processing Requests and Authorizations

1. Responding to an Individual's Request to Release Protected Health Information

- If an Individual requests the Provider to release or Disclose his/her Protected Health Information or medical record to another person or entity, inform the Individual that, in some cases, the Individual will need to submit a completed Authorization (Form No. 2) before the Provider can honor the request.

- The Privacy Officer or his/her designee will determine whether an Authorization is required for the use or Disclosure of the Individual's Protected Health Information.
- Individuals may come to the Provider to complete the Authorization, or the Provider will mail or fax the Authorization form to the Individual. The Individual may bring the completed Authorization form to the Provider in-person, or the Individual can mail or fax the completed form to the Provider.

2. Responding to an Authorization

- When an Authorization is received by the Provider, whether by mail, fax or in person, the Authorization is to be reviewed by the Privacy Officer or his/her designee.
- The Privacy Officer or his/her designee will check the Authorization to ensure that: (a) all required elements are present; (b) the Authorization is signed and dated by the Individual or his/her personal representative; and (c) the Authorization is not expired or revoked.
- If an Authorization is determined to be defective, for any reason, the Individual should be contacted by telephone and informed of the Provider's inability to complete the release of information. The Provider should document the reason for the defective Authorization and attempt to assist the Individual in completing a valid Authorization.
- The Privacy Officer or his/her designee will obtain the appropriate requested Health Information from the Individual's file and will only gather the Health Information that is needed to meet the Individual's request. Refer to the Minimum Necessary policy, if needed.
- The Privacy Officer or his/her designee will copy the requested Health Information and the Authorization.
- Place the original Authorization in the Individual's file. Complete the Accounting of Disclosures Tracking Log.
- Disclose or release the copied Protected Health Information to the receiving party as identified in the Authorization in the manner specified by the Individual (by mail, fax, or by hand-delivery).

VI. INDIVIDUAL'S RIGHT TO REVOKE AN AUTHORIZATION

Provider Policy:

An Individual has a right to revoke (cancel) an Authorization that he/she submitted to the Provider for the Use, release or Disclosure of Protected Health Information.

If an Individual revokes his/her Authorization, the Provider must comply with the Individual's request. An Individual's revocation of an Authorization must be (1) in writing and (2) signed and dated by the Individual.

An Individual's revocation of an Authorization affects only the use and Disclosure of Protected Health Information after the date that the Provider receives written notice from the Individual.

VII. USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION SPECIAL RESTRICTIONS FOR PHI FOR MARKETING, FUNDRAISERS OR SALE

Provider Policy:

Provider will comply with HIPAA and its limitations for the Use or Disclosure of Protected Health Information for Marketing, Fundraising, or Sale. Provider agrees to consult with legal counsel before any Use of Protected Health Information these purposes.

VIII. RELEASE OR DISCLOSURE OF PROTECTED HEALTH INFORMATION WITHOUT AUTHORIZATION MANDATORY DISCLOSURES AND REPORTING

Provider Policy:

Provider will comply with both Federal and State laws concerning the mandatory Disclosure of Protected Health Information. Provider will consult legal counsel before any of Mandatory Disclosures or Reports for public health activities or organizations, abuse or neglect reports, healthcare oversight, judicial or administrative proceedings, law enforcement, decedent information, organ donation organizations, health or safety threats or specialized government functions or workers' compensation benefits.

IX. RELEASE OF PROTECTED HEALTH INFORMATION TO ENTITIES NOT COVERED BY HIPAA PROTECTED HEALTH INFORMATION SUBJECT TO RE-DISCLOSURE

Provider Policy:

The Privacy Officer will handle or supervise all Disclosures to entities not covered by HIPAA in conjunction with legal counsel.

X. TRANSMITTING PROTECTED HEALTH INFORMATION BY FAX, E-MAIL, TELEPHONE AND ANSWERING MACHINES

Provider Policy:

Provider will use reasonable safeguards to prevent the unauthorized, improper or unintended Use and Disclosure of Protected Health Information, including the following:

A. Transmitting an Individual's Protected Health Information by Fax

- Check the Individual file to make sure that the Protected Health Information may be faxed to the recipient or whether the Individual has designated an alternative location or alternative means of communication.

- Before sending the fax, check the number to make sure the fax is sent to the correct recipient.
- If a fax is being sent to a recipient who does not usually receive Protected Health Information in this manner, call the recipient before faxing to alert the recipient to the incoming fax.
- Always use a fax cover sheet.
- A copy of the fax transmission report should be placed in the Individual file.

B. Leaving Messages on Answering Machines or Voice Mail

1. Check the Individual file to make sure that the Provider can contact the Individual or other persons by telephone or to check whether the Individual has designated an alternative location or alternative means of communication. Check also to make sure that a message may be left with a person, on an answering machine, or on voice mail at the telephone number.
2. Before placing a telephone call to the Individual or Health Care Provider, check the number before dialing.
3. If the call is answered, ask whether you can speak with the Individual. If the Individual is not available, leave a message for the Individual to call the Provider. Do not leave detailed medical information such as test results with another person or on an answering machine.

4. If the call is answered by an answering machine or voice mail, leave a brief message such as: "This is Provider calling for (Individual name), please call us back at xxx-xxxx" OR "This is Provider calling to remind (Individual name) about his/her appointment on date at time p.m."

C. Email Communications.

Provider will not communicate with patients by email.

XI. PROTECTING AN INDIVIDUAL'S PROTECTED HEALTH INFORMATION FROM INCIDENTAL USES AND DISCLOSURES

Provider Policy:

It is the policy of the Provider to comply with the Privacy Rule and to take reasonable efforts to safeguard the privacy and confidentiality of Individuals and prevent Protected Health Information from being viewed or overheard by unintended or unauthorized persons.

XII. MINIMUM NECESSARY STANDARD

Provider Policy:

It is the policy of the Provider to comply with the Privacy Rule and follow the Minimum Necessary Standard when Using or Disclosing the Protected Health Information.

To comply with the Minimum Necessary Standard, the Provider will identify those Workforce members who need access to Protected Health Information to perform their job duties. The Provider will also make reasonable efforts to limit the access of Workforce to Protected Health Information to the minimum necessary amount required to accomplish job-related tasks.

For any Disclosures occurring on a routine and daily basis, all Workforce with access will Use only the Protected Health Information in an Individual's record or file that is necessary to accomplish the specific task.

Workforce will not Disclose a Individual's entire record or file unless the request is specifically justified as the amount of information that is reasonably necessary to accomplish the purpose of the Disclosure or request.

XIII. USE AND DISCLOSURE OF A MINOR'S PROTECTED HEALTH INFORMATION

Provider Policy:

Provider will contact legal counsel about any Use or Disclosure of a Minor's Protected Health Information outside of an Authorization, Treatment, Payment or Healthcare Operations.

XIV. DISCLOSURE OF PROTECTED HEALTH INFORMATION TO FAMILY MEMBERS OR PERSONAL REPRESENTATIVES

Provider Policy:

A. **If the Individual is present:** Ask the Individual whether his/her Protected Health Information may be Disclosed to the accompanying family member or other person. If the Individual agrees or does not object or the Provider member making the Disclosure reasonably infers from the circumstances that the Individual does not object, the Disclosure may be made.

B. **If the Individual is not present or is incapacitated and in emergency situations:** The Provider may use professional judgment and allow, if in the Individual's best interests, a family member, personal representative, relative, friend or other person to act on behalf of the Individual for purposes of picking up prescriptions, x-rays, medical supplies, and other similar forms of Protected Health Information.

XV. INDIVIDUAL'S REQUEST TO ACCESS, INSPECT OR COPY PROTECTED HEALTH INFORMATION

Provider Policy:

A. If an Individual asks to inspect or copy records, provide him/her with the Request to Access, Inspect and Copy Records Form (Form No. 4).

B. The form must be completed and signed by the Individual or the Individual's Personal Representative. The Provider does not need to witness that signature.

C. Completed forms may be returned by mail or in person. All completed forms requesting inspection and copying should be directed to the Privacy Officer or his/her designee.

D. Requests should be processed (granted or denied) within 30 days from the date of receiving the completed form.

E. The Privacy Officer or his/her designee should review the record to determine what information/document is part of a Designated Record Set and whether any other information is privileged and not available for inspection. If the Provider making this initial determination has a question, clarification should be sought from legal counsel.

F. Once the records have been approved for release, they are returned to the appropriate Workforce member who will contact the Individual and arrange for the release. The Individual making the request can arrange for: (a) an appointment to inspect the records; or (b) the mailing of the requested records (at an address specified by the Individual—check for any requests for an alternative address); or (c) the mailing of a summary of the Protected Health Information in lieu of production of the records themselves; or (d) coming in to the Provider to pick up the records; or (e) sending a representative to pick up the records.

G. If the Individual requests that medical records be copied and sent, have him/her complete an Authorization.

H. The Provider may charge the requesting Individual certain costs such as copying and postage as permitted by State law.

I. If the person requesting to inspect the record is the Individual's Personal Representative, photocopy that person's driver's license or identification card and make sure that the Personal Representative Form matches. If the person claims to be the Individual's "attorney-in-fact" under a Durable Power of Attorney for Healthcare Decisions, or the Individual's Guardian or Executor, request a copy of the authorizing document in advance of the inspection date.

J. The Individual has a right to obtain a copy of his/her PHI in electronic format and, if the Individual chooses, to direct the Provider to transmit the ePHI to an entity or person designated by the Individual, provided that the Individual's choice is clear, conspicuous and specific. Any fee that the Provider may impose for providing the Individual with a copy of ePHI (or a summary or explanation of ePHI) must not be greater than the Provider's labor costs in responding to the request.

XVI. REQUEST TO RESTRICT DISCLOSURE OF PROTECTED HEALTH INFORMATION

Provider Policy:

A. If an Individual asks to restrict the Use or Disclosure of certain Health Information or records, provide the Individual with the Request to Restrict Use and Disclosure Form (Form No. 7).

B. The form must be completed and signed by the Individual or Individual's Personal Representative. You do not need to witness that signature.

C. Completed forms may be returned by mail or in person. All completed forms requesting restriction should be directed to legal counsel for review and instruction on next steps. Requests should be processed (granted or denied) as soon as reasonably practicable.

XVII. REQUEST TO AMEND OR CORRECT PROTECTED HEALTH INFORMATION

Provider Policy:

A. If an Individual asks to amend records, provide the Individual with the appropriate Request for Amendment of Records Form (Form No. 11).

B. The form must be completed and signed by the Individual or Individual's personal representative. You do not need witness that signature. The form must provide a reason to support the Individual's requested amendment.

C. Completed forms may be returned by mail or in person. All completed forms requesting an amendment should be directed to legal counsel for review and advice on next steps. Requests should be processed (granted or denied) within 60 days from the date of receiving the completed form.

XVIII. REQUEST FOR AN ACCOUNTING OF DISCLOSURES

Provider Policy:

It is the policy of the Provider to comply with the Privacy Rule and to allow Individuals to exercise their Individual privacy rights.

Under the Privacy Rule, an Individual (or his/her Legal Representative) has the right to request an accounting of the Disclosures of his/her Protected Health Information made by the Provider during the previous six (6) years.

An accounting of Disclosures must include the following information:

- The date that Protected Health Information was Disclosed;
- The name and address of the entity or person receiving the Protected Health Information, if known;
- A brief description of the Protected Health Information that was Disclosed;
- A brief statement of the purpose of the Disclosure that reasonably informs the Individual of the basis for the Disclosure, or a copy of the written request to use the Protected Health Information as required by the Secretary, Department of Health and Human Services, or a copy of the request for the Protected Health Information for which an Authorization is not required (see Mandatory Disclosures and Reporting Policy);

- The frequency, periodicity or number of Disclosures made to the person or entity; and
- The date of the last Disclosure occurring in the accounting period if multiple Disclosures were made to a single person or entity.

An accounting does not include Disclosures made by the Provider:

- To carry out Treatment, Payment and Health Care operations;
- Directly to the Individual or his/her Personal Representative;
- Incident to a Use or Disclosure permitted by the Privacy Rule;
- In response to an Authorization;
- To include the Individual in a facility directory;
- To persons involved in the Individual's care or for notification purposes; and
- To correctional institutions or law enforcement officials.

If a health oversight agency or law enforcement official provides the Provider with a written or oral statement notifying the Provider that an accounting of Disclosures will reasonably impede the agency's or official's activities, the Provider must not inform the Individual about these Disclosures.

The health oversight agency or law enforcement official must provide the Provider with a time period after which the information may be Disclosed in an accounting requested by the Individual (no longer than 30 days).

If the Provider has Disclosed Protected Health Information for research purposes, it must comply with the additional accounting requirements under 45 CFR §164.528(b)(4)

Procedure:

A. If an Individual asks for an accounting of Disclosures, provide the Individual with the Request for Accounting of Disclosures Form (Form No. 16).

B. The form must be completed and signed by the Individual or the Individual's Personal Representative. You do not need witness that signature.

C. The Privacy Officer or his/her designee should review the form to ascertain whether the requested information may be Disclosed to the Individual in an accounting under this policy.

D. Once the completed form is received, the Provider has 60 days to respond to the Individual's request. If the Privacy Officer cannot provide an accounting within the 60 days, an additional 30 days may be available if the Individual is provided with a written statement describing the reason for the delay and the date by which the Provider will provide the accounting. Only one extension is permitted by the Privacy Rule.

E. The Privacy Officer or his/her designee should prepare the accounting of Disclosures as described in the policy above (see Form No. 17).

F. If this is the first request for an accounting by the Individual in a 12–month period, do not charge the Individual for any fees incurred by the Provider to prepare the accounting.

G. If an Individual submits a subsequent request for an accounting in the same 12-month period, inform the Individual that a charge will be assessed, as described in the Notice of Privacy Practices. Ask the Individual if he/she wants to proceed with the accounting, if he/she wants to modify the request or withdraw the request in order to reduce or avoid any fees.

H. If the request for an accounting is a subsequent request by the Individual in the same 12-month period as the first request, the Provider will charge the Individual the then established copy charge depending on document produced (i.e. paper, x-rays etc.) and postage. The Individual will be advised of the costs at the time of the request.

I. A copy of the accounting should also be placed in the Individual's file.

XIX. REQUEST FOR COMMUNICATION OF PROTECTED HEALTH INFORMATION BY AN ALTERNATIVE MEANS

Provider Policy:

An Individual (or his/her Personal Representative) has the right to request in writing the Provider to communicate with him/her at an alternative location or by an alternate means. This right allows an Individual to direct how and where confidential communications made by the Provider and concerning Protected Health Information are sent, faxed, e-mailed or telephoned. For example, an Individual can ask the Provider not to call him at a work telephone number.

If an Individual requests that communications be directed to an alternative location or by an alternate means, provide the Individual with the Request to Receive Confidential Communications Form (Form No. 19). The Privacy Officer will decide if the request can be reasonably accommodated by the Provider. If yes, the Provider must honor the Individual's request and Form 19 will be placed in the Individual's file next to his/her contact information.

If the Individual's request cannot be reasonably accommodated, or if the Individual's request would hinder his/her care and treatment or the Provider's billing and payment for services, the Provider is not required to honor the request. If the Privacy Officer determines the Provider cannot reasonably accommodate the Individual's request, notice should be provided to the Individual by an appropriate method explaining the reason for the denial of the request. Attach the notice provided to the Individual (with the reason for the denial) to the Request Form and place both in the Individual's file (see Form No. 20).

XX. BUSINESS ASSOCIATE AGREEMENTS

Provider Policy:

The Provider will enter into compliant Business Associate Agreements (BAA) in the form provided in this Plan (See Form No. 24) with all appropriate parties. The Provider will keep all such BAAs on file.

XXI. COMPLAINT RESOLUTION PROCEDURE

Provider Policy:

A. If an Individual, or other person, contacts the Provider to make a complaint, provide the Individual with the Complaint Form (by fax, mail, or e-mail) (see Form No. 21).

B. If the Individual, or other person, wants to submit a complaint orally (by telephone or in person), refer the Individual to the Privacy Officer.

C. Assure the Individual, or other person, that his/her Complaint will be immediately investigated. Inform the Individual that the Provider will respond to the complaint within 30 days.

D. The Privacy Officer or his/her designee will record all complaints using the Complaint Record and Disposition Form (Form No. 22) and include:

- The date the complaint was received, nature of the complaint;
- The date when violation allegedly occurred;
- Name of person(s) who allegedly violated the Individual's privacy or security right;
- Description of the investigation;
- Any actions taken; and
- Description of the correspondence or feedback provided to the Individual.

E. The Privacy Officer or his/her designee will analyze the complaint by interviewing the Individual or Workforce members involved, and other methods of investigation as necessary and appropriate.

F. If the complaint is validated, the Privacy Officer will implement the appropriate and reasonable remedial actions to resolve the complaint. This may entail revising Provider policies and procedures, job responsibilities, or other Provider functions.

G. If the complaint is validated (if the Individual or person identifies himself), and if the Privacy Officer will provide the Individual or person with a letter summarizing the results of the investigation and the remedial actions taken by the Provider in response to the Individual's complaint.

H. If the Individual's complaint is not reasonable, or cannot be adequately addressed by the Provider, the Privacy Officer will send a letter to the Individual summarizing the results of the investigation and an explanation why action cannot be taken in response to the Individual's complaint.

I. The Privacy Officer will inform the Individual whether the complaint is validated or not, that he/she may also submit a complaint to the Secretary, Department of Health and Human Services and will provide the Secretary's address in any letter sent to the Individual.

J. A statement should be included in all letters to Individuals making complaints:

"Because we understand your concerns about the privacy and confidentiality of medical and health information, it is the policy of the Provider not to retaliate against any Individual making a complaint directly to us or to the Secretary, Department of Health and Human Services."

K. A copy of the Individual's complaint should not be placed in the Individual file. Instead, a copy of the Individual's complaint, along with any follow-up letters and investigation documentation, should be kept in a separate HIPAA-compliance file and the Complaint Log, maintained by the Privacy Officer.

K. The Provider prohibits its Workforce from retaliation against any Individuals who files a complaint using the Provider's Complaint Resolution Procedure or submits a complaint to the Secretary, Department of Health and Human Services. Workforce members who retaliate against an Individual, or the Individual's personal representative or family members, may be subject to disciplinary measures as set forth in the Employee Handbook.

XXII. WORKFORCE CONFIDENTIALITY AGREEMENT

Provider Policy:

As a part of the Provider's commitment to protecting the privacy and security of its Individuals' Protected Health Information, Workforce members are required to sign and abide by a Confidentiality Agreement and participate in annual HIPAA training. .

XXIII. DUTY OF WORKFORCE TO REPORT PRIVACY BREACHES

Provider Policy:

Workforce members must report verbally or writing any Breach of privacy, or a concern about the privacy or confidentiality of Protected Health Information to the Privacy Officer or Corporate Compliance Officer. All reports will be kept confidential. The Provider will implement at least means for anonymous reporting.

XXIV. PRIVACY RULE INVESTIGATION PROTOCOL

Provider Policy:

If the Provider becomes the subject of an investigation, Workforce should:

- Inform the Privacy Officer, Corporate Compliance Officer and legal counsel immediately.
- Recognize that the Provider will cooperate with all investigations.
- Not destroy, alter or hide documents.
- Not talk among themselves or with former Workforce members about the investigation unless legal counsel is present or permits conversation about the matter.
- Cooperate with the persons who are investigating the violation.
- Report all investigation-related concerns to the Privacy Officer or Corporate Compliance Officer.
- Remain calm if an agent shows up at a Provider's office(s) and immediately get the Administrator or Privacy Officer.
- Do not answer questions without first obtaining the approval of general legal counsel. Do not volunteer any information or documents.

SECURITY RULE POLICIES

XXV. SECURITY STANDARDS: GENERAL RULES

Provider Policy:

To comply with the HIPAA Security Rule and its standards, the Provider will develop and implement reasonable policies, procedures and practices to safeguard Electronic Protected Health Information (ePHI) as provided in the Security Rule's implementation specifications as follows.

1. The Provider will adopt policies and procedures for implementation specifications that are designated as:

- **(R)** – Means the Provider is **required** to comply with and implement the Security Rule's implementation specification.

- **(A)** – Means the Security Rule's implementation specification is **addressable**. If a implementation specification is addressable, the Provider must: Assess whether the implementation specification is a reasonable and appropriate safeguard in the Provider's particular environment, when analyzed with reference to its likely contribution to safeguarding electronic protected health information and Individuals' identities and implement the implementation specification if reasonable and appropriate.

  If the implementation specification is not reasonable and appropriate, document why it is not reasonable and appropriate for the Provider. Maintain such documentation in the Provider's compliance records.

The Provider will review and modify security measure and policies as needed after implementation to continue the provision of reasonable and appropriate protection of ePHI and Individuals' identities.

XXVI. ADMINISTRATIVE SAFEGUARDS

Provider Policy:

It is the policy of the Provider to take administrative actions to manage the selection, development, implementation, and maintenance of security measures to protect Electronic Protected Health Information and to manage the conduct of the Provider's Workforce as relating to the protection of that information to comply with the HIPAA Security Rule.

A. Security Management Process

1. Risk Analysis **(R)**

The Provider will conduct accurate and thorough assessments of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the covered entity.

A risk assessment will be conducted to determine the Access to and Use and Disclosure of ePHI and Individuals identities in the Provider's facilities and/or workforce. The risk assessment will:

- Identify the scope of the analysis;
- Gather information and data;
- Identify and document potential threats and vulnerabilities to ePHI and identity theft;
- Assess the Provider's current security and protection measures;
- Determine the likelihood that a threat to ePHI will occur;
- Determine the potential impact if a threat occurred;
- Determine the level of risk; and
- Identify the appropriate Security measures that should be taken to protect against threats and risks to EPHI and Individual identity theft.

The Security Officer or designee will conduct periodic risk assessments to monitor compliance with the Security Rule, determine whether policies and practices require changes, and to analyze any new or modified Security needs. All risk assessments will be documented and maintained in the Provider's compliance files maintained by the Security Officer or designee.

2. Risk Management **(R)**

The Provider will implement policies and procedures for maintaining the Security of ePHI and Individuals' identities, in addition to adopting adequate security measures to reduce risks and vulnerabilities to a reasonable and appropriate level. The Provider will strive to ensure the confidentiality, integrity, and availability of all ePHI that it creates, receives, maintains, or transmits. The Provider will address potential risks and vulnerabilities identified in Risk Analysis as part of Risk Management.

The Provider creates, stores and transmits ePHI in a secure manner. The Provider also maintains Individuals' identities in a secure manner.

To manage risks and to address issues arising from periodic risk assessments, the Provider will:

(a) Develop and implement a risk management plan;

(b) Implement security measures;

(c) Evaluate whether Security measures are appropriate, reasonable, and effective;

(d) Require all Workforce members to abide by the Provider's Security policies; and

(e) Consult with appropriate software/hardware vendor(s) to appropriately and adequately address risks and vulnerabilities to the ePHI that is created and stored in the Provider's computer and/or network systems. Each external IT vendor is expected to enter into a Business Associate Agreement.

3. Sanction Policy **(R)**

The Provider will apply appropriate sanctions against Workforce members (employees, volunteers, contractors, etc.) who fail to comply with Security policies and procedures.

Workforce members who fail to comply with Security policies will be subject to disciplinary action as reflected in the Employee Handbook including possible termination of employment.

4. Information System Activity Review **(R)**

The Provider will regularly review records of information system activity, and maintain records of Security incidents, actions, and outcomes.

(a) The Provider will perform periodic audits of electronic media access and use by Workforce members, internally and in collaboration with external vendor(s) and auditors. The Security Officer or designee will maintain records of such audits, findings and response(s).

(b) The Security Officer or designee will document and maintain records of security incident, actions taken, and outcomes.

B. Workforce Security

The Provider will implement procedures to ensure that all members of the Workforce have appropriate access to ePHI and to prevent those Workforce members who do not need access to ePHI from obtaining access to ePHI.

ePHI may be accessed by the Privacy Officer, Compliance Officer, Administrator, providers, billing personnel and vendors, and those authorized by the Privacy Officer or Compliance Officer.

1. Authorization and/or Supervision **(A)**

For all Workforce members, the Security Officer, in collaboration with the Privacy Officer, manager and other required personnel, will:

(a) Provide proper supervision of a Workforce member's access, Use, and Disclosure of ePHI according to the Provider's organizational structure.

(b) Review periodically the authorization and supervision of Workforce members to determine whether changes or updates are necessary.

(c) Provide physical access to areas where ePHI may be accessed only to Workforce members with proper clearance when possible.

2. Workforce Clearance Procedure **(A)**

On the date of hire for a new employee or other workforce member or for changes in employment or position within the Provider, the Security Officer, in collaboration with the Privacy Officer, the managers and other required personnel will:

(a) Assess the Workforce member's need to access, Use, and Disclose ePHI.

(b) If practicable, assign the Workforce member a unique user identification (user ID), password, and level of access.

(c) Inform the Workforce member about his/her level of access to ePHI, including any areas of restricted access.

(d) Provide the Workforce member with appropriate passwords and other security clearance as necessary.

(e) Review periodically all Workforce members' access rights to ePHI to determine whether modification is necessary. A review will consider whether access should be granted, should be restricted or not granted, or should be removed if a Workforce member does not have clearance or a need to access the ePHI.

3. Termination Procedures **(A)**

Upon a Workforce member's termination, or upon any other event that changes a Workforce member's duties with the Provider, the manager or other designated person, in collaboration with the Security Officer and Compliance Officer will:

(a) Review the Workforce member's clearance and access rights.

(b) Remove the Workforce member's ability to access ePHI, such as terminating the Workforce member's user identification (ID) and password.

(c) Require the Workforce member to return all keys, access cards, equipment, transportable disks and files, and other materials that are the property of the Provider.

C. Information Access Management

The Provider will implement policies and procedures for authorizing Access to ePHI

1. Access Authorization **(A)**

The Provider will use the following steps for granting Access to ePHI:

(a) Determine the Workforce member's level of Access by job position and need to Access ePHI to complete job functions.

(b) If practicable, provide a Workforce member with the appropriate user ID and passwords to Access only those areas of ePHI required to perform his/her job functions.

(c) Depending upon the Workforce member's position with the Provider, he /she may Access ePHI at his/her workstation.

2. Access Establishment and Modification **(A)**

The Administrator, Security Officer, Compliance Officer and other designees will implement the Provider's Access authorization policies and will document, review, and modify a Workforce member's right of Access to ePHI according to both the procedures set forth in these security policies and the Provider's employee policies.

D. Security Awareness and Training

The Provider will implement a Security awareness and training program for all Workforce members, including management, and periodically update such awareness and training.

1. Security Reminders **(A)**

(a) Periodic updates about Security issues will be provided to Workforce members utilizing personal and video presentations, and written materials including e-mail and intranet postings.

(b) Periodic Security updates and notices may also be posted on bulletin boards or other location in Provider locations.

(c) Security updates and information will be provided at staff meetings.

2. Protection from Malicious Software **(A)**

The Provider will adopt methods to guard against, detect, and report malicious software (i.e. a virus designed to damage or disrupt a system):

(a) Use of various software or other application installed in the Provider's information systems to protect ePHI.

(b) Enforce an Electronic Use Policy.

E. Security Incident Procedures

The Provider will implement procedures for addressing Security Incidents.

1. Response and Reporting **(R)**

The Provider will identify and respond to suspected or known Security Incidents and mitigate, to the extent practicable, harmful effects resulting from Security Incidents that are known to the Provider.

(a) All Workforce members must immediately report any suspected or known Security Incidents, such as virus contamination, unauthorized Access by a Workforce member, Access by any other person, loss of ePHI, or disruption to ePHI to a manager, Privacy Officer, Security Officer or Compliance Officer.

(b) The manager, Security Officer, or other designated person will investigate the report of a Security Incident using the appropriate form (see Security Incident Report form).

(c) The Security Officer in collaboration with the Privacy Officer, Compliance Officer and other designee(s), will determine the appropriate method to address or mitigate the Security Incident.

(d) All efforts to investigate, address, and mitigate will be documented, along with the outcome of the Security Incident. All Security Incident Report forms will be maintained by the Security Officer for the Provider's compliance file.

F. Security Contingency Plan

The Provider will establish, and implement as necessary, policies and procedures for responding to an emergency or other occurrence (i.e. fire, vandalism, system failure, and natural disaster) that damages computer and/or network systems containing ePHI. Such policies will include a data backup plan and disaster recovery plan.

1. Data Back-Up Practice **(R)**

The Provider will establish and implement procedures to create and maintain retrievable exact copies of ePHI by:

(a) When needed, copying ePHI onto transportable media (such tape, CD-ROM, paper, or other storage device) and send it to a secure offsite storage location.

(b) Following the Provider's data backup and storage Practice.

(c) the Device and Media Controls section of the Provider's security policies.

2. Disaster Recovery Practice **(R)**

The Provider will attempt to recover any data losses by:

(a) Timely obtaining stored back-up and re-loading onto to the Provider's information systems, network or computers.

(b) Consulting with an appropriate external vendor to determine the best method for recovering data losses.

3. Emergency Mode Operation Practice **(R)**

In the event of an emergency that disrupts the Provider's Electronic Media, the Provider will continue with its critical business processes to the extent practicable and for protection of the Security of ePHI while operating in emergency mode by:

(a) Determining the critical Provider operations and activities, if any, that must continue to function during the emergency and disruption.

(b) Continuing with critical Provider operations using alternate methods or locations. For example, paper and other available media will be used until the data and information can be transferred to the Provider's electronic records.

(c) Using generators for continued power and other similar measures, if necessary.

(d) The Security Officer, Privacy Officer, Compliance Officer, others in senior management will determine the best course of action if the emergency threatens the Provider's Electronic Media or ePHI.

4. Testing and Revision Procedure **(A)**

The Security Officer, or other designated person, will periodically review the Provider's practices and action steps for emergency mode operations. External vendor(s) may be consulted to review the Provider's action steps for safeguarding and securing the confidentiality and integrity of ePHI.

5. Applications and Data Criticality Analysis **(A)**

The Security Officer will periodically analyze the Provider's action plan and steps for emergency mode operations of its information systems. External vendor(s) may be consulted to review the Provider's action steps for safeguarding and securing the confidentiality and integrity of ePHI during an emergency or disaster.

G. Evaluation.

The Provider will perform periodic technical and non-technical evaluations to assess security based initially upon the standards implemented and in response to environmental or operational changes affecting the security of ePHI .

(a) The Provider will include Security evaluations in its review of compliance with other laws.

(b) The Security Officer, or other designated person, will perform on-going reviews/evaluations to reflect all of the steps taken to comply with the Security Rule. These reviews/evaluations will be documented and maintained by the Security Officer for the Provider's compliance file.

H. Business Associates and Other Contractual Arrangements

To comply with the Security Rule, the Provider will:

(a) Review current Business Associates to determine whether ePHI is Used by the Business Associate to perform a function or activity on behalf of the Provider.

(b) Determine whether an addendum or modification is required to the existing Business Associate Agreement to address the safeguarding of ePHI.

(c) Determine whether new vendors, advisors, consultants, etc. require a Business Associate Agreement.

(d) Obtain the appropriate Business Associate Agreements and/or addenda.

(e) Ensure that its Business Associate Agreements are revised, when and as required.

XXVII. PHYSICAL SAFEGUARDS

Provider Policy:

It is the policy of the Provider to use physical measures, policies, and procedures designed to protect its electronic information systems and related buildings and equipment from natural hazards, environmental hazards, and unauthorized intrusion to comply with the HIPAA Security Rule.

A. Facility Access Controls

The Provider will implement policies and procedures to limit physical access to electronic information systems and the facility in which they are housed while ensuring that properly authorized Access is allowed.

1. Contingency Operations **(A)**

The Security Officer will be responsible for establishing and implementing procedures that allow access to both information systems and the facility to restore lost data and other damaged equipment in the event of an emergency.

2. Facility Security Plan **(A)**

The Provider will safeguard all of its facilities and equipment from unauthorized physical access, tampering, and theft by:

(a) Providing keys only to Workforce members with a need for 24-hour access to the Provider's facilities.

(b) Prohibiting unauthorized persons, including Workforce members without clearance, Individuals, and Individual's friends and family, from physically accessing and tampering with the Provider's hardware and equipment by restricting such locations as "employee only."

(c) Using and activating an appropriate theft-deterrent system or alarm.

(d) Monitoring use of access cards and keys.

(e) Deactivating lost or stolen access cards or changing locks, when necessary.

3. Access Control Procedures **(A)**

The Provider will control access to facilities based on the Workforce member's job role or function. The Provider will implement "visitor" control policies.

4. Maintenance Records **(A)**

A manager will document all repairs and modifications to the physical components of a facility which are related to security, including any changes to hardware, walls, doors, and locks. Documentation may be kept in the Provider's business records or compliance file.

B. Workstation Use (R)

All of the Provider's Workstations will be used by authorized Workforce members solely for purposes related to Treatment, Payment, Health Care Operations, treatment, payment, health care operations, and the business of the Provider.

C. Workstation Security (R)

The Provider will restrict Access to workstations to those Workforce members who are authorized users. To further promote Workstation security, Workforce members will:

(a) Comply with the Provider's HIPAA Privacy Policy to protect a Individual's Protected Health Information from unintentional view or overheard conversations.

(b) Shield computer screens located in public areas from unauthorized viewing and/or visitors, when necessary.

(c) Control Individual, family, and visitor access to "employee only" areas of the Provider's facilities.

(d) Only authorized users may log-in and access ePHI at the Provider's Workstations. Users must log-out when leaving their workstations and/or protect their workstations from access by others.

D. Device and Media Controls

The Provider will implement policies and procedures that govern the receipt and removal of hardware and Electronic Media from the Provider's offices and facilities. The Provider will adopt a procedure for tracking any ePHI that comes into and out of the Provider (i.e. information needs to be shared between Provider's locations, offices or facilities).

1. Disposal **(R)**

The Provider will implement procedures to address the final disposition of ePHI and/or the hardware or Electronic Media on which it is stored. The Provider's record disposition policy for the destruction of Individual-related and health care information (and business records) will use:

(a) A disposal destruction method which prevents any possibility of reconstructing ePHI as appropriate to the media storing the ePHI. Disposal methods include, but are not limited to:

- For paper: burning, shredding, pulping, pulverizing
- For microfilm or microfiche: recycling or pulverizing
- For laser disks in write once-read many (WORM) documents: pulverizing
- For computerized data: magnetic degaussing or overwriting (total destruction does not occur until all original and backup data are destroyed)
- For magnetic tapes: magnetic degaussing (and possibly overwriting)

(b) When necessary, the Provider will use one or more vendor(s) certified/licensed to appropriately dispose of ePHI, hardware, or Electronic Media.

(c) The Provider will document the disposal of ePHI using a form, certificate or record. Documentation will include date of destruction, method used, person(s) responsible, dates of records destroyed, a statement that the

records were destroyed in the normal course of business, and signature of the supervising Individual(s).

2. Media Re-use **(R)**

The Provider will appropriately remove ePHI from electronic media before the media are made available for re-use when required by:

(a) Deleting ePHI from tapes, diskettes, rewritable CDs, and other reusable media, when necessary, using an appropriate software program.

(b) Consulting with the Provider's information systems vendor to determine the appropriate removal method for the electronic media being re-used.

3. Accountability **(A)**

The Provider will maintain a record of the hardware and Electronic Media owned by the Provider and transported by Workforce members responsible for the items in a given timeframe by:

(a) Keeping an inventory and log of the Provider's computers, hardware, and other Electronic Media storing ePHI.

(b) Maintaining a record of Workforce members who have access to the Provider's transportable Electronic Media, such as laptops and personal electronic devices.

(c) If a laptop or other electronic device is made available or shared between workforce members, maintaining a log for signing out and returning such electronic equipment.

4. Data Backup and Storage **(A)**

The Provider will create a retrievable, exact copy of ePHI when needed, before movement of equipment by:

(a) Creating periodic backup tapes of all ePHI stored in the Provider's information systems.

(b) Backup tapes will be stored in a secure and fireproof location.

(c) All old computers will be backed up before the ePHI is deleted, if applicable.

XXVIII. TECHNICAL SAFEGUARDS

Provider Policy:

It is the policy of the Provider to comply with HIPAA's Security Rule by implementing policies and procedures when using technology to protect ePHI and to control Access to it.

A. Access Control.

The Provider will implement technical policies and procedures for its electronic information and computer systems to maintain ePHI and to allow Access to only those Workforce members who have been granted Access rights

1. Unique User Identification **(R)**

If practicable, each Workforce member with access to ePHI will be assigned a unique name and/or number for identifying and tracking user identity. The Security Officer or designee will assign and track the unique user identification according to the Provider's employee and security policies.

2. Emergency Access Procedure **(R)**

The Provider will use, as needed, the following procedures for obtaining necessary ePHI during an emergency:

(a) The Security Officer, Privacy Officer, and others in senior management will determine the necessary amount of ePHI requiring access during an emergency.

(b) Senior management will determine whether backup tapes should be obtained from storage.

(c) The Security Officer, Privacy Officer and others in senior management may consult with one or more vendors to determine what, if any, additional actions to take in the event of an emergency.

3. Encryption and Decryption **(A)**

If required, reasonable, and attainable, the Provider will implement a mechanism to encrypt and decrypt stored ePHI. The Provider will assess whether this Security measure is reasonable during the periodic evaluations required by the security policies.

4. Automatic Logoff **(A)**

If reasonable and appropriate for the Provider's operations, and to implement additional security measures without jeopardizing the integrity and confidentiality of ePHI, the Provider will:

(a) Develop and use a method for terminating an electronic session (i.e. computer access) after a predetermined time of inactivity.

(b) Assess additional Security measures are required during the periodic evaluations required by the Security policies.

B. Audit Controls (R)

When reasonable and practicable, the Provider will use any and all hardware, software, and/or procedural mechanisms that record and examine activity in its information systems that contain or use ePHI. The Security Officer will audit such information at regular intervals. The Provider will assess whether this Security measure is reasonable during the periodic evaluations required by the Security policies.

C. Integrity (A)

The Provider will protect ePHI from improper alteration or destruction. The Provider will determine reasonable methods for authenticating ePHI. The Provider may use one or more external vendors.

D. Person or Entity Authentication (R)

If practicable, the Provider will verify that a person or entity seeking Access to ePHI is the one claimed through the use of unique user IDs and passwords.

E. Transmission Security

The Provider will use appropriate and reasonable technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communication network.

1. Integrity Controls **(A)**

The Provider will comply with all government and commercial payor requirements for transmitting billing data and other Individual information to ensure the Integrity and Security of transmitted ePHI, when applicable

2. Encryption **(A)**

The Provider will comply with all government and commercial payor requirements for transmitting billing data to ensure the Integrity and Security of transmitted ePHI.

XXIX. BREACH NOTIFICATION

Provider Policy:

In case of Security Incident, Provider will immediately contact legal counsel to perform a Breach analysis and consider all of the following:

- Nature of Protected Health Information
- Who

- Evidence of Access or Disclosure
- Mitigation of Risk

The Provider shall, upon discovery of a Breach of Unsecured Protected Health Information, notify each Individual whose Unsecured Protected Health Information has been, or is reasonably believed by the Provider to have been, Accessed, acquired or Disclosed as a result of the Breach. Such notice will be given as soon as possible, but in no case longer than sixty (60) days after the Breach is discovered.

- Notification of Provider by Business Associate: A Business Associate of the Provider that accesses, retains, modifies, records, stores, destroys or otherwise holds, Uses or Discloses Unsecured Protected Health Information shall, following the discovery of a Breach of such information, notify the Provider of such Breach. Such notice shall include the identification of each Individual whose Unsecured Protected Health Information has been, or is reasonably believed by the Business Associate to have been, accessed, acquired or Disclosed during the Breach.

- Breaches Treated as Discovered: A Breach shall be treated as discovered by the Provider or a Business Associate as of the first day on which such Breach is known to such entity or associate to have occurred (including any person, other than the person committing the Breach that is an employee, officer or agent of the entity or associate) or should reasonably have been known to such entity or associate to have occurred.

- Timeline of Notification: All required notifications shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of a Breach by the Provider involved (or Business Associate). The Provider and/or the Business Associate shall have the burden of demonstrating that all notifications were made as required, including evidence demonstrative the necessity of any delay.
- Methods of Notice;
  - Individual Notice
    - Notice shall be provided promptly and in the following form:
      - Written Notice -- Written notification by first-class mail to the Individual (or next of kin) at the last known address of the Individual (or next of kin) or, if specified, by electronic mail. The notification may be provided in one or more mailings as information is available.
      - Substitute Notice -- If there is insufficient or out of date contact information that precludes direct written or electronic notification to an Individual, a substitute form of notice shall be provided, including, in the case that there are 10 or more Individuals for which there is insufficient contact information, a conspicuous posting for a period determined by the Secretary of Health and Human Services on the home page of the Provider's website or notice in major print or broadcast media, including major media in geographic areas where the Individuals affected by the Breach

likely reside, that includes a toll-free phone number where an Individual can learn whether or not the Individual's Unsecured Protected Health Information is possibly included in the Breach.

- Additional Notice in Urgent Situations -- If the Provider deems any case to require urgency because of possible imminent misuse of Unsecured Protected Health Information, the Provider may also provide information to Individuals by telephone or other means, as appropriate.

- Media Notice
  - Notice shall be provided to prominent media outlets serving the relevant State or jurisdiction, following the discovery of a Breach of the Unsecured Protected Health Information of more than 500 residents is, or is reasonably believed to have been, Accessed, acquired, or Disclosed during such Breach.
- Notice to the Secretary of Health and Human Services
  - The Provider shall notify the Secretary immediately if a Breach of Unsecured Protected Health Information involves 500 or more Individuals. If the Breach involves less than 500 Individuals, the Provider will notify the Secretary of Health and Human Services within sixty (60) days of Discovery.
- Posting on HHS public website
  - The Secretary shall make available to the public on the Internet website of the Department of Health and Human Services a list that identifies each Covered Entity involved in a Breach involving more than 500 Individuals.

- Content of Notification: The Provider shall provide Notice of Breach that includes, to the extent possible:

  1. a brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known;
  2. a description of the types of Unsecured Protected Health Information that were involved in the Breach (such as full name, Social Security number, date of birth, home address, account number, or disability code);
  3. the steps Individuals should take to protect themselves from potential harm resulting from the Breach;
  4. a brief description of what the Provider is doing to investigate the Breach, to mitigate losses, and to protect against any further Breaches; and
  5. contact procedures for Individuals to ask questions or learn additional information, which will include a toll-free telephone number, an email address, website or postal address.

- Delay of Notification Authorized for Law Enforcement Purposes: If a law enforcement official determines that a required notification, notice or posting would impede a criminal investigation or cause damage to national security, the Provider will delay notification, notice or posting. In such instances, the Provider must:

  - document the statement, including the identity of the agency or official making the statement;

- temporarily suspend the Individual's right to an accounting of Disclosures subject to the statement; and
- limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement is provided specifying the time for which such a suspension is required.

Breach Exclusions:

- any 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, if it was made in good faith and within the scope of authority and does not result in further Use or Disclosure in a manner not permitted;
- any inadvertent Disclosure by a person who is authorized to access Protected Health Information as a Covered Entity or Business Associate to another person authorized to access Protected Health Information at the same Covered Entity or Business Associate, or organized health care arrangement in which the Covered Entity participates and the information received is not further Used or Disclosed in a manner not permitted; and
- a Disclosure of Protected where a Covered Entity or Business Associate has a good faith belief that an unauthorized person to whom the Disclosure was made would not reasonably have been able to retain such information.

Notification by a Business Associate:

- Business Associates shall notify the Provider of any Breach.
- A Breach is treated as discovered by a Business Associate as of the first day on which the Breach is known by the Business Associate or, by exercising reasonably diligence, would have been known by the Business Associate.
- A Business Associate is deemed as having knowledge of a Breach if the Breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the Breach, who is an employee, officer or other agent of the Business Associate.
- Notification shall be provided by the Business Associate without unreasonable delay and in no case later than 60 calendar days after discovery of a Breach.
- The notification shall include, to the extent possible, the identification of each Individual who's Unsecured Protected Health Information has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, used or Disclosed during the Breach. In addition, the Business Associate shall provide the Provider with any other available information that the Provider is required to include in notification to the Individual either at the time of notification or as promptly thereafter as information becomes available.

Administrative Requirements:

- Training: The Provider will train all Workforce members on these policies and procedures as necessary and appropriate for their functions within the Provider to be carried out and will do so within a reasonable time after any material change to these policies and procedures.
- Complaints: The Provider will provide a process for Individuals to make complaints concerning these policies and procedures or the Provider's compliance with such policies and procedures or the requirements of HIPAA.

- Sanctions: The Provider has and will apply appropriate sanctions against Workforce members who fail to comply with these policies and procedures or the requirements of HIPAA, up to and including termination.
- Refraining from Intimidating or Retaliatory Acts: The Provider will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any Individual for the exercise of any right established, or for participation in any process provided for, by HIPAA, including the filing of a complaint.
- Waiver of Rights: The Provider shall not require Individuals to waive their rights as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.
- Policies and Procedures: This policy and these procedures are intended to comply with HIPAA. The Provider will change these policies and procedures as necessary and appropriate to comply with changes in the law.
- Maintaining Documentation: The Provider shall maintain documentation sufficient to meet its burden of proof of compliance with the Breach notification requirements of HITECH/HIPAA.

XXX. SECURITY RULE DOCUMENTATION

The Provider will document all steps and actions taken to comply with the HIPAA Security Rule. Documentation will include:

- Risk analyses and assessments, including evaluation of whether an addressable implementation specification applies to the Provider.
- Security Incident Reports
- Audit Reports
- Business Associate Agreements
- Disposal/destruction of Electronic Media
- Records related to information system updates, Security modifications, software or hardware changes, etc.
- Workforce training and updates on Security
- All other records relating to steps taken by the Provider to comply with the Security Rule

Documentation will be maintained by the Security Officer or in the Provider's compliance file.

Documentation will be available to persons responsible for implementing the Provider's Security measures and policies.

Documentation will be reviewed by the Security Officer periodically and updated as needed, in response to operational, environmental, personnel, or administrative changes affecting the security of ePHI.

XXXI. DUTY OF WORKFORCE MEMBERS TO REPORT SECURITY BREACHES

Provider Policy:

It is the policy of the Provider to maintain compliance with the HIPAA Security Rule and require Workforce members to report all known or suspected security incidents and Breaches to the Security Officer, Privacy Officer, or Corporate Compliance Officer.

Workforce members should:

- Report any unauthorized persons Accessing the Provider's computers and electronic media.
- Not download or upload any unapproved software or files sent by e-mail without permission from the Security Officer.
- Be aware of Workforce, Individuals, visitors, and all other persons who are present in the Provider's offices, at all times.

HIPAA FORMS

FORMS
HIPAA Forms

Form No. 1: Notice of Privacy Practices & Acknowledgment
Form No. 2: Authorization
Form No. 3: Revocation of Authorization
Form No. 4: Request to Access, Inspect and Copy
Form No. 5: Accept Request to Access, Inspect and Copy Records
Form No. 6: Deny Request to Access, Inspect and Copy Records
Form No. 7: Request to Restrict Use and Disclosure
Form No. 8: Deny Request to Restrict Use and Disclosure
Form No. 9: Request to Terminate Restriction by Individual
Form No. 10: Notice to Terminate Restriction
Form No. 11: Request for Amendment of Records
Form No. 12: Accept Request to Amend Records
Form No. 13: Deny Request to Amend Records
Form No. 14: Statement of Disagreement
Form No. 15: Rebuttal Statement
Form No. 16: Request for Accounting of Disclosures
Form No. 17: Accept Request to Accounting of Disclosures
Form No. 18: Deny Request for Accounting of Disclosures
Form No. 19: Request to Receive Confidential Communications
Form No. 20: Deny Request to Receive Confidential Communications
Form No. 21: Concern or Complaint Form
Form No. 22: Complaint Record and Disposition
Form No. 23: Security Incident Report
Form No. 24: Business Associate Agreement
Form No. 25: Appointment of Personal Representative Form
Form No. 26: Workforce Training Certificate

FORM NO. 1: NOTICE OF PRIVACY PRACTICES AND ACKNOWLEDGMENT

HIPAA Notice of Privacy Practices
Ohio Eye Surgeons, Inc.

THIS NOTICE OF PRIVACY PRACTICES (THE "NOTICE") DESCRIBES HOW HEALTH INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW THIS NOTICE CAREFULLY.

This Notice applies to the Ohio Eye Surgeons, Inc. (OES). The purpose of this Notice is to describe how OES may use and disclose your protected health information ("PHI") in accordance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act") and the HIPAA Omnibus Final Rule (the "Final Rule"). This Notice also describes the obligations of OES with respect to your protected health information, describes how your protected health information may be used or disclosed to carry out treatment, payment or healthcare operations, and describes your rights to control and access your protected health information. OES has agreed to the provisions set forth in this Notice.

We are required to provide this Notice to you pursuant to HIPAA.

The HIPAA Privacy Rule protects only certain medical information known as "protected health information." Generally, protected health information is health information, including demographic information, collected from you or created or received by a health care provider, a health care clearinghouse, a health plan, or your employer on behalf of a group health plan, from which it is possible to individually identify you and that relates to:

(a) your past, present, or future physical or mental health or condition;

(b) the provision of health care to you; or

(c) the past, present, or future payment for the provision of health care to you.

1. Responsibilities of OES.

OES is required under HIPAA to maintain the privacy of your protected health information. Protected health information includes all individually identifiable health information transmitted or maintained by OES that relates to your past, present or future health, treatment or payment for health care services. OES must abide by the terms of this Notice, and must provide you with a copy of this Notice upon request.

2. How OES May Use and Disclose Your Protected Health Information.

The following categories describe the different situations in which OES is permitted or required to use or disclose your protected health information:

- **For Treatment**. OES may use or disclose your protected health information to facilitate medical treatment or services by providers. OES may disclose medical

information about you to providers, including doctors, nurses, technicians, medical students, or other hospital personnel who are involved in taking care of you.

- **For Payment Purposes**. OES has the right to use and disclose your protected health information to satisfy their responsibilities with respect to the billing and payment collected from you, an insurance company or a third party, for treatment and services you receive from OES. For example, OES may need to give your health plan information about therapy or nursing services you receive in order to receive reimbursement from your health plan for those services. OES may also tell your health plan about a treatment you are going to receive to obtain prior approval or to determine whether your plan will cover the treatment.
- **Health Care Operations**. OES has the right to use and disclose your protected health information to perform functions necessary for the operation of OES. For example, OES may use health care information to review Ohio Eye Surgeons, Inc.'s treatment and services and to evaluate the performance of our staff in caring for you. OES may combine health care information about many of our patients to decide what additional services we should offer, what services are not needed, and whether certain new treatments are effective. OES may also disclose information to doctors, nurses, therapists, technicians, aides, students and other OES personnel for review and learning purposes. OES may remove information that identifies you from the health care information so others may use it to study health care and health care delivery without learning the identity of any specific patient.
- **Appointment Reminders**. OES may use and disclose health care information to contact you as a reminder that you have an appointment with OES.
- **Treatment Alternatives**. OES may use and disclose health care information to tell you about or recommend possible treatment options or alternatives that may be of interest to you.
- **Health-Related Benefits and Services**. OES may use and disclose health care information to tell you about health-related benefits or services that may be of interest to you.
- **To the Individual**. OES may disclose protected health information, which you are the subject of, to you.
- **Individuals Involved in Your Care or Payment for Your Care**. OES may release health care information about you to a friend or family member who is involved in your health care. OES may also give information to someone who helps pay for your care. In addition, we may disclose health care information about you to an entity assisting in a disaster relief effort so that your family can be notified about your condition, status and location. This release requires written or oral consent from you.
- **Research**. Under certain circumstances, OES may use and disclose health care information about you for research purposes. For example, a research project may involve comparing the health and recovery of all parties who received one

type of treatment to those who received another for the same condition. All research projects, however, are subject to a special approval process. This process evaluates a proposed research project and its use of health care information, trying to balances the research needs with patients' need for privacy of their health care information. Before we use or disclose health care information for research, the project will be approved through this research approval process, but OES may, however, disclose health care information about you to people preparing to conduct a research project, for example, to help them look for patients with specific health care needs, so long as the health care information they review does not leave our control. We will almost always ask for your specific permission if the researcher will have access to your name, address or other information that reveals who you are, or will be involved in your care with us.

- **Business Associates**. OES may contract with certain service providers ("Business Associates") to perform various functions on behalf of OES. To provide these services, the Business Associates may receive, create, maintain, use or disclose protected health information. OES and each Business Associate will enter into, or have already entered into, an agreement requiring the Business Associate to safeguard your protected health information as required by law and in accordance with the terms of this Notice.

- **Required By Law**. OES may use or disclose your protected health information to the extent required by federal, state or local law. For example, OES may disclose your protected health information when required by national security laws or public health disclosure laws.

- **Lawsuits and Disputes**. OES may disclose your protected health information in response to a court or administrative order. Your protected health information may also be disclosed in response to a subpoena, discovery request or other lawful process if efforts have been made to tell you about the request or to obtain an order protecting your protected health information.

- **Certain Government Agencies and Officials**. OES may disclose your protected health information to (i) government agencies involved in oversight of the health care system, (ii) government authorities authorized to receive reports of abuse, neglect or domestic violence, (iii) law enforcement officials for law enforcement purposes, (iv) military command authorities, if you are or were a member of the armed forces, (v) correctional institutions, if you are an inmate or in under the custody of a law enforcement official and (vi) federal officials for intelligence, counterintelligence, and other national security activities.

- **Public Health and Research Activities; Medical Examiners**. OES may also disclose your protected health information (i) for public health activities or to prevent a serious threat to health and safety, (ii) to organizations that handle organ donations, if you are an organ donor, (iii) to coroners, medical examiners and

funeral directors as necessary, and (iv) to researchers, if certain conditions regarding the privacy of your protected health information have been met.

- **Workers' Compensation**. OES may disclose your protected health information to comply with workers' compensation laws and other similar programs that provide benefits for work-related injuries or illnesses.
- **Military and Veterans**. If you are a member of the armed forces, OES may release health care information about you as required by military command authorities. We may also release health care information about foreign military personnel to the appropriate foreign military authority.
- **Disclosures to the Secretary of the U.S. Department of Health and Human Services**. OES may be required to disclose your protected health information to the Secretary of the U.S. Department of Health and Human Services to investigate or determine OES's compliance with the HIPAA Privacy Rules.
- **Other Uses and Disclosures With Written Authorization**. Disclosures and uses of your protected health information that are not described above may be made by OES with your written authorization. If OES is authorized to use or disclose your protected health information, you may revoke that authorization, in writing, at any time, except to the extent that OES has taken action relying on the authorization. OES will not be able to take back any disclosures of your protected health information that have already been made with your authorization.

3. Your Rights With Respect to Your Protected Health Information.

The following summarizes your rights with respect to your protected health information:

- **Right to Request a Restriction on Uses and Disclosures of Protected Health Information.** You have the right to request a restriction or limitation on the protected health information used or disclosed about you by OES for treatment, payment or health care operations. You also have the right to request a limit on the disclosure of your protected health information to someone who is involved in your care or the payment for your care, such as a family member, friend or other person you have identified as responsible for your care. In your request, you must tell OES (i) what information you want to limit; (ii) whether you want to limit OES's use, disclosure, or both; and (iii) to whom you want the limits to apply, for example, disclosures to your spouse. OES will comply with any restriction request if (iv) except as otherwise required by law, the disclosure is to the health plan for purposes of carrying out payment or health care operations (and is not for purposes of carrying out treatment); and (v) the protected health information pertains solely to a health care item or service for which the health care provider involved has been paid out-of-pocket in full. If OES agrees to your request, OES will honor the restriction until you revoke it or we notify you.

- **Right to Request Confidential Communications**. You have the right to request that OES communicate with you about your protected health information in a certain way or at a certain location. For example, you can request that OES only contact you at work or by mail. OES will accommodate all reasonable requests.

- **Right to Inspect and Copy Your Protected Health Information**. You have the right to inspect and copy your protected health information. Under certain limited circumstances, we may deny your access to a portion of your records. For example, you do not have a right to inspect and copy psychotherapy notes or information that OES have collected in connection with, or in reasonable anticipation of, any legal claim or proceeding. If you request copies, we may charge you reasonable copying and mailing costs.

- **Right to Amend Your Protected Health Information**. You have the right to request an amendment of your protected health information that is maintained by OES if you believe that the information is inaccurate or incomplete. OES may deny your request if your protected health information is accurate and complete or if the law does not permit OES to amend the requested information. OES cannot amend information created by your doctor or any person other than OES.

- **Right to Receive an Accounting of Disclosures of Your Protected Health Information.** You have the right to request an accounting of disclosures OES has made of your protected health information during the six (6) years prior to the date of your request. However, you will not receive an accounting of (i) disclosures made to you, (ii) disclosures made pursuant to your authorization, (iii) disclosures for purposes of treatment, payment or health care operations and (iv) disclosures made to friends or family in your presence or because of an emergency. Certain other disclosures are also excluded from the HIPAA accounting requirements. If you request more than one accounting in any twelve (12) month period, OES will charge you a reasonable fee for each accounting after the first accounting statement.

- **Uses and Disclosures that Require Your Authorization**. The following uses and disclosures will be made by OES only with your authorization:

    - uses and disclosures for marketing purposes, including subsidized treatment communications;

    - uses and disclosures that constitute the sale of PHI;

    - if OES maintains psychotherapy notes, the use and disclosure of such notes will only be made upon the authorization from you; and

    - other uses and disclosures not described in this Notice.

You may revoke your authorization at any time, so long as the revocation is in writing. Once we receive your written revocation, it will only be effective for future uses and disclosures. It will not be effective for any information that may have been used or disclosed in reliance upon the written authorization and prior to receiving your written revocation.

- **Right to Opt-Out of Fundraising Communications**. If OES conducts or engages in fundraising communications, you shall have the right to opt-out of such fundraising communications.

- **Right to Receive a Paper Copy of this Notice**. You have the right to receive a paper copy of this Notice upon request, even if you agreed to receive this Notice electronically. To obtain a paper copy of this Notice, contact the Privacy Officer at 419-756-8000.

- **Right to Be Notified of a Breach**. You have the right to be notified in the event that OES (or a Business Associate) commits or discovers a breach of unsecured protected health information.

- **To Exercise Your Individual Rights**. To exercise any of your rights listed above, you must complete the appropriate form. To obtain the required form, please contact the Privacy Officer at 419-756-8000.

4. Filing a Complaint With OES or the U.S. Dept. of Health and Human Services.

If you believe that OES has violated your HIPAA privacy rights, you may complain to OES or to the Secretary of the U.S. Department of Health and Human Services. Complaints to OES should be sent to Attn: Privacy Officer, Ohio Eye Surgeons, Inc. 466 South Trimble Road Mansfield, Ohio 44906. Complaints to the Secretary should be sent to the U.S. Department of Health and Human Services, Hubert H. Humphrey Building, 200 Independence Ave. S.W., Washington, D.C. 20201. OES will not penalize you or retaliate against you for filing a complaint.

5. Changes to this Notice.

OES reserves the right to change the provisions of this Notice and to apply the changes to all protected health information received and maintained by OES. If OES makes a material change to this Notice, a revised version of this Notice will be provided to you within thirty (30) days of the effective date of the change at your address of record.

6. Effective Date.

This Notice has been effective since September 2013.

7. Contact Information.

If you have any questions regarding this Notice or would like to exercise any of your rights described in this Notice, please contact:

Ohio Eye Surgeons, Inc.
Attention: Privacy Officer
466 South Trimble Road
Mansfield, Ohio 44906
Telephone: 419-756-8000

Ohio Eye Surgeons, Inc.

Acknowledgment by Individual or Personal Representative of Receipt of Notice of Privacy Practices

I acknowledge receiving a copy of the Notice of Privacy Practices given to me by OES.

I understand this Notice explains how OES is permitted to Use and Disclose my Protected Health Information.

I understand I should keep the Notice and refer to it if I have questions. I also understand I should call the OES Privacy Officer at 419-756-8000 if I have a question or concern about my privacy rights.

_____
Print name of Individual

_____
(If applicable) Print name of Individual's Personal Representative and Relationship to Individual

_____
Signature by Individual or Individual's Personal Representative

_____
Date

OFFICE STAFF USE ONLY IF ACKNOWLEDGMENT NOT SIGNED

The following attempt(s) were made to obtain a written Acknowledgment of Receipt:

☐ NPP given to Individual, who refused to sign.

☐ NPP was mailed to Individual's home address as stated in records.

☐ NPP was mailed to an alternate address, at Individual's request.

☐ NPP was faxed or emailed to Individual, at Individual's request.

Other reason(s) why written acknowledgment not obtained: _____

_____

_____

_____ _____
Signature of Person attempting to obtain signed Acknowledgment Date

ORIGINAL MAINTAINED IN FILE

FORM NO. 2: AUTHORIZATION

Ohio Eye Surgeons, Inc.

AUTHORIZATION FOR DISCLOSURE OF PROTECTED HEALTH INFORMATION—KEEP IN FILE

1. **I authorize OES to Use or Disclose the following information from my medical record:**
   - □ My entire medical record
   - □ My medical records dated from _____ to _____
   - □ Protected Health Information relating to _____
     (Specify diagnosis, procedure, condition, injury, etc.)
   - □ Other (please explain): _____

2. **I authorize OES to Disclose my health information to:** _____

   Address: _____ City: _____ State: _____ Zip: _____
   Telephone: _____ Fax: _____

3. **Disclosure of my health information is being made for the purpose(s) of:**
   - □ At the request of the Individual or Individual's personal representative
   - □ Permission to return to work, sick note, or medical excuse
   - □ Insurance enrollment or coverage
   - □ Life insurance, automobile insurance or disability insurance claim
   - □ Employment purpose (please specify): _____
   - □ Other (please specify): _____

4. **Authorization for Disclosure of my health information will expire in 60 days or on:**
   - □ Please specify date: _____
   - □ Please specify event, if not a specific date: _____
   - □ Adjudication of claim

5. I understand that if the person or entity to whom OES is disclosing my information is not a doctor, health care provider or health plan, the information may not be protected by HIPAA, and that person may Use or Disclose that information to other non-covered entities. I understand that the information in my health record may include information relating to sexually transmitted diseases, acquired immunodeficiency syndrome (AIDS), or human immunodeficiency virus (HIV). It may also include information about behavioral or mental health services, and treatment for alcohol and drug abuse.

6. I understand that my refusal to sign this Authorization will not affect my ability to obtain treatment from OES It may affect my ability to return to work or receive an employee or insurance benefit.

7. I understand I have the right to inspect or copy information Disclosed by this Authorization. I understand I may revoke (cancel) this Authorization at any time. Revocation must be in writing. OES cannot be held responsible for having Disclosed information in reliance on this Authorization before receiving a written revocation.

8. I understand that OES and its Workforce are released from legal responsibility or liability for disclosing protected health information authorized by my signature below.

9. I acknowledge I had an opportunity to ask questions before I signed and that I may receive a copy of the signed Authorization.

_____ _____
Print Name of Individual or Individual's Personal Representative Date

_____ _____
Signature Individual's Date of Birth

FORM NO. 3: REVOCATION OF AUTHORIZATION

Ohio Eye Surgeons, Inc.

REVOCATION OF AUTHORIZATION

I revoke the Authorization that I gave to OES on _____, 20_____ for the Use or Disclosure of:

□ My entire medical/health record
□ My medical/health records dated from _____ to _____
□ Protected health information relating to _____
(Specify diagnosis, procedure, condition, injury, etc.)
□ Other (please explain): _____
_____

My medical/health information was to be Disclosed to:

Name/Organization: _____
Address: _____
City: _____State: _____Zip: _____
Telephone: _____
Fax: _____

The purpose of the Disclosure: _____

I understand that, by signing below, my protected health information will not be Disclosed to the Name/Organization specified above, except to the extent that OES has already Disclosed in reliance upon the Authorization that I had previously provided.

I further understand that if I authorized OES to Disclose my protected health information for the purpose of obtaining insurance coverage, other laws provide the insurer with the right to contest the policy itself or a claim under the policy.

_____
Print Name of Individual

_____
Signature

_____
Print Name of Individual's Representative
(if signing for the Individual)

_____
Date

FORM NO. 4: REQUEST TO ACCESS, INSPECT AND COPY PROTECTED HEALTH INFORMATION

Ohio Eye Surgeons, Inc.

REQUEST TO ACCESS, INSPECT & COPY PROTECTED HEALTH INFORMATION

As stated in our Notice of Privacy Practices, you may request access to and obtain a copy of your protected health information created and maintained by OES.

Under the HIPAA Privacy Rule, you may not be able to access protected health information that (1) is contained within Psychotherapy Notes; (2) is compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding; or (3) is prohibited from Disclosure under Federal or State law.

We will respond to your Request to Access within 30 days from the time we receive a fully-completed form. (We will contact you if your form is not complete, and ask you to re-submit the form.)

If we are able to grant your Request, we will contact you to set up an appointment for you to come to our office to access, inspect and copy your protected health information. You may be charged a fee for copies of your health information.

If we are unable to grant your Request, we will send you an explanation in writing, along with information regarding your right to review our denial of your Request.

****

By signing below, I request access to inspect and obtain a copy of my protected health information maintained by OES. I understand that this Request does not provide me the right to access, inspect or copy any of my protected health information that is prohibited from Disclosure by the Privacy Rule or other Federal or State law.

Describe the medical or health information that you wish to access, inspect or obtain a copy of:

_____

_____

_____ _____

Print Name Telephone

_____

Signature

_____

Print Name of Individual's Personal Representative
(if signing for Individual)

_____ _____

Date Date Request Received
(to be completed by OES)

FORM NO. 5: ACCEPT REQUEST TO ACCESS, INSPECT AND COPY RECORDS

Ohio Eye Surgeons, Inc.

RESPONSE TO REQUEST TO ACCESS, INSPECT AND COPY RECORDS

Date: _____

Dear _____,

As stated in our Notice of Privacy Practices, you may request access to and obtain a copy of your health information created and maintained by OES.

We have reviewed your Request to Access, Inspect and Copy your health information received by our office on _____, 20__.

We have agreed to your Request, either in whole or in part. If we did not agree to your entire request, you will receive another letter explaining our decision to deny access to part of your protected health information, along with an explanation of your rights for review.

We will contact you within one week to set up an appointment for you to access, inspect and copy your medical records. You cannot make changes in your original record.

Please note that State law allows us to charge certain fees for providing copies of medical records. You may be charged for copies of your medical records in accordance with State law. If applicable, we may ask you to pay copy charges in advance. We may also charge you for postage costs to mail copies of your medical records to you.

Please call the Privacy Officer at 419-756-8000 if you have any questions. You can also refer to our Notice of Privacy Practices for additional information on your right to access, inspect and copy your protected health information.

Sincerely,

_____
Signature

_____
Name

_____
Title

FORM NO. 6: DENY REQUEST TO ACCESS, INSPECT AND COPY RECORDS

Ohio Eye Surgeons, Inc.

RESPONSE TO REQUEST TO ACCESS, INSPECT AND COPY RECORDS

Date: _____

Dear _____,

As stated in our Notice of Privacy Practices, you may request access to and obtain a copy of your health information created and maintained by OES.

We have reviewed your Request to Access, Inspect and Copy Records received by our office on _____, 20_____.

At this time, we cannot honor your request because:

- ☐ Your request involves information compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding.

- ☐ Your request involves information prohibited from Disclosure by Federal or State law. Disclosure is prohibited by: _____
  _____
- ☐ _____
  _____

- ☐ Your request involves Disclosure of information that a licensed health care professional has determined, in the exercise of professional judgment, is reasonably likely to endanger the life or physical safety of you or another person.

- ☐ Other: _____
- ☐ _____
- ☐ _____
- ☐ _____

You have a right to review our denial of your Request to Access, Inspect and Copy Records. You may request a review of our denial if our decision involved the exercise of professional judgment by a physician or other health care provider, or if the Disclosure was not expressly prohibited by law.

Please call the Privacy Officer at 419-756-8000 to inform us if you would like a review of our denial of your Request to Access, Inspect and Copy Records. The review of our denial will be conducted by a licensed health care professional who was not involved in our decision to deny you access. We will provide you with the determination of the reviewing professional within thirty (30) days after being notified of your request for a review.

You may also file a complaint with us for an internal review of our decision as described in our Notice of Privacy Practices. Please call the Privacy Officer at 419-756-8000 to file a complaint. You may also contact the Secretary, U.S. Department of Health and Human Services, to request an external review of our decision to deny access.

Please also refer to our Notice of Privacy Practices for information on your right to access, inspect and copy your health information and medical records.

Sincerely,

_____

Signature

_____

Name

_____

Title

FORM NO. 7: REQUEST TO RESTRICT USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION

Ohio Eye Surgeons, Inc.

REQUEST TO RESTRICT USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION

As stated in our Notice of Privacy Practices, you may request OES to restrict the Use and Disclosure of your health information for certain treatment, payment and health care operations.

You may also restrict us from communicating your health information to family members, friends or other persons involved in your care.

HIPAA's Privacy Rule, however, gives us the right to deny all or part your request to restrict the Use and Disclosure of your health information. Please see our Notice of Privacy Practices for details.

If we are able to grant your Request, we will make the appropriate notation in your file to inform all persons involved in your care that you have requested health information to be restricted from certain Uses and Disclosures.

If we are unable to grant your Request, we will send you an explanation in writing.

Please FULLY EXPLAIN your request to restrict the Use and Disclosure of your health information:

_____

_____

_____

Please specify the person, entity or organization that you DO NOT want your health information Disclosed to:

_____

_____

_____

_____ _____

Print Name of Individual Telephone

_____

Signature

_____

Print Name of Individual's Personal Representative (if signing for Individual)

_____ _____

Date of Request Date Request Received
(to be completed by OES)

FORM NO. 8: DENY REQUEST TO RESTRICT USE AND DISCLOSURE

Ohio Eye Surgeons, Inc.

REQUEST TO RESTRICT USE AND DISCLOSURE

Date: _____

Dear _____ ,

As stated in our Notice of Privacy Practices, you may request OES to restrict the Use and Disclosure of your health information for treatment, payment and health care operations. You may also restrict us from notifying family members, friends and other persons about your health information. The Privacy Rule, however, gives us the right to deny all or part your Request to Restrict the Use and Disclosure of your health information.

We received your Request to Restrict Use and Disclosure of your health information on _____, 20 _____.

You requested that we restrict the Use and Disclosure of your health information in the following manner: _____
_____
_____

At this time, we cannot honor your request because:
_____
_____
_____
_____

Please contact the Privacy Officer at 419-756-8000 if you have questions about our denial of your request.

You can also refer to our Notice of Privacy Practices for information about your right to restrict Use and Disclosure of your health information.

Sincerely,

_____
Signature

_____
Name

_____
Title

FORM NO. 9: REQUEST TO TERMINATE RESTRICTION BY INDIVIDUAL

Ohio Eye Surgeons, Inc.

REQUEST TO TERMINATE THE REQUESTED RESTRICTION ON USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION

I, _____, request that OES terminate all or part of my requested restriction on the Use and Disclosure of my protected health information.

Please FULLY EXPLAIN your request to terminate the restriction on the Use and Disclosure of your health information:

_____
_____
_____
_____
_____
_____

Please specify when you want the restriction to terminate:

- ☐ Immediately
- ☐ On this date: _____
- ☐ After this event: _____

_____ _____
Print Name of Individual Telephone

_____
Signature

_____
Print Name of Individual's Personal Representative (if signing for Individual)

_____ _____
Date Date Request Received
(to be completed by OES)

FORM NO. 10: NOTICE TO TERMINATE RESTRICTION

Ohio Eye Surgeons, Inc.

NOTICE TERMINATING RESTRICTION ON USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION

Date: _____

By Certified Mail

Dear _____ ,

As stated in our Notice of Privacy Practices, you may request OES to restrict the Use and Disclosure of your health information for treatment, payment and health care operations.

We agreed to your Request to Restrict the Use and Disclosure of your health information in the following manner: _____

_____

At this time, we ask you to terminate this restriction because:

_____

_____

The termination of your restriction is only effective with respect to health information created or received by us after the date that you receive this letter.

If you agree to have your restriction terminated, for the reasons stated above, please sign below:

_____ _____

Signature of Individual or Individual's Personal Representative Relationship

Please return the signed copy of this letter to us in the enclosed envelope. Retain the second copy for your files.

Please contact the Privacy Officer at 419-756-8000 if you have any questions.

Sincerely,

_____

Signature

_____

Name

_____

Title

FORM NO. 11: REQUEST FOR AMENDMENT OF RECORDS

Ohio Eye Surgeons, Inc.

REQUEST TO AMEND PROTECTED HEALTH INFORMATION

As stated in our Notice of Privacy Practices, you may request OES to amend incorrect or incomplete facts in the protected health information that we created and maintain about you, for as long as the information is maintained by us. Please see our Notice of Privacy Practices for details.

After you have fully completed and submitted this form, we will respond to your Request to Amend within 60 days from the time we receive your completed form.

If we are able to grant your Request, either in whole or in part, we will make the appropriate amendment to your health information. We will then notify you about the amendment, as well as ask you to identify all relevant persons (such as physicians, schools, employers, etc.) that we should notify about the amendment.

If we are unable to grant your Request, we will send you an explanation in writing, along with information regarding your right to a review of our denial of your Request and to submit a Statement of Disagreement.

Please EXPLAIN your request to amend your health information. Be sure to PROVIDE DETAILS, such as dates of treatment, diagnosis, testing performed, etc.:

_____
_____
_____
_____
_____
_____
_____
_____

_____ _____
Print Name Telephone

_____
Signature

_____
Print Name of Individual's Personal Representative
(if signing for Individual)

_____ _____
Date Date Request Received
(to be completed by OES)

FORM NO. 12: ACCEPT REQUEST TO AMEND RECORDS IDENTIFICATION OF PERSONS TO BE NOTIFIED

Ohio Eye Surgeons, Inc.

RESPONSE TO REQUEST TO AMEND RECORDS

Date: _____

Dear _____,

As stated in our Notice of Privacy Practices, you may request OES to amend incorrect or incomplete facts in your protected health information that we created or maintain.

We received your Request to Amend your health information on _____, 20_____.

You requested that we make the following correction, change or amendment to your protected health information:

_____

_____

_____

We have reviewed your request, and the following amendment will be made to your protected health information:

_____

_____

_____

_____

Enclosed with this letter is a form for you to identify all persons (such as physicians, hospitals, employers, organizations, etc.) that should receive a copy of your amended protected health information. Please fill out this form completely and mail it to us as soon as possible. We will then make a reasonable effort to notify the persons and entities identified by you, in addition to those persons and entities identified by us, about the amendment to your protected health information.

Please contact the Privacy Officer at 419-756-8000 if you have questions.

Sincerely,

_____

Signature

_____

Name

_____

Title

Ohio Eye Surgeons, Inc.

IDENTIFICATION OF PERSONS TO BE NOTIFIED

The HIPAA Privacy Rule requires us to notify all persons, such as health care providers, insurers, employers, etc., of any amendment made to your protected health information. Please identify all persons who should be notified of this amendment.

Please list each person (including hospitals, physicians, employers, organizations, agencies or companies) and include a complete address and telephone number. Be sure to include all persons who may have received the previously incorrect or incomplete facts in your protected health information and who should be notified of the amendment.

Please print legibly. Use the back of this sheet if necessary.

Individual Name:_____

Name of Person or Entity to be Notified of Amendment	**Address**	**Telephone**

Please send completed form to:
Ohio Eye Surgeons, Inc.
Attn: Privacy Officer
466 South Trimble Road
Mansfield, Ohio 44906

FORM NO. 13: RESPONSE TO REQUEST TO AMEND RECORDS

Ohio Eye Surgeons, Inc.

RESPONSE TO REQUEST TO AMEND RECORDS

Date: _____

Dear _____,

As stated in our Notice of Privacy Practices, you may request OES to amend incorrect or incomplete facts in your protected health information that we created or maintain.

We received your Request to Amend your health information on _____, 20____.

You requested us to make the following amendment to your health information:

_____

_____

After carefully considering the explanation you provided, we cannot honor your request at this time because:

☐ Your request involves health information that was not created by us. If you believe that this health information cannot be amended by the original source, please contact our Privacy Officer at 419-756-8000. Please see our Notice of Privacy Practices.

☐ Your request to amend involves health information that we cannot provide to you under either Federal or State law. Specifically, _____

☐ _____

☐ _____

☐ Your request involves health information that we have determined to be accurate and complete.

☐ Other: _____

☐ _____

☐ _____

You have a right to disagree with our decision to deny your Request to Amend your health information. You may submit a Statement of Disagreement, included with this letter, to explain why you believe that our decision to deny your request is incorrect or inaccurate.

If you disagree with our decision, but do not file the Statement of Disagreement, you may request us to provide your Request to Amend and this denial letter with any and all future Disclosures of the health information that is the subject of the requested amendment.

You may also file a complaint with us for an internal review of our decision to deny the amendment as described in our Notice of Privacy Practices. Please contact the Provider Manager to file a complaint.

You may also contact the Secretary, U.S. Department of Health and Human Services to request an external review of our decision to deny the amendment of your health information.

Please call the Privacy Officer at 419-756-8000 if you have any questions. You can also refer to our Notice of Privacy Practices for information on the right to amend your health information.

Sincerely,

_____
Signature

_____
Name

_____
Title

FORM NO. 14: STATEMENT OF DISAGREEMENT

Ohio Eye Surgeons, Inc.

STATEMENT OF DISAGREEMENT

Under HIPAA's Privacy Rule, you have a right to disagree with OES's decision to deny all or part of your Request to Amend protected health information. You may submit this Statement of Disagreement to explain why you believe our decision is improper or in error.

Your Statement of Disagreement will be attached or linked to the disputed protected health information, along with our Statement of Rebuttal (if any), your Request to Amend, and our denial letter.

I, _____, disagree with the decision to deny my Request to Amend my protected health information because (use the back of this sheet, if necessary):

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

_____ _____
Signature Date

_____
Address

_____
Telephone

Please send your completed Statement of Disagreement to:
Attn: Ohio Eye Surgeons, Inc.
Attn: Privacy Officer
466 South Trimble Road
Mansfield, Ohio 44906

FORM NO. 15: REBUTTAL STATEMENT

Ohio Eye Surgeons, Inc.

Date: _____

RE: Statement of Rebuttal

Dear _____,

Under HIPAA's Privacy Rule, OES may prepare a written rebuttal to support the denial of your request to amend protected health information, in response to a Statement of Disagreement.

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

This Statement of Rebuttal will be attached or linked to the disputed protected health information, along with your Statement of Disagreement, your Request to Amend, and our denial letter.

Please contact me if you have any questions.

Sincerely,

_____
Signature

_____
Name

_____
Title

FORM NO. 16: REQUEST FOR ACCOUNTING OF DISCLOSURES

Ohio Eye Surgeons, Inc.

REQUEST FOR AN ACCOUNTING OF DISCLOSURES OF PROTECTED HEALTH INFORMATION

As stated in our Notice of Privacy Practices, you have the right to request an Accounting of Disclosures of your protected health information made by OES.

Please note that we cannot provide an Accounting of: (1) Disclosures made for treatment, payment, and health care operations; (2) Disclosures made to you or on your behalf to a personal representative; (3) Disclosures made pursuant to an Authorization; (4) Disclosures made more than 6 years ago.

After you have fully completed and submitted this form, we will respond to your request within 60 days from the time we receive the form.

You will not be charged for your first Request for an Accounting in a 12-month period.

You will be charged for any additional Requests for an Accounting that occur within the same 12-month period.

☐ **I am requesting a complete Accounting of Disclosures of my protected health information.**

☐ **I am requesting an Accounting of Disclosures of my protected health information for the time period indicated below:**

Beginning Date (month/day/year): _____

Ending Date (month/day/year): _____

_____ _____

Print Name Telephone

_____

Signature

_____

Print Name of Individual's Personal Representative
(if signing for Individual)

_____ _____

Date Date Request Received
(to be completed by OES)

FORM NO. 17: ACCEPT REQUEST TO ACCOUNTING OF DISCLOSURES

Ohio Eye Surgeons, Inc.

RESPONSE TO REQUEST FOR AN ACCOUNTING

Date: _____

Dear _____ ,

As stated in our Notice of Privacy Practices, you have the right to request an Accounting of Disclosures of your protected health information made by OES.

We have reviewed your Request for an Accounting form received by our office on _____, 20____.

You requested:

- ☐ A complete Accounting of Disclosures of your protected health information.

- ☐ An Accounting of Disclosures of your protected health information for the time period indicated below:

  Beginning Date (month/day/year): _____
  Ending Date (month/day/year): _____

☐ Enclosed you will find the results of your Request. Because this was your first Request for an Accounting in a 12-month period, you will not be charged for the Accounting.

OR

☐ Because this was not your first Request for an Accounting of Disclosures in a 12-month period, we must charge you $ _____ for your request. Please send a check or money order for this amount, payable to OES. Upon receipt of your check or money order, we will send you the results of the Accounting.

Please contact the Privacy Officer at 419-756-8000 if you have any questions.

Sincerely,

_____
Signature

_____
Name

_____
Title

FORM NO. 18: RESPONSE TO REQUEST FOR AN ACCOUNTING

Ohio Eye Surgeons, Inc.

RESPONSE TO REQUEST FOR AN ACCOUNTING

Date: _____

Dear _____ ,

As stated in our Notice of Privacy Practices, you have the right to request an Accounting of Disclosures of your protected health information made by OES.

We have reviewed your Request for an Accounting of Disclosures form received by our office on _____ , 20 ____. At this time, we cannot honor your request because:

☐ You have requested an Accounting of Disclosures made for treatment, payment and health care operations. As stated in our Notice of Policy Practices, we are not required to track such uses and Disclosures of your protected health information.

☐ You have requested an Accounting of Disclosures previously made to you or on your behalf to a personal representative within the last 12 months, on _____, and you did not provide payment in the amount of $ ___ per page to cover your request. As stated in our Notice of Privacy Practices, we are not required to provide you an accounting of Disclosure under these circumstances.

☐ You have requested an Accounting of Disclosures made pursuant to an Authorization. As stated in our Notice of Privacy Practices, we are not required to track such Uses and Disclosures of your protected health information.

☐ You have requested an Accounting of Disclosures made more than 6 years ago. As stated in our Notice of Privacy Practices, we are not required to track such Uses and Disclosures of your protected health information.

☐ Other: _____

Please contact the Privacy Officer at 419-756-8000 if you have any questions.

Sincerely,

_____
Signature

_____
Name

_____
Title

FORM NO. 19: REQUEST TO RECEIVE CONFIDENTIAL COMMUNICATIONS

Ohio Eye Surgeons, Inc.

REQUEST TO RECEIVE CONFIDENTIAL COMMUNICATIONS AT AN ALTERNATIVE LOCATION OR BY ALTERNATIVE MEANS

As stated in our Notice of Privacy Practices, you may request OES to communicate confidential protected health information to you at an alternative location or by an alternative means. The HIPAA Privacy Rule requires us to accommodate your request(s), if reasonable. **Please indicate your request regarding the communication of protected health information to you:**

☐ Please do not call my home telephone number with confidential information.

☐ Please do not call my work telephone number with confidential information.

☐ Please do not leave messages on my telephone answering machine.

☐ If a telephone call is required, please use this number: _____

☐ Please do not send confidential communications to my home address.

☐ Please do not send confidential communications to my work address.

☐ Please use this address to send confidential communications: _____
☐ _____

☐ Please do not send confidential communications to my email address.

☐ Other (please explain): _____
☐ _____

If your Request involves billing information, please explain:

_____
_____

_____
Print Name

_____
Signature

_____ _____
Print Name of Individual's Personal Representative (if signing for Individual) | Date Request Received (to be completed by OES)

_____
Date

FORM NO. 20: RESPONSE TO REQUEST TO RECEIVE CONFIDENTIAL COMMUNICATIONS

Ohio Eye Surgeons, Inc.

RESPONSE TO REQUEST TO RECEIVE CONFIDENTIAL COMMUNICATIONS

Date: _____

Dear _____,

As stated on our Notice of Privacy Practices, you may request OES to communicate confidential health information to you by an alternative means or in an alternative location. The Privacy Rule requires us to accommodate your request(s), if reasonable.

We received your Request to Receive Confidential Communications of your health information on _____, 20_____.

You requested: _____
_____
_____

At this time, we cannot honor your request because _____
_____
_____
_____
_____

Since we recognize the importance of your privacy, we are willing to work with you to find another alternative means or location for you to receive confidential communications about your health information.

Please contact the Privacy Officer at 419-756-8000 if you would like us to help you find an alternative means or location to communicate with you about your health information, or if you have any questions about our inability to honor your request.

Sincerely,

_____
Signature

_____
Name

_____
Title

FORM NO. 21: CONCERN OR COMPLAINT FORM

Ohio Eye Surgeons, Inc.

CONFIDENTIAL HIPAA QUESTION OR COMPLAINT FORM

Please let us know immediately if you have a question, concern or complaint about our Privacy Practices and your legal rights.

Please complete this form, mark the envelope "Confidential" and send it to the attention of the Privacy Officer, Ohio Eye Surgeons, Inc.

If you prefer to discuss your questions, concerns or complaint, please call the Privacy Officer, at 419-756-8000 during our normal corporate business hours.

What is your Privacy question, concern or complaint?

_____

_____

_____

If you believe your privacy rights have been violated, when do you believe this violation occurred? _____

Is there a particular person who you believe violated your privacy rights? If so, please identify, either by name or by job description: _____

_____

It is not necessary for you to give us your name, telephone number or address. However, we encourage you to include this information, so we may give you an answer or give you direct feedback in resolving your concern or complaint. We appreciate your bringing any problems to our attention and will never "retaliate" against you for expressing a concern or complaint.

_____

Name

_____

Address Telephone

We promise to address all questions and investigate all concerns and complaints promptly.

Do you prefer for us to send you a written response or call you? Please provide address and/or phone number. _____

We believe in the confidentiality and proper Use and Disclosure of your health information.

We pledge to resolve concerns and complaints to your satisfaction.
Thank you for your cooperation.

FORM NO. 22: COMPLAINT RECORD AND DISPOSITION

COMPLAINT RECORD AND DISPOSITION

Date Complaint Received: _____

Nature of the question, concern or complaint _____
_____
_____
_____

Date when violation allegedly occurred _____

Person(s) who allegedly violated the Individual's privacy rights _____
_____
_____

Investigation steps, including documents reviewed and persons interviewed _____
_____
_____
_____
_____

Disposition: Violation _____ No violation_____

If violation, Corrective Action or Discipline taken _____
_____
_____
_____
_____
_____

Should Privacy Practices be revised to prevent the same or similar recurrences: Yes____ No__

Feedback to Individual/Individual: Date_____ Written _____ Oral _____

Did the Individual/Individual appear satisfied? Yes _____ No _____

Is there a reasonable expectation the Individual may file a complaint with the Office of Civil Rights?

Yes_____ No _____

Signature of person completing this form: _____

FORM NO. 23: SECURITY INCIDENT REPORT

SECURITY INCIDENT REPORT FORM

Date:_____ Location:_____

*Name:_____ *Position:_____

*Phone Number:_____ *Supervisor:_____

Incident
Description of incident (including number of patients affected):_____

_____

_____

_____

_____

Is this incident likely to compromise the privacy or security of the PHI at issue? _____

The following is to be completed by Security Officer or his/her designee.

Date reviewed by Security Officer:_____

Action taken:_____

_____

_____

_____

Follow-up:_____

_____

_____

_____

_____

FORM NO. 24: BUSINESS ASSOCIATE AGREEMENT

OHIO EYE SURGEONS, INC.
BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("Agreement") is entered into by and between Ohio Eye Surgeons, Inc. ("Covered Entity") and _____ ("Business Associate"), effective as of _____, 20__ ("Effective Date").

RECITALS

Ohio Eye Surgeons, Inc. is a "Covered Entity" as that term is defined under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the HIPAA administrative simplification regulations, 45 C.F.R. Parts 160 and Part 164, Subparts A, C and E (Subpart E, together with the definitions in Subpart A is known as the "Standards for Privacy of Individually Identifiable Health Information" (the "Privacy Rule") and Subpart C, together with the definitions in Subpart A, is known as the "Security Standards for the Protection of Electronic Protected Health Information" (the "Security Rule") (the Privacy Rule and the Security Rule are collectively called the "Privacy and Security Rules").

In connection with Business Associate's provision of services to Covered Entity, Covered Entity discloses to Business Associate "Protected Health Information" ("PHI"), including "Electronic Protected Health Information" ("ePHI"), as defined in 45 C.F.R. §160.103. Such disclosure results in Business Associate's use, disclosure, maintenance and/or creation of PHI, including ePHI, on behalf of Covered Entity.

Business Associate's provision of services to Covered Entity, when coupled with Covered Entity's disclosure of PHI to Business Associate, makes Business Associate a "business associate" of Covered Entity, as the term is defined in as defined in 45 C.F.R. §160.103.

The purpose of this Agreement is to comply with the requirements of the Privacy and Security Rules, including, but not limited to, the Business Associate Agreement requirements at 45 C.F.R. §§ 164.314(a) and 164.504(e), and to satisfy the provisions of the Health Information Technology for Economic and Clinical Health Act, set forth in Division A, Title XIII, of the American Recovery and Reinvestment Act of 2009, and its implementing regulations and guidance (collectively, "HITECH"), including the Final Omnibus Rule, that: (i) affect the relationship between a Business Associate and a Covered Entity and which under HITECH require amendments to the Business Associate Agreement; and (ii) enable Covered Entity to comply with HITECH's requirements to notify affected individuals in the event of a Breach of Unsecured Protected Health Information.

Covered Entity's disclosure of PHI to Business Associate, and Business Associate's use, disclosure and creation of PHI for or on behalf of Covered Entity, is subject to protection and regulation under the Privacy Rule. To the extent such use, disclosure or creation involves ePHI, such ePHI is subject to protection and regulation under the Security Rule. Business Associate acknowledges it shall comply with the Privacy and Security Rules regarding the use and disclosure of PHI and ePHI, pursuant to this Agreement and when and as required by HITECH and its implementing regulations.

Therefore, Covered Entity and Business Associate agree as follows:

1. Definitions.

(a) Unless otherwise provided in this Agreement, capitalized terms have the same meanings as set forth in the Privacy Rule, Security Rule, and HITECH.

(b) "PHI" means "Protected Health Information," as that term is defined in the Privacy and Security Rules. "ePHI" means "Electronic Protected Health Information," as that term is defined in the Privacy and Security Rules. PHI includes PHI that is ePHI as well as PHI that does not constitute ePHI.

(c) "Unsecured PHI" or "Unsecured Protected Health Information" includes PHI in any form that is not secured through use of a technology or methodology specified in HITECH, those being: (1) encryption for ePHI in accordance with the appropriate NIST standards for data at rest and in transit; or (2) destruction for other forms of PHI.

2. Scope of Uses and Disclosures by Business Associate.

(a) In General. Except as otherwise limited in this Agreement or by law, Business Associate may use or disclose PHI provided to Business Associate by Covered Entity to perform the functions, activities, or services for or on behalf of Covered Entity that are specified in the Underlying Agreement, provided that such uses or disclosures would not violate the Privacy Rule if done by a Covered Entity or the Minimum Necessary policies and procedures of Business Associate.

(b) Use of PHI. Except as otherwise limited in this Agreement or by law, Business Associate may use PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate.

(c) Disclosure of PHI. Except as otherwise limited in this Agreement or by law, Business Associate may disclose PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate, provided that disclosures are required by law, or Business Associate obtains reasonable assurances, in writing, from the person to whom the information is disclosed that it will remain confidential and be used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies Business Associate, in writing, within five (5) business days, of any instances of which it is aware in which the confidentiality of the information has been breached.

(d) Data Aggregation. Except as otherwise limited in this Agreement or by law, Business Associate may use PHI to provide Data Aggregation services to Covered Entity as permitted by 45 CFR § 164.504(e)(2)(i)(B).

(e) Limitation on Use and Disclosure of PHI. With regard to its use and/or disclosure of PHI necessary to perform its obligations to Covered Entity, Business Associate

agrees to limit disclosures of PHI to the Minimum Necessary (as defined in the Privacy Rule, as modified by HITECH and implementing regulations) to accomplish the intended purpose of the use, disclosure or request, respectively, whenever the Privacy Rule limits the use or disclosure in question to the Minimum Necessary.

(f) Limitation on Remuneration for PHI. With regard to its use and/or disclosure of PHI necessary to perform its obligations to Covered Entity and to comply with HITECH, Business Associate agrees not to receive direct or indirect remuneration for any exchange of PHI not otherwise authorized under HITECH without individual authorization, unless (i) specifically required for the provision of services under the Underlying Agreement (ii) for treatment purposes; (iii) providing the individual with a copy of his or her PHI; or (iv) otherwise determined by the Secretary in regulations.

(g) Reporting Violation of Law. Business Associate may use PHI to report a violation of law to appropriate Federal and/or State authorities, consistent with 45 CFR §164.502(j)(1).

3. Obligations of Business Associate.

(a) In General. Business Associate shall use or further disclose PHI only as permitted or required by this Agreement or as required by law.

(b) Safeguards. Business Associate shall use reasonable and appropriate safeguards to prevent use or disclosure of PHI other than as specifically authorized by this Agreement. Such safeguards shall at a minimum include: (i) a comprehensive written information privacy and security policy addressing the requirements of the Privacy and Security Rules, as amended by HITECH, that are directly applicable to Business Associate; and (ii) periodic and mandatory privacy and security training and HIPAA compliance awareness for members of Business Associate's Workforce.

(c) Mitigation. Business Associate shall mitigate any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate that violates the requirements of this Agreement or applicable law.

(d) Reporting. Business Associate shall report to Covered Entity any use or disclosure of PHI that is not sanctioned by this Agreement of which Business Associate becomes aware within five (5) business days.

(e) Subcontractors. Business Associate shall require subcontractors or agents to whom Business Associate provides PHI to agree, in writing, to comply with the Privacy and Security Rules, as amended by HITECH, to the same extent Business Associate is required to comply.

(f) Inspection by Secretary. Business Associate shall make available to the Secretary of Health and Human Services Business Associate's internal practices, books and

records relating to the use and disclosure of PHI for purposes of determining Covered Entity and Business Associate's compliance with the Privacy and Security Rules and HITECH, subject to any applicable legal privileges.

(g) Accounting of Disclosures of PHI. Business Associate shall document disclosures of PHI and information related to those disclosures necessary to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with the Privacy Rule, when and as required by HITECH, and provide to Covered Entity, and in the time and manner it reasonably specifies but in no case longer than five (5) business days, the information necessary to make an accounting of disclosures of PHI about an Individual. If PHI is maintained in an Electronic Health Record ("EHR"), Business Associate shall document and maintain documentation of such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures in an EHR, when and as required by HITECH.

(h) Access to PHI. Business Associate shall provide to Covered Entity, at Covered Entity's request and in the time and manner it reasonably specifies but in no case longer than ten (10) business days, PHI necessary to respond to Individuals' requests for access to PHI about them, in the event that the PHI in Business Associate's possession constitutes a Designated Record Set. If PHI is maintained in an Electronic Health Record, Business Associate shall provide access electronically, upon reasonable request of Covered Entity, when and as required by HITECH.

(i) Amendment to PHI. Business Associate shall, upon receipt of notice from Covered Entity but in no case longer than ten (10) business days, incorporate any amendments or corrections to the PHI in accordance with the Privacy Rule, in the event that the PHI in Business Associate's possession constitutes a Designated Record Set.

(j) Security of PHI. Business Associate shall, as described in HITECH Act §13401, comply with 45 CFR §§ 164.308, 164.310, 164.312, and 164.316 of the Security Rule and acknowledges that such provisions apply to Business Associate in the same manner that they apply to Covered Entity. Therefore, Business Associate agrees that it is required to maintain appropriate and reasonable administrative, physical, and technical safeguards, including documentation of the same, so as to ensure that PHI is not used or disclosed other than as provided by this Agreement or as required by law, including the following:

(i) Administrative safeguards (implementation of policies and procedures to prevent, detect, contain, and correct security violations; conducting and documentation of risk analysis and risk management);

(ii) Physical safeguards (implementation of policies and procedures to limit physical access to PHI or ePHI or electronic information systems and related facilities);

(iii) Technical safeguards (implementation of policies and procedures creating and tracking unique user identification, authentication processes, and transmission security, which may include encryption);

(iv) Policies and procedures to reasonably and appropriately document the foregoing safeguards as required by the Security Rule; and

(v) Ensuring that any agent, including any subcontractor, to whom Business Associate provides ePHI agrees, in writing, to comply with these administrative, physical, and technical safeguards, as well as the policies, procedures, and document requirements contained within the Security Rule.

(k) Civil and Criminal Liability. Business Associate acknowledges that it shall be liable under the civil and criminal enforcement provisions set forth at 42 USC §§1320d-5 and 1320d-6, as amended from time to time, for failure to comply with any use or disclosure requirements of this Agreement with respect to PHI and for failure to comply with its direct obligations under the Privacy and Security Rules and HITECH.

(l) Notification of Security Incidents and Breach of Unsecured PHI. Business Associate shall immediately, but in no case longer than five (5) business days following discovery, notify Covered Entity of any actual or suspected Security Incident or Breach of Unsecured Protected Health Information. The notice shall include: (i) the identification of each Individual whose PHI or Unsecured PHI has been or is reasonably believed by Business Associate to have been accessed, acquired, used or disclosed during the Security Incident or Breach, (ii) a brief description of what happened, including the date of the Security Incident or Breach and the date of the discovery of the Security Incident or Breach, (iii) a description of the types of PHI or Unsecured PHI that were involved in the Security Incident or Breach, (iv) any preliminary steps taken to mitigate the damage, and (v) a description of any investigatory steps taken. In addition, Business Associate shall provide any additional information reasonably requested by Covered Entity for purposes of investigating a Breach of Unsecured PHI. A Breach shall be treated as discovered by Business Associate as of the first day on which the Breach is known to Business Associate (including any person, other than the Individual committing the Breach, that is an employee, officer, or other agent of Business Associate) or should reasonably have been known to Business Associate to have occurred. Covered Entity shall have the sole right to determine, with respect to a Breach: (i) whether notice is to be provided to Individuals, regulators, law enforcement agencies, consumer reporting agencies, media outlets and/or the Department of Health and Human Services, or others as required by law or regulation, in Covered Entity's discretion; and (ii) the contents of such notice, whether any type of remediation may be offered to Individuals affected, and the nature and extent of any such remediation. The provision of the notices to affected Individuals, and any remediation which Covered Entity determines is

required or reasonably necessary, shall be at Business Associate's sole cost and expense.

4. Obligations of Covered Entity.

(a) Limitation in Notice of Privacy Practices. Covered Entity will notify Business Associate of any limitation in Covered Entity's Notice of Privacy Practices in accordance with the Privacy Rule, to the extent that the limitation may affect Business Associate's use or disclosure of PHI.

(b) Changes in Permission by Individual. Covered Entity will notify Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose PHI to the extent that the change may affect Business Associate's use or disclosure of PHI.

(c) Restriction on Use/Disclosure of PHI. Covered Entity will notify Business Associate of any restriction on the use or disclosure of PHI that has been agreed to with an Individual and any restrictions on marketing or fundraising to the extent that the restriction may affect Business Associate's use or disclosure of PHI.

(d) Permitted by the Privacy Rule or HITECH. Covered Entity will not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule or HITECH if done by a Covered Entity, except to the extent Business Associate will use or disclose PHI for, and this Agreement includes provisions for, Data Aggregation by or management, administrative, and legal activities of Business Associate.

5. Term and Termination.

(a) Term of the Agreement. The term of this Agreement begins on the Effective Date and ends when the entire PHI provided to Business Associate by Covered Entity, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity. To the extent it is infeasible for Business Associate to return or destroy the PHI, upon the agreement of Covered Entity; protections shall be extended to that PHI in accordance with the termination provisions in this Section.

(b) Termination for Breach. Either party may terminate this Agreement if it determines that the other party has breached a material term of this Agreement. Alternatively, the non-breaching party may choose to provide the breaching party with notice of the existence of an alleged material breach and afford an opportunity to cure the material breach. If the breaching party fails to cure the breach to the satisfaction of the non-breaching party, the non-breaching party may immediately thereafter terminate this Agreement and report the breaching party to the Secretary.

(c) Automatic Termination. This Agreement will automatically terminate on the date Business Associate ceases to provide to the services described in the Underlying Agreement.

(d) Effect of Termination. Upon termination of this Agreement, Business Associate will return or destroy all PHI received from Covered Entity or created or received by Business Associate on behalf of Covered Entity that Business Associate still maintains and will retain no copies of that PHI. However, if this return or destruction is not feasible, upon the agreement of Covered Entity, then Business Associate will extend the protections of this Agreement to the PHI and will limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

6. Agreement. Covered Entity and Business Associate agree to take any reasonable action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity and Business Associate to comply with the requirements of the Privacy and Security Rules, HITECH, and any other implementing regulations or guidance.

7. Interpretation. Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy and Security Rules and HITECH.

8. Survival. The obligations of Business Associate under Section 5(d) of this Agreement survive any termination of this Agreement.

9. No Third Party Beneficiaries. Nothing express or implied in this Agreement is intended to confer, nor shall anything in this Agreement confer, upon any person other than the parties and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

10. General Administrative Provisions.

(a) Any notices required by this Agreement will be sent to the latest known address of either party by (i) facsimile, email, registered or certified mail or by private delivery service that provides receipts to the sender and recipient, (ii) personally delivered or (iii) by regular mail. Each party reserves the right to designate an additional address or a separate address for notices to be sent. Notices are deemed given (i) on the date of the facsimile or email transmittal, (ii) the date shown on the registered mail, certified mail or private delivery service receipt, (iii) the date personally delivered, or (iii) two business days after the date of mailing of a notice sent by regular mail.

(b) Each party agrees to promptly perform any further acts and execute, acknowledge, and deliver any documents which may be reasonably necessary to carry out the provisions of this Agreement or affect its purpose.

(c) In the event that any of the provisions or portions of this Agreement are held to be unenforceable or invalid by any court of competent jurisdiction, the validity and enforceability of the remaining provisions or portions will not be affected.

(d) The waiver by a party of any breach of any term, covenant, or condition in this Agreement will not be deemed to be a waiver of any subsequent breach of the same or any other term, covenant, or condition of this Agreement. A party's subsequent acceptance of performance by the other party shall not be deemed to be a waiver of any preceding breach of any term, covenant or condition of this Agreement other than the failure to perform the particular duties so accepted, regardless of knowledge of such preceding breach at the time of acceptance of the performance.

(e) This Agreement constitutes the entire agreement among the parties with respect to the subject matter of this Agreement and supersedes any prior agreements, whether written or oral, pertaining to that subject matter.

(f) This Agreement may be executed in one or more counterparts, any one of which may be considered an original copy.

COVERED ENTITY: Ohio Eye Surgeons, Inc.	BUSINESS ASSOCIATE:
By:_____ [Printed name]	By:_____ [Printed name]
Title:_____	Title:_____
Date:_____	Date:_____

FORM NO. 25: APPOINTMENT OF PERSONAL REPRESENTATIVE FORM

Ohio Eye Surgeons, Inc.

APPOINTMENT OF PERSONAL REPRESENTATIVE
TO RECEIVE PROTECTED HEALTH INFORMATION

You may rely upon your spouse, relatives or friends from time to time to understand your treatment options, visit your physicians, acquire prescriptions, get test results, and otherwise be involved in your medical care. However, federal law does not allow us to Disclose any of this information to these people unless you appoint them as your "personal representatives".

To appoint an Individual as your personal representative, complete this form.

I hereby authorize Ohio Eye Surgeons to release the following protected health information to the Individual I have designated:

Name	Relationship	Personal Health Information That May Be Disclosed
_____	☐ Spouse ☐ Other Relative ☐ Friend ☐ Other	☐ All personal health information OR One or more of these choices: ☐ Times of appointments ☐ Prescriptions & ancillary equipment ☐ Test results ☐ Copies of medical records ☐ Other:
If you wish to designate more than one Individual, use an additional form.		

I may revoke this appointment at any time. My revocation will NOT affect any actions that have been already taken in reliance on my original appointment.

_____ Date:_____
Individual's Printed Name

_____
Individual's Signature

Individual's Address: _____
_____
_____

FORM NO. 26: WORKFORCE TRAINING CERTIFICATE & CONFIDENTIALITY AGREEMENT

Ohio Eye Surgeons, Inc.

HIPAA AWARENESS TRAINING CERTIFICATION
& CONFIDENTIALITY AGREEMENT

On _____, 20_____, I completed HIPAA awareness training that included: (1) an overview of the basic terms and operation of HIPAA's Privacy and Security Rules concerning the Use and Disclosure of Protected Health Information; (2) a review of the OES's Privacy Practices, including Individual Rights; (3) the OES's Complaint Resolution Procedure; and (4) the HITECH amendments to the HIPAA Privacy and Security Rules.

I understand that maintaining confidentiality and the proper Use and Disclosure of Protected Health Information is an integral part of my job description. I understand that each member of the Workforce shares a responsibility to assist the OES and its designated Privacy and Security Officers to comply with the Privacy and Security Rules. I promise to take reasonable steps in performing my job duties to safeguard the privacy and security of our Individuals' Protected Health Information. I will not attempt to access Protected Health Information beyond what is Minimally Necessary for me to perform my job duties and responsibilities.

I will report my concerns about suspected violations, privacy Breaches, security incidents, and Breaches of Unsecured Protected Health Information so that corrective action can be taken. I will make suggestions to improve the effectiveness and efficiency of the OES's privacy and security practices.

I understand that the duty to respect and maintain the privacy and security of Protected Health Information is ongoing and does not end if I voluntarily or involuntarily leave the OES's Workforce.

If I leave the OES, regardless of reason, I agree not take with me originals or copies of Individual records or Protected Health Information. If I have in my possession any Protected Health Information, I agree to return it or to destroy it, so I do not violate HIPAA's Privacy or Security Rules, Breach any Individual's privacy rights, or subject the OES and/or myself to any risk of administrative fines, penalties, civil or criminal liability.

Upon my leaving the OES, I agree to return any confidential and proprietary information belonging to the OES, including (without limitation) Individual lists and demographic information, billing information, financial information, contract and strategic planning information. I promise not to Disclose this confidential and proprietary information to any unauthorized person or competitor of the OES, and I promise not to use it to the detriment of the OES.

_____
Print Name

_____ _____
Signature Date