HIPAA SECURITY POLICIES AND PROCEDURES
FAMILY EYE CARE SERVICES, P.A. (HEREIN "THE PRACTICE")

If you should have any questions or concerns regarding these Policies and Procedures, the Practice's HIPAA forms attached hereto, or your obligations under any of them or under state or federal law, please contact Paul Vaccarella, O.D., 908-704-8855, pv001@aol.com before taking any further action.

Part I. General Security Requirements

§ 1 Introduction.

Covered entities, such as **FAMILY EYE CARE SERVICES, P.A.** (the "Practice"), as well as their business associates, must comply with the requirements of subpart C of 45 C.F.R. Part 164 (the "HIPAA Security Rules"). The HIPAA Security Rules adopt national standards for safeguards to protect the *confidentiality, integrity, and availability* of electronic protected health information ("ePHI") pursuant to sections 261 through 264 of the Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191), as amended and supplemented by the Health Information Technology for Clinical Health Act (P.L. 111-05) (the "HITECH Act"). The foregoing laws are hereinafter referred to as "HIPAA," and such references shall include the regulations promulgated and amended from time to time there under. As noted above, the HIPAA Security Rules require the Practice to protect three important aspects of the ePHI it uses or discloses:

> ***Confidentiality*** assures that data or information is not made available or disclosed to unauthorized persons or processes.
>
> ***Integrity*** assures that data or information has not been altered or destroyed in an unauthorized manner.
>
> ***Availability*** assures that data or information is accessible and usable upon demand by an authorized person.

The HIPAA Security Rules define standards and implementation specifications for the administrative, physical, and technical safeguards required to protect the security of ePHI. In contrast, the HIPAA privacy rules, subpart D of 45 C.F.R. Part 164 (the "HIPAA Privacy Rules"), set standards for ensuring the *privacy* of protected health information in all forms, including written and electronic. The Practice's implementation of the HIPAA Privacy Rules can be found in the Practice's HIPAA Privacy Policies and Procedures. The HIPAA Privacy Rules, as implemented by the Practice's HIPAA Privacy Policies and Procedures, define the uses and disclosures are permissible, required by law, or otherwise require written authorization, and what rights patients have with respect to their PHI. These HIPAA Security Policies and Procedures are intended to ensure the security of the ePHI used and disclosed.

The Practice's HIPAA Security Policies and Procedures will be applied to: data "at rest," including data that resides in a database, file systems, laptop personal computers, flash drives, memory cards or sticks, mobile devices, and any other structured storage method; data "in motion," including electronic transmission of data through a network, including wireless transmission, whether by e-mail or structured electronic interchange; data "in use," including data in the process of being created, retrieved, updated, or deleted; and data "disposed," including discarded hard drives, workstations, laptop computers, smartphones and personal data assistants, flash drives or other storage media, paper records or recycled electronic media.

"Electronic transmissions" include transactions using any type of electronic media, even when the information is physically moved from one location to another using magnetic tape, disk, or other machine readable media. The physical movement of electronic media from place to place is not limited to magnetic tape, disk, or compact disk. Transmissions over the Internet, extranet (using Internet technology to link a business with information only accessible to collaborating parties), leased lines, dial-up lines, and private networks are included. The transmission of information not in electronic form before the transmission, for example, paper faxes or voice calls, however, is not covered by this definition. Non-electronic transmissions remain subject to the Practice's HIPAA Privacy Policies & Procedures, however.

The HIPAA Security Rules draw no distinction between internal and external data movement. The HIPAA Security Rules protect ePHI at rest, in motion, in use, and dispose. Appropriate protections will be applied, regardless of the state of the data. However, the specific protections determined by the Practice to be appropriate will vary, and will be determined by each type of data and the nature and complexity of the Practice's health care and other business activities.

The HIPAA Security Rules set a baseline, or minimum level, of reasonable and appropriate security measures that must be taken by the Practice with respect to administrative, physical, and technical safeguards. The HIPAA Security Rules do not, however,

prohibit a covered entity from employing more stringent security measures, nor does HIPAA preempt state laws that may be stricter than HIPAA. The following policies and procedures apply to all ePHI created, received, used, disclosed or maintained by the Practice and its business associates, and also apply to all ePHI of the group health plan components of the Practice, if any.

§ 2 HIPAA Security Compliance – General.

Policy. It is the policy of the Practice to ensure the confidentiality, integrity and availability of all electronic protected health information, or ePHI, that is created, received, maintained or transmitted by the Practice, by applying the applicable standards, implementation specifications, and requirements of the HIPAA Security Rules with respect to all such ePHI.

Procedure. The Practice will identify the various sources, uses, disclosures and locations of ePHI within the Practice. This includes:

- Identifying the different ways in which PHI is used, stored or transmitted electronically by the Practice
- Maintaining a list or inventory of all computers, network servers, laptops, hard drives, flash drives, smart phones (e.g. Blackberry devices) and other mobile devices or storage media used by the Practice that may contain PHI.
- Documenting and maintaining records of all workforce members and business associates that have access to ePHI. Records must include sign-on and authentication information, training records, records of authorizations and disabling of any access specific to any individual.
- Maintaining records of audits, risk assessments and implementation of HIPAA Security policies, procedures and safeguards to ensure ongoing compliance. See Organizational Requirements, below.

§ 3 HIPAA Security Implementation.

Purpose. To establish that the Practice will implement and maintain appropriate security measures to address its own unique security needs.

Policy. The Practice will ensure the confidentiality, integrity, and availability of all ePHI the Practice creates, receives, maintains, or transmits. The Practice will (a) implement reasonable and appropriate measures to protect against any reasonably anticipated threats or hazards to the security or integrity of such information, (b) implement reasonable and appropriate measures to protect against anticipated uses or disclosures of such information that are not permitted or required under the HIPAA Privacy Rules, and (c) ensure compliance with the HIPAA Security Rules by its workforce, business associates, subcontractors and agents. How individual security requirements will be satisfied and which technology will be used are business decisions that the Practice will make based on the HIPAA Security Rules and the Practice's unique security needs and activities.

Procedures. The Practice will adopt security measures that allow it to implement the standards and implementation specifications specified under the HIPAA Security Rules in a reasonable and appropriate manner. In deciding which security measures to use, the Practice will take into account the following factors:

- The Practice's size, complexity, and capabilities.
- The Practice's technical infrastructure, hardware, and software security capabilities.
- The costs of security measures.
- The probability and criticality of potential risks to ePHI.

Standards. As a covered entity, the Practice will comply with the standards and implementation specifications as provided in 45 C.F.R. Part 164, subpart C, with respect to all ePHI.

Implementation Specifications. Implementation specifications are provided in the HIPAA Security Rules to assist covered entities with effectively implementing the HIPAA standards. Implementation specifications are "required" or "addressable." If an implementation specification is required, the word "Required" appears in parentheses after the title of the implementation specification. If an implementation specification is addressable, the word "Addressable" appears in parentheses after the title of the implementation specification.

When a standard provided in the HIPAA Security Rules includes required implementation specifications, the Practice must implement the implementation specifications. When a standard provided in the HIPAA Security Rules includes addressable implementation specifications, the Practice will conduct an implementation decision analysis as follows:

- Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely relative value of the implementation specification with respect to protecting the Practice's ePHI; and

- As applicable:

    - Implement the implementation specification if reasonable and appropriate; or

    - If implementing the implementation specification is not reasonable and appropriate:

        - Document why it would not be reasonable and appropriate to implement the implementation specification; and

        - Implement an equivalent alternative measure that is reasonable and appropriate.

Whether a given addressable implementation specification is a reasonable and appropriate security measure for the Practice will depend on a variety of factors, such as, among others, the Practice's risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation. Based upon this decision the following applies:

- If a given addressable implementation specification is determined to be reasonable and appropriate, the Practice will implement it.

- If a given addressable implementation specification is determined to be an inappropriate and/or unreasonable security measure for the Practice, but the standard cannot be met without implementation of an additional security safeguard, the Practice may implement an alternate measure that accomplishes the same end as the addressable implementation specification.

- If a given standard is met through alternative measures the Practice will document the decision not to implement the addressable implementation specification, the rationale behind that decision, and the alternative safeguard(s) implemented to meet the standard.

- The Practice may also decide that a given implementation specification is simply not applicable (that is, neither reasonable nor appropriate) to its situation and that the standard can be met without implementation of an alternative measure in place of the addressable implementation specification. In this scenario, the Practice will document the decision not to implement the addressable specification, the rationale behind that decision, and how the applicable HIPAA Security Rule standard is being met.

Maintenance of Security. Security measures, policies and procedures implemented to comply with standards and implementation specifications adopted under the HIPAA Security Rules must be reviewed periodically by the Practice's Security Officer and modified as needed to continue provision of reasonable and appropriate protection of ePHI, as required under 45 C.F.R. § 164.316 of the HIPAA Security Rules.

Part II. Administrative Safeguards

§ 4 Security Management and Risk Assessment.

Purpose. To safeguard ePHI by preventing, detecting, containing, and correcting security incidents and violations of the HIPAA Security Rules.

Policy. It is the policy of the Practice to develop and implement, under the direction of the Security Officer, policies and procedures and take actions to prevent, detect, contain, and correct security violations and to comply with the HIPAA Security Rules.

Procedures. Under the direction of the Security Officer, the Practice will:

- Risk Assessment and Management. Conduct an accurate and thorough risk assessment of the potential vulnerabilities to the confidentiality, integrity and availability of ePHI and the probability of occurrence and magnitude of such risks. This risk assessment may include conducting an inventory of systems and

applications used to access or house data and classifying the respective levels of risk. The Practice will then take appropriate actions to reduce or manage any identified risks or vulnerabilities to an acceptable level, through risk management measures.

- Sanctions. Apply appropriate sanctions, in accordance with the Practice's disciplinary procedures, against workforce members who fail to comply with the security procedures.

- Information System Activity Review. Regularly review records of information system activity, such as audit logs, access reports, and security incident reports, as determined by the Security Officer, to determine if any ePHI has been used or disclosed in an inappropriate manner.

§ 5 Security Officer - Assigned Security Responsibility.

Purpose. To establish administrative responsibility for the development and implementation of the security policies and procedures required by the HIPAA Security Rules.

Policy. The Practice is committed to safeguarding the ePHI of its patients. As a result, the position of HIPAA Security Officer has been created to ensure that this is accomplished. The Practice shall appoint a manager to serve as HIPAA Security Officer with oversight responsibility for the development, implementation, and operation of the Practice's security compliance program. The position of HIPAA Security Officer may be held by the Privacy Officer, or another appropriately qualified and experienced manager, and need not be the manager's full-time role in the organization, depending on the reasonable and appropriate duties of the position.

Responsibilities of Security Officer. In general, the HIPAA Security Officer's job responsibilities include general responsibility for overseeing and enforcing the security policies and procedures that must be adopted by the Practice with regard to ePHI. These responsibilities include, but are not limited to, the following tasks:

- Establish an HIPAA security team charged with the development and implementation of a security compliance program;

- Coordinate and facilitate the HIPAA security team's activities;

- Collaborate with the HIPAA team, management, legal counsel, security, regulatory affairs and appropriate staff to create, implement, and monitor the HIPAA Security Policies and Procedures.

- Assist in the development, implementation, and monitoring of Business Associate Agreements to ensure that all security requirements are adequately addressed;

- Work with legal counsel, security and regulatory affairs to develop methods of investigating allegations of noncompliance with the Practice's security policies, and, in conjunction with Human Resources, Regulatory Affairs and Legal Counsel, develop appropriate sanctions for noncompliance by workforce members and business associates;

- Provide periodic reports to management on the status of the security compliance program;

- Maintain current knowledge of applicable standards and, in conjunction with Legal Counsel, revise the security compliance program as necessary to reflect changes in the law or security policy;

- In conjunction with Legal Counsel and Regulatory Affairs, serve as an internal resource for all security-related matters and cooperate with external parties in any compliance reviews or investigations; and

- Delegate his or her duties and responsibilities under the security compliance program as appropriate.

§ 6 Workforce Security and Information Access Management.

Purpose. To ensure that all members of the Practice's workforce have appropriate access to ePHI, and to prevent unauthorized workforce members from obtaining access to ePHI.

Policy. It is the policy of the Practice that workforce members (employees and others under the direct control of the Practice) who work with or around ePHI shall be appropriately supervised and provided with appropriate authorization to access ePHI. Only those workforce members with appropriate authorization shall be permitted to access ePHI.

Procedures.

- Workforce Authorization. The Security Officer, in consultation with the Practice's Information Systems Manager, shall implement procedures for establishing access of workforce members to ePHI on Practice computers and mobile devices, based on assigned job duties and "need to know" basis for access to ePHI. The Security Officer shall ensure that the Practice's Information Systems Manager and executive management have access to all files and documents present on Practice computers and mobile devices.

- Workforce Clearance. The Security Officer shall ensure that procedures are implemented for determining the appropriate level of access for a workforce member to ePHI of the Practice's patients. This includes screening of employees, review of employee training and capabilities on computer systems, and documenting access codes and clearance for access to various systems. The Security Officer shall ensure that the Information Systems Manager maintains a master list of all workforces members with the assigned access codes and log-in information for each workforce member stored in a secure location, with appropriate data file back up.

- Workforce Termination Procedures. Upon a change in status of a workforce member (termination of contract or discharge from employment, separation, re-assignment to new position), the Information Systems Manager will immediately terminate the electronic authorization privileges to ePHI of the workforce member, and/or electronically block or restrict access to ePHI. The information systems manager shall ensure that a log of attempted access by unauthorized workforce members is maintained and regularly reviewed following workforce changes, and reported to the Security Officer when any inappropriate activity is detected.

§ 7 Security Awareness and Training.

Purpose. To implement a security awareness and training program for all members of the Practice's workforce (including employees, management, and non-employees under the Practice's direct control).

Policy. It is the policy of the Practice to provide training to all members of its workforce on the HIPAA Security Policies and Procedures as necessary and appropriate for the workforce members to carry out their specific job duties.

Procedures. The following requirements shall apply to all members of the Practice's workforce, including employees and any non-employees under the Practice's direct control, who may use, handle or have access to or be exposed to ePHI:

- Current Employees. The Practice will provide security training programs to all current workforce members who may use, handle, have access to or be exposed to ePHI. All applicable persons will be expected and required to attend such training. Attendance will be taken to ensure that all such persons have received appropriate training.

- New Employees. As part of each new workforce member's orientation, the Practice will provide training regarding the HIPAA Security Policies and Procedures.

- Additional Training. When material changes are made to a security policy or procedure or whenever environmental or operational changes affect the security of ePHI, all members of the workforce whose functions are affected by the changes must receive training on the new policies and procedures within a reasonable time after the material change or environmental or operational changes have been made. Additional training sessions may be conducted for specific workforce members who have responsibilities involving specific compliance issues. In addition, the Security Officer or his or her designee may direct specific workforce members to attend privacy training if he or she believes that such training is warranted.

- Documentation. The Security Officer will document the time, date, place and content of each training session, as well as the attendees at each training session.

- Content of Training. In security training, workforce members will review the HIPAA Security Policies and Procedures and will discuss any recent changes. The training program will focus on periodic security updates, reporting security incidents and breaches of unsecured PHI, procedures for guarding against, detecting and reporting malicious software, procedures for monitoring log-in attempts and reporting discrepancies, and procedures for creating, changing and safeguarding passwords.

§ 8 Security Reminders.

Purpose. To ensure that the Practice regularly informs its workforce of their security responsibilities.

Policy. It is the policy of the Practice to issue periodic security updates and reminders, not less frequently than semi-annually, to all workforce members, advising of any changes to Practice policies and procedures, and reminding workforce members of the various methods and requirements for protecting ePHI while using Practice computer systems and mobile devices.

§ 9 Protection from Malicious Software.

Purpose. To ensure that only authorized programs and processes are permitted to access ePHI.

Policy. It is the policy of the Practice to ensure the protection of ePHI by limiting the types of software permitted on the Practice's computer workstations and other devices handling ePHI. Loading and using unauthorized personal software programs is not permitted. Examples of unauthorized personal software include screen savers, games, internet access and any other programs that could hinder the productivity of the Practice's operations or create a security risk. Individuals who are found to be in violation of the restrictions will be subject to the Practice's employee disciplinary action policy.

Procedures. The Security Officer, working in conjunction with the Practice's Information Systems Manager, shall ensure that all computer systems are equipped with firewalls to trap viruses and to restrict unauthorized transmittal of ePHI between and among other unauthorized computer systems. The Security Officer shall ensure that the Practice's policy against use of unauthorized software programs on Practice computers and devices is reasonably and consistently enforced.

In the event of a virus, any affected employee must contact the information systems manager and Security Officer to report the virus.

The Practice's Information Systems Manager shall submit system security reports, including reports of viruses, malware or network access attempts to the Security Officer. Virus alerts shall be communicate to Practice's affected workforce members, and appropriate measures implemented until any virus is removed from Practice systems. See also, Security Incidents.

§ 10 Log-In Monitoring; Incident Reporting.

Purpose. To effectively monitor and respond to unauthorized access by workforce members and business associates to Practice systems containing ePHI.

Policy. It is the policy of the Practice to monitor log-ins to Practice computer systems in efforts to ensure the integrity and confidentiality of ePHI. Unauthorized access of such systems will subject the workforce member or business associate to sanctions up to and including termination.

Procedures. The Security Officer shall ensure each user log-in is recorded on an electronic log.

- Log is subdivided according to workstation sites throughout the Practice.
- Log identifies the user's name, date, time and file accessed.
- Log is able to identify attempts to access restricted files.

The Practice's Information Systems Manager shall review logs to identify any attempts to access files by an unauthorized user, and immediately report incidents to the Security Officer. The Security Officer shall investigate and promptly inform the Practice management of any unauthorized attempt to access a file by a Practice workforce member or business associate, pursuant to the Security Incidents policy.

The Security Officer shall develop reports that identify attempts by users to access restricted files, on a monthly basis. The Security Officer shall review the monthly report with the Practice's Privacy Officer and CSI Management. The Security Officer shall ensure logs are stored electronically and securely for the required document retention period.

In the event of unauthorized access by a workforce member or business associate, CSI Management shall follow-up with the appropriate resolution, including disciplinary sanctions when warranted by Practice policy, and shall document any actions taken. The disciplinary sanction documentation shall be placed in the workforce member's personnel file, and a copy forwarded to the Security Officer.

§ 11 Password Management.

Purpose. To effectively safeguard and manage log-in identification and security passwords.

Policy. It is the policy of the Practice to manage the passwords used to access ePHI. The Practice's Information Systems Manager is responsible for creating and issuing log-in identification and passwords to all Practice workforce members. Sharing of log-ins by any user may result in the loss of access to Practice computer systems, or other disciplinary action.

Procedures. The Practice's Human Resources Manager notifies the Practice's Privacy and Security Officers, and the Practice Information Systems Manager, of new hires.

The Practice's Information Systems Manager ensures that each workforce member is assigned a log-in and password upon hire; creates and issues all log-in identifications and passwords; maintains a master list of log-ins and passwords and ensures they are kept confidential and locked in the Practice's information system; and ensures user log-ins and passwords are changed in the event of a change in employment status or if the workforce member is becoming a member of a department that changes the amount of access permitted.

The Practice's Human Resources Manager informs the information systems manager of any changes in workforce status to create a new log-in and password and to disable the former log-in and password.

The Security Officer ensures a log of all user log-ins and password changes are maintained by the Information Systems Manager pursuant to the Log-In Monitoring Policy.

The Security Officer ensures that all workforce members are provided periodic reminders, not less frequently than semi-annually, to change their passwords, and to update and remind them of appropriate password management procedures.

§ 12 Security Incidents.

Purpose. To effectively address security incidents in a manner that reasonably and appropriately mitigates harmful effects and notifies the appropriate persons and authorities, and reduces future vulnerabilities.

Policy. It is the policy of the Practice to identify, investigate and respond appropriately to suspected or known security incidents. In addition, the Practice will mitigate, to the extent practicable, harmful effects of security incidents that are known to the Practice. The Practice will document all security incidents and their outcomes.

Procedures. The Security Officer will promulgate written procedures describing how workforce members are to report, and Practice management should respond to, a suspected or known security incident. This shall include: immediately reporting to the Security Officer any security incident of which an employee becomes aware or reasonably suspects; communicating incident reports to the Privacy Officer and Practice management, preserving evidence; mitigating, to the extent possible, the situation that caused the security incident; documenting the security incident and the outcome; and evaluating security incidents as part of ongoing risk management.

The Security Officer will, in accordance with 45 C.F.R. §§ 164.400 et seq., develop and implement a system for internal investigation and reporting of security incidents that give rise to breaches of unsecured ePHI.

The Security Officer will, in accordance with 45 C.F.R. §§ 164.400 et seq., make the required notifications in the case of a security incident that gives rise to a breach of unsecured ePHI.

§ 13 Security Contingency Plans.

Purpose. To establish and implement reasonable and appropriate safeguards and actions for responding to an emergency or other occurrence (such as natural disaster, fire, vandalism, or system failure) that damages or threatens damage to, Practice systems containing ePHI.

Policy. It is the policy of the Practice to establish and maintain the following plans, policies and procedures to safeguard the confidentiality, integrity and availability of ePHI:

- Data Backup Plan
- Disaster Recovery Plan
- Emergency Mode Operation Plan
- Testing and Revision Procedures
- Applications and Data Criticality Analysis

Procedures. In establishing a contingency plan for responding to an emergency or other occurrence, the Security Officer will, as appropriate:

- Create a data backup plan to create and maintain retrievable exact copies of ePHI.
- Establish (and implement as needed) reasonable and appropriate security procedures to restore any loss of data.

- Establish (and implement as needed) reasonable and appropriate security procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.

- Periodically test and revise contingency plans, as necessary.

- Assess the relative criticality of specific applications and data in support of other contingency plan components.

§ 14 Evaluation.

Purpose. To periodically evaluate the extent to which the Practice's technical and nontechnical security measures reasonably and appropriately safeguard ePHI, and the extent to which the Practice's HIPAA Security Policies and Procedures meet the requirements of the HIPAA Security Rules.

Policy. It is the policy of the Practice to evaluate all security measures, policies and procedures related to the protection of ePHI, in accordance with the HIPAA Security Rules.

Procedures. The Security Officer shall, at least annually, cause the performance of a technical and nontechnical evaluation of the Practice's compliance with the HIPAA Security Rules and effectiveness of the Practice's security measures, policies and procedures in reasonably and appropriately safeguarding the confidentiality, integrity and availability of ePHI. Technical and nontechnical evaluations must also be performed in response to significant environmental or operational changes that affect the security of ePHI and should also be completed as new technology is introduced. Evaluations and resulting security improvement plans or actions shall be appropriately documented and maintained by the Security Officer.

§ 15 Business Associate Agreements and Other Arrangements.

Purpose. To ensure that all arrangements with business associates and other third parties include reasonable and appropriate measures to safeguard ePHI in accordance with these HIPAA Security Policies and Procedures and the HIPAA Security Rules.

Policy. It is the policy of the Practice to permit a business associate to create, receive, use, disclose, transmit or maintain ePHI for or on behalf of the Practice only if pursuant to a written Business Associate Agreement (which contains satisfactory assurances that the business associate will appropriately safeguard the PHI) approved by the Practice's Security Officer and only in accordance with the HIPAA Security Rules, HITECH Act requirements and these HIPAA Security Policies and Procedures. Except as otherwise provided under HIPAA, all other persons or entities to whom ePHI may be disclosed for purposes permitted under HIPAA, but not falling under the business associate definition, must execute an appropriate confidentiality agreement with the Practice.

Procedures.

- The Security Officer shall identify all "business associates", as defined under 45.C.F.R. 160.103, of the Practice who create, receive, use, disclose, transmit or maintain ePHI for or on behalf of the Practice, and all other persons or entities to whom ePHI is disclosed by the Practice.

- The Security Officer, working with the Practice Management, and Legal Counsel where necessary, shall ensure that all business associates have executed a Business Associate Agreement or Addendum that meets the requirements of 45 C.F.R. § 164.314(a) and 45 C.F.R. § 164.514, and that incorporates the privacy and security requirements applicable to covered entities and extended to business associates under the HITECH Act.

- The Security Officer shall ensure that all other third parties to whom ePHI is disclosed for purposes permitted under HIPAA, but not falling under the business associate definition, execute an appropriate confidentiality agreement with the Practice that, at a minimum, obligates the recipient to: keep the ePHI confidential; implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of any ePHI; report to the Practice's Security Officer any security incident, or breach or potential breach of unsecured PHI, of which the recipient becomes aware; and authorize termination of the contract by the Practice if it determines, in its sole discretion, that the recipient violated the HIPAA Privacy or Security Rules, or violated a material term of the contract.

- The Security Officer shall maintain a log of all business associate agreements and other confidentiality agreements entered into by the Practice, including a summary of the contract terms.

- The Security Officer shall report violations of any Business Associate Agreement or Addendum to the Privacy Officer and the Practice's Management.

Part III. Physical Safeguards

§ 16 Facility Access Controls.

Purpose. To reasonably and appropriately limit physical access to electronic information systems and the physical facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

Policy. It is the policy of the Practice to limit and control access to the Practice's property and equipment to those employed by the Practice, authorized persons supporting the Practice's operations, patients, and authorized visitors. Access to the Practice's health information systems, including those systems containing ePHI, shall be limited to those authorized workforce members or authorized business associates who need such information for the provision of treatment, payment, or health care operations of the Practice, or for other purposes related to the management and administration of the Practice, or as required by law.

Procedures. The Security Officer shall, as appropriate:

- Identification and Inventory of Facilities. Identify all equipment and facilities in which ePHI is located, and create and orderly system of logging and updating the identity, location, purpose and access controls maintained for all such equipment and facilities.

- Contingency Operations. Establish and implement where needed, reasonable and appropriate security procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

- Facility Security Plan. Implement reasonable and appropriate security procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering and theft. This may include a review of risk analysis data on persons or workforce members and business associates that need access to data or that need access to facilities and equipment, and the training of such individuals to know and understand their roles in facility security.

- Access Control and Validation. Implement reasonable and appropriate security procedures to control and validate a person's access to equipment or facilities based on his or her role or function, including visitor control and control of access to software programs for testing a revision.

- Maintenance Records. Document repairs and modifications to the physical components of all equipment and facilities which contain, or are related to the security of, ePHI.

§ 17 Workstation Use and Security.

Purpose. To ensure the security of ePHI by implementing appropriate workstation use and security controls.

Policy. It is the policy of the Practice to specify functions to be performed with respect to ePHI maintained by the Practice in computer workstations or similar facilities; to regulate the manner in which those functions are to be performed using workstations, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI; and to implement physical safeguards for all workstations that access ePHI to restrict access to authorized users.

Procedures. The Security Officer or his or her designee shall specify and document functions to be performed using ePHI on Practice workstations and other computers, shall specify those other uses of workstations and computers deemed reasonable and appropriate consistent with the HIPAA Security Rules and these HIPAA Security Policies and Procedures. The Security Officer or his or her designee shall also direct the implementation of appropriate use policies and physical safeguards for all workstations and computers that access ePHI (including laptop computers), whether they be in the office, at a satellite office, at home, or at another facility, to restrict access to authorized users. These safeguards will, among other things, ensure that workstations are appropriately located in areas apart from general access and that cannot be viewed or accessed by unauthorized individuals, visitors, family members or other workforce members. These workstation use and security measures and policies shall be evaluated by the Security Officer not less than annually. See also Workforce Authorization and Clearance; User Authentication; and Log-In Monitoring.

§ 18 Device and Media Controls.

Purpose. To maintain the confidentiality and integrity of all ePHI during the receipt, delivery, removal and disposal or re-use of equipment, devices and media throughout the organization.

Policy. It is the policy of the Practice to implement reasonable and appropriate security measures, policies and procedures that govern the receipt, removal and disposal of hardware and electronic media that contain ePHI at a particular facility and the movement of these items within the facility.

Procedures. The Security Officer or his or her designee shall:

- Ensure that appropriate device and media controls exist and are documented with respect to acquisition, use and disposition of devices and storage media for ePHI of the Practice.

- Identify the receipt, removal and disposal of all devices and media containing ePHI at the Practice. Before moving or disposing of, or re-using, any device or media, a retrievable, exact copy of any ePHI shall be made.

- Track the final disposition of ePHI and/or the hardware or electronic media on which ePHI is stored by the Practice and provide for the removal of any ePHI from electronic media before the media are made available for re-use. Electronic media upon which ePHI is stored will be deemed destroyed if it has been cleared, purged, or destroyed in accordance with NIST Special Publication 800-88, Guidelines for Media Sanitization, or other standards approved by the U.S. Department of Health and Human Services, such that the ePHI cannot be retrieved.

- Maintain a record of the movement or disposal or re-use of hardware and electronic media containing ePHI and any person responsible therefor.

Part IV. Technical Safeguards

§ 19 System Access Controls.

Purpose. To safeguard the Practice's electronic information systems that maintain ePHI by allowing access only to those persons or software programs that have been granted access rights, as specified in 45 C.F.R. § 164.308(a)(4) of the HIPAA Security Rules.

Policy. It is the policy of the Practice to limit and control access to ePHI to and by authorized users only, to regulate time periods of system access, and to adopt appropriate methods of rendering ePHI unusable, unreadable or indecipherable to unauthorized persons.

Procedures. The Security Officer shall implement the following access security procedures, as appropriate:

- Assign a unique name and/or identity for identifying and tracking user identity.

- Establish reasonable and appropriate security procedures for obtaining necessary ePHI, if any, during an emergency.

- Terminate an electronic session involving ePHI after fifteen (15) minutes of inactivity.

- Implement a mechanism to encrypt and decrypt remote system access sessions, data in transit (e.g., via e-mail), and data at rest containing ePHI that may be at risk of unauthorized use or disclosure (e.g., laptop computers, mobile devices, remote storage or "co-location" facilities). In the case of encryption, the encryption key must be kept on a separate device from the encrypted data. Any encryption process must be consistent with the guidance and industry standards outlined in The U.S. Department of Health and Human Services, Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals, 74 Fed. Reg. 42740, 42741-42743 (August 24, 2009). Referred to in the foregoing guidance are NIST Special Publications, including: 800-111, Guide to Storage Encryption for End User Devices; 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementation; 800-77, Guide to IPsec VPNs; 800-113, Guide to SSL VPNs; or others which are Federal Information Processing Standards (FIPS) 140-2 validated.

§ 20 Audit Controls.

Purpose. To safeguard ePHI by recording and examining activity on Practice information systems that contain or use ePHI.

Policy. It is the policy of the Practice to implement reasonable and appropriate security hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.

Procedures. The Practice's Security Officer, in consultation with the Practice's Information Systems Manager, shall:

- Ensure that each Practice computer system has an integrated electronic logging and tracking mechanism whereby accesses to the system are logged according to employee user identification and authentication policies.

- Ensure that each Practice computer system generates a daily report of all user identifications logged into the system and the location of data accessed, provided, removed or deleted. This report shall be permanently stored and remain available for not less than six (6) years after the creation of each report.
- Ensure that each Practice computer system reads the access level of the user, as programmed through the user identification and authentication process, and determines if any unauthorized access attempts are made.
- Ensure that each Practice computer system flags those unauthorized access attempts and that a separate access log and report are generated.
- Designate a person, who shall report directly to the Security Officer, to review the routine and unauthorized access attempt logs daily, and who shall report unauthorized access attempts directly to the Security Officer.
- Review reports, investigate potential security incidents, pursuant to the Security Incidents and Breach Notification Policy, and follow-up with the Privacy Officer and Practice Management or department manager, as appropriate, depending upon the findings from the daily access logs.

§ 21 Data Integrity – Protection from Alteration or Destruction.

Purpose. To ensure that all ePHI has not been altered, modified or destroyed in an unauthorized manner.

Policy. It is the policy of the Practice to implement reasonable and appropriate policies and mechanisms to protect ePHI from improper alteration or destruction.

Procedures. The Security Officer shall, as appropriate, implement electronic mechanisms to confirm that the ePHI has not been altered or destroyed in an unauthorized manner. This shall include:

- Ensure that each Practice computer system has a method of documenting entries into the patient's records through the use of user identification.
- Ensure that each time a user logs into a Practice computer system, the user's identification will electronically sign the record to which information has been added.
- Ensure that each Practice computer system will log each portion of the electronic record the user accesses with the user's identification, date and time of access.
- Ensure that each Practice computer system maintains the above-described log electronically, and generates daily reports for analysis.

§ 22 User Authentication.

Purpose. To ensure that only authorized users are permitted to access ePHI maintained on Practice information systems.

Policy. It is the policy of the Practice to implement reasonable and appropriate security procedures to verify that a person or entity seeking access to ePHI is the one claimed.

Procedures. The Practice shall authenticate workforce members, business associates or other authorized persons using Practice computers, as follows:

- The Security Officer shall ensure that the Practice's information systems manager provides each workforce member, business associate or other authorized person with a unique user identification.
- Each user identification shall include a personal identification number (PIN) to be used in conjunction with an identified password.
- In accordance with § 19 above, each Practice computer workstation shall have an automatic logoff in the event the system is left unattended for greater than fifteen (15) minutes.
- In the event the system is automatically logged off, the system will generate a report identifying the user who left the system unattended.
- This information will be given to the Security Officer for review and possible workforce disciplinary action.

If authenticating workforce members, business associates or other authorized persons telephonically, the Practice shall use a telephone callback procedure that includes a series of predetermined questions and expected "answers" to validate the authenticity of the individual requesting the ePHI.

If authenticating workforce members, business associates or other authorized persons biometrically, the practice shall utilize a biometric identification system that meets NIST guidelines, including, as applicable, hand print, retinal scan, iris scan, fingerprint, facial characteristics, DNA sequencing, voice print or hand written signature.

If authenticating workforce members, business associates or other authorized persons with a token, the Practice shall:

- Assign a unique token device to each workforce member, business associate or other authorized person.
- Prohibit workforce members from lending their assigned token to others for accessing PHI.
- Record token sign-on as part of the routine log-in monitoring and access reporting procedures.

§ 23 Transmission Security Controls.

Purpose. To ensure the security of all ePHI transmitted electronically.

Policy. It is the policy of the Practice to implement reasonable and appropriate technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.

Procedures. The Security Officer shall implement security measures, as appropriate, to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed. In addition, a mechanism to encrypt ePHI will be implemented, whenever deemed appropriate. Encryption methods shall comply with the U.S. Department of Health and Human Services Guidance on Methodologies for Rendering Protected Health Information Unusable, Unreadable or Indecipherable to Unauthorized Persons, as promulgated from time to time.

Part V. Organizational Requirements

§ 24 Group Health Plan Security Policy. [If Applicable]

Purpose. To ensure that the Practice's group health plan documents will reasonably and appropriately safeguard ePHI created, received, maintained, or transmitted to or by the Practice on behalf of the Practice's group health plan.

Policy. It is the policy of the Practice to ensure that all ePHI created, received, used or disclosed by the Practice's group health plan components, if any, are reasonably and appropriately protected by administrative, physical and technical safeguards, as provided under the HIPAA Security Rules.

Procedures. The Practice's Security Officer, in consultation with the Privacy Officer, shall oversee and be responsible for the group health plan's compliance with the HIPAA Security Rules. The Practice's HIPAA Security Policies and Procedures shall be applicable to all ePHI created, received, used, disclosed, maintained or transmitted by or on behalf of the Practice's group health plan components. The group health plan documents will be amended to incorporate provisions that require the Practice, when applicable, to:

- Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that it creates, receives, maintains, or transmits on behalf of the plan;
- Ensure that the adequate separation required by § 164.504(f)(2)(iii) of the HIPAA Privacy Rules is supported by reasonable and appropriate security measures;
- Ensure that any agent, including a subcontractor, to whom it provides ePHI, agrees to implement reasonable and appropriate security measures to protect the information; and
- Report to the group health plan any security incident of which the Practice becomes aware.

§ 25 Updates and Record Retention.

Purpose. To establish procedures under which the Practice will maintain and update reasonable and appropriate security policies and procedures and documentation to comply with the HIPAA Security Rules.

Policy. In accordance with 45 C.F.R. § 164.306(e) of the HIPAA Security Rules, it is the policy of the Practice to:

- Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of the HIPAA Security Rules, taking into account those factors specified in 45 C.F.R. § 164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of the HIPAA Security or Privacy Rules. The Practice may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with the HIPAA Security Rules;

- Maintain the policies and procedures implemented to comply with the HIPAA Security Rules in written (which may be electronic) form;

- If an action, activity, assessment or policy is required by the HIPAA Security Rules to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment; and

- See also: Evaluation § 14 above.

Procedures. The following implementation specifications shall be established and maintained by the Practice, under the direction of the Security Officer:

- Time limit. Retain all required documentation related to these Policies and Procedures, and any other agreements, reports, analyses or other documentation required under the HIPAA Security Rules, for six (6) years from the date of its creation or the date when it last was in effect, whichever is later.

- Availability. Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

- Updates. Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the ePHI.

§26 Amendment.

These Policies and Procedures may be updated and amended as necessary only by the Practice's Security Officer, or his or her designee, [with approval of the Practice's Board of Directors/Managers or Administrator]. The Practice will take such action to amend these Policies and Procedures from time to time as is necessary for the Practice to comply with the requirements of HIPAA. In the event that this Agreement is not timely amended to comply with HIPAA or other required applicable law or regulations as promulgated from time to time, these Policies and Procedures shall be deemed to incorporate such requirements.

_____

[Signature of Employee/ Name and position] [Date]

_____

[Security Officer or Practice Manager's signature, name and title] [Date]

Adopted effective _____
Revised: _____