SUPERIOR VISION

SUPERIOR VISION CORP.
AND SUBSIDIARIES

HIPAA Privacy Rule
Policies &
Procedures

Last Revision Date: December 22, 2014

SUPERIOR VISION CORP. AND SUBSIDIARIES
PRIVACY POLICIES AND PROCEDURES

TABLE OF CONTENTS

INTRODUCTION.

GENERAL

Superior Vision Corp. is the parent company of the following subsidiaries which are engaged in various aspects of the vision benefit management business: Superior Vision Services, Inc. ("SVS"); Superior Vision Insurance, Inc. ("SVI"); Superior Vision Benefit Management, Inc. ("SVBM"); Block Vision of Texas, Inc. d/b/a/ Superior Vision of Texas ("SVT"); Superior Vision of New Jersey, Inc. ("SVNJ"); UVC Independent Practice Association, Inc. ("UVC"); Superior Vision Insurance Plan of Wisconsin, Inc. ("SVIP"); and Vision 21 Managed Eye Care of Tampa Bay, Inc. d/b/a/ Eye Specialists ("Eye Specialists"). For purposes hereof, Superior Vision Corp. and its subsidiaries may be collectively referred to as the "Company" and such subsidiaries may be collectively referred to as the "Subsidiaries" or individually referred to as a "Subsidiary".

Individual privacy has always been an important issue to the Company. The Company respects the privacy of health information and has enacted procedures to ensure that private health information is not used or released inappropriately. As a result of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the federal Standards for Privacy of Individually Identifiable Health Information promulgated thereunder at 45 C.F.R. part 160 and part 164, subparts A and E (the "Privacy Rule"), covered entities (health plans, health care providers and health care clearinghouses) are subject to a uniform set of federal standards regarding the confidentiality of individual protected health information ("PHI"). To further the Company's goals regarding individual privacy and to maintain compliance with HIPAA, these Privacy Policies and Procedures have been adopted to comply with the HIPAA Privacy Rule effective April 14, 2003, as thereafter amended by the HITECH Act effective September 23, 2009, and the Final Omnibus Rule effective September 23, 2013. The Company will update these Privacy Policies and Procedures, as applicable, to maintain compliance with these privacy laws.

APPLICABILITY

These Privacy Policies and Procedures apply to Superior Vision Corp. and its Subsidiaries to the extent that such Privacy Policies and Procedures are applicable to the various business activities of each of such entities. The various business activities of the Subsidiaries are as follows:

SVS, SVBM, SVNJ, Eye Specialists, and UVC provide comprehensive management of wellness vision programs and/or medical/surgical eye care programs on behalf of health care plans and other payors which are "covered entities" under HIPAA. In their capacity as vision benefit managers, none of these Subsidiaries are "covered entities" under HIPAA and, therefore, certain

provisions of the Privacy Rule, such as the HIPAA privacy notice requirements, are not applicable to such Subsidiaries.

SVT is licensed as a Texas single service HMO. SVT acts both as a Provider HMO and as a health plan. As a health plan, SVT enrolls eligible employees in its group vision plan and arranges for the provision of wellness vision benefits to such members through its network of participating providers. As a health plan, SVT is a "covered entity," has a direct customer relationship with its members and sends privacy notices to such members. In its capacity as a Provider HMO, SVT provides comprehensive management of wellness vision programs on behalf of managed healthcare plans and other payors which are "covered entities" under HIPAA, and does not have a direct customer relationship with the members for whom it is arranging care. Thus, SVT is not required to provide privacy notices to members enrolled through its client health plans.

SVIP is licensed as a Wisconsin limited service health organization. SVIP acts both as a health plan offering wellness vision benefits to employer groups and as a reinsurer of wellness vision benefits administered by its affiliates, SVBM and SVNJ, which are underwritten by another insurance company. As a health plan, SVIP is a "covered entity," enrolling eligible employees in its group vision plans and arranging for the provision of covered vision care services to such enrollees through its network of participating providers. In its capacity as a health plan, SVIP has a direct customer relationship with its enrollees and issues privacy notices to such enrollees. SVI is licensed as an Arizona disability (health) insurer. SVI acts as a reinsurer of wellness vision benefits administered by its affiliate, SVS, which are underwritten by another insurance company.

Due to the nature of the activities performed by (i) SVS, SVBM, SVT in its capacity as a Provider HMO, SVNJ, UVC, and Eye Specialists in connection with their respective management of vision and/or eye care benefit programs on behalf of HMOs and other third party payors, and (ii) SVI as a reinsurer of vision plans administered by SVS that are underwritten by another insurance company, and SVIP as a reinsurer of vision plans administered by SVBM or SVNJ that are underwritten by another insurance company, each of these Subsidiaries may be a "business associate" of their respective "covered entity" clients. Although the activities of such Subsidiaries may also come within the definition of a "health care clearinghouse" to the extent such activities do come within such definition, it is the intent of such Subsidiaries to perform the role of a health care clearinghouse only in their capacity as a "business associate" of their client health plans. Regardless of the Subsidiaries' status as "business associates," the Subsidiaries must independently comply with the applicable sections of the HIPAA Privacy Rule, the HIPAA Security Rule, and the Breach Notification Rule.

QUESTIONS

Any questions or concerns regarding these Privacy Policies and Procedures should be directed to the Privacy Officer.

PROTECTION OF INDIVIDUAL PRIVACY **POLICY: 1**
CONFIDENTIALITY
GENERAL

POLICY

The Company and its workforce (the "Company Workforce") will not use or disclose protected health information ("PHI") except as permitted by the HIPAA Privacy Rule. Uses and disclosures permitted under the HIPAA Privacy Rule are set forth in these Privacy Policies and Procedures.

PURPOSE

The HIPAA Privacy Rule restricts the use or disclosure of PHI by covered entities, unless specifically authorized. 45 CFR § 164.502.

The purpose of this policy is to provide guidance on the general rule regarding release of PHI and the definitions of the terms "use", "disclosure" and protected health information for compliance with the HIPAA Privacy Rule.

PROCEDURE

Regardless of whether a particular Subsidiary is a "covered entity" by virtue of its status as a "health plan" or "health care clearinghouse" or is a "business associate" of another covered entity, the Company and Company Workforce members may use and disclose protected health information only as set forth in these Privacy Policies and Procedures.

The term "protected health information" ("PHI") is defined in 45 CFR § 164.103, a copy of which is referenced at the end of these Privacy Policies and Procedures. Generally, protected health information is any information that does or may identify someone and relates in any way either to the provision of health care or payment for health care. This includes demographic, eligibility and enrollment information.

The term "use" is defined in 45 CFR § 164.103, a copy of which is referenced at the end of these Privacy Policies and Procedures. A "use" of PHI is defined as the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

The term “disclosure” is defined in 45 CFR § 164.103, a copy of which is referenced at the end of these Privacy Policies and Procedures. A “disclosure” of PHI is defined as the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

Questions regarding this policy or knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer.

PROTECTION OF INDIVIDUAL PRIVACY **POLICY: 2**
CONFIDENTIALITY
THIRD PARTIES

POLICY

When a third-party provides services to the Company or performs or assists in performing a function or activity on behalf of the Company that involves the access to, use and/or disclosure of PHI, the Company will require the third party to be contractually obligated for compliance with the standards, implementation specifications and other requirements of the HIPAA Privacy Rule regarding such PHI.

PURPOSE

Depending on the nature of the activities performed by a particular Subsidiary, the Subsidiary may itself be considered to be a covered entity under the HIPAA Privacy Rules 45 CFR § 160.102, or may be a business associate of another covered entity for which it provides payment or health care operation services. In its capacity as a business associate of another covered entity, a Subsidiary may be requested to sign a business associate agreement with the covered entity obligating the Subsidiary to comply, and to ensure compliance by its subcontractors, with the HIPAA Privacy Rule. The purpose of this policy is to provide guidance on how these HIPAA Privacy Rule obligations will be handled by the Company.

PROCEDURE

Except as otherwise set forth herein, any third-party that provides services to or performs or assists in performing a function or activity on behalf of the Company that involves the access to, use and/or disclosure of PHI will be considered a business associate of the Company and will sign a business associate agreement with the Company or the applicable Subsidiary. See Policy 22 (Protected Health Information – Use or Disclosure of PHI – Business Associate). Any third-party that provides services to the Company but is itself a "covered entity" in the capacity in which such services are provided, will not be required to sign a business associate agreement since it is already subject to HIPAA requirements due to its covered entity status. If a provider does nothing more than act as a provider, the provider is not a business associate and is not required to sign a business associate agreement. For example, the health care providers which contract with the Subsidiaries for participation on the Subsidiary's provider network will not be required to sign business associate agreements for such network participation. However, a health care provider that renders consulting services to the Subsidiary(ies) in connection with the quality assurance program activities of the Subsidiary(ies) and has access to PHI

relating to such consulting services will be required to sign business associate agreements for purposes of their quality assurance program participation because such services are not being provided by the health care provider in his/her capacity as a provider.

The business associate agreements will address the issue of subcontractor compliance with the HIPAA Privacy Rule for the Company. This includes, without limitation, access to PHI, accounting of PHI disclosures, limitation on disclosure of PHI, amendment of PHI, complaints regarding PHI, and confidential communication of PHI.

ADMINISTRATIVE REQUIREMENTS **POLICY: 3**
PRIVACY OFFICER DESIGNATION

POLICY

The Company will designate a Privacy Officer to be responsible for the development of the policies and procedures regarding the privacy of PHI, along with other duties that may be set forth in these Privacy Policies and Procedures. The Privacy Officer may also be the contact person who is responsible for receiving complaints regarding PHI, or one or more of the Subsidiaries may designate an individual other than the Privacy Officer to be the contact person who is responsible for receiving complaints regarding PHI for such Subsidiary. See Policy 8 (Administrative Requirements – Privacy Compliance – Complaint Procedures).

Until such time as the Company designates a new Privacy Officer, the Privacy Officer contact information is as follows:

Name:	Audrey M. Weinstein
Email:	aweinstein@blockvision.com
Telephone:	877-730-2347
Facsimile:	561-241-5126
Mailing address:	939 Elkridge Landing Rd, Suite 200 Linthicum, Maryland 21090

PURPOSE

The HIPAA Privacy Rule requires covered entities to designate a Privacy Officer to be responsible for privacy policies and procedures and other privacy rights. 45 CFR § 164.530. Even if a particular Subsidiary is not a covered entity, the designation of a Privacy Officer is intended to facilitate implementation of these Privacy Policies and Procedures by the Company.

This policy is designed to designate a privacy official and to give guidance and ensure compliance with requirements of the HIPAA Privacy Rule regarding a privacy official.

PROCEDURES

The Privacy Officer will be knowledgeable and/or trained regarding the Company's routine business activities and the policies and procedures for the secure transmission and storage of PHI, including:

The secure transmission and storage of PHI in any form;

Controlling access to PHI;

The secure management of PHI;

The proper use and disclosure of PHI at the request of the individual;

The proper use and disclosure of PHI without the authorization of the individual;

Individual authorization for the use or disclosure of PHI;

Individual rights regarding PHI;

Developing and maintaining contracts with business associates regarding the use and disclosure of PHI;

The proper use of the Notice of Privacy Practices;

The incident and contingency plan for improper release of PHI;

Auditing access to PHI; and

The maintenance of records regarding access to PHI.

Questions regarding this policy or knowledge of a violation or potential violation of this policy must be reported directly to the Chief Executive Officer of the Company.

ADMINISTRATIVE REQUIREMENTS
PRIVACY OFFICER JOB DESCRIPTION
FORM

PRIVACY OFFICER JOB DESCRIPTION

JOB SUMMARY (Brief statement summarizing main functions and purpose of the job):

The Privacy Officer oversees all activities related to compliance with applicable law governing the privacy of individual health information. This includes the development, implementation, and maintenance of policies and procedures regarding individual health information. The Privacy Officer may also serve in other capacities for the Company.

DUTIES AND RESPONSIBILITIES:

1. Oversee development and implementation of privacy policies and procedures regarding privacy of protected health information.

2. Oversee development and implementation of processes and forms to maintain the privacy of protected health information.

3. Oversee development and implementation of a regular and ongoing training program for Company Workforce regarding the use and disclosure of protected health information.

4. Oversee development and implementation of a regular program to measure effectiveness and compliance with protected health information policies and procedures.

5. Oversee development and implementation and administer a process for individuals to exercise their rights to protected health information, including a complaint process

6. Coordinate with the Security Officer in the investigation of any incident of improper acquisition, access, use or disclosure of protected health information to determine whether notification must be given to the victims of the incident. See Policy 32 (Administrative Requirements – Breach Notification).

7. Coordinate with the Human Resources department regarding appropriate employee sanctions for improper use or disclosure of protected health information.

8. Coordinate with the Security Officer regarding appropriate and reasonable security measures for electronic media containing protected health information.

9. Coordinate with the Security Officer regarding appropriate and reasonable physical security measures for protected health information.

SUPERVISION:

Function under general supervision of the Chief Executive Officer

EDUCATIONAL EXPERIENCE, TRAINING (Include Licenses and Professional Activities):

1. Minimum Education:
   Bachelor's Degree
2. Minimum Experience:
   3 years, or equivalent training
3. Minimum field-of-expertise:
   Familiarity with managed care operations and federal and state laws regarding the privacy of individual health records.

ABILITIES AND CHARACTERISTICS:

Leadership/management skills
Communication – written and oral skills
Problem identification and resolution.

ADMINISTRATIVE REQUIREMENTS **POLICY: 4**

PRIVACY COMPLIANCE

POLICY AND PROCEDURE DOCUMENTATION

POLICY

The Company will implement an electronic and written version of these Privacy Policies and Procedures with respect to protected health information, which are designed to comply with the standards, implementation specifications, or other requirements of the HIPAA Privacy Rule.

The Company will maintain documentation, in written or electronic form, of these Privacy Policies and Procedures, communications in writing, actions or activities required to be in writing, and other administrative documents for a period of at least six (6) years from the date of creation or the date when last in effect, whichever is later.

The Company will incorporate into its policies, procedures and other administrative documents any changes in the Privacy Rule. SVIP and SVT, as appropriate, will not implement a material change in policy or procedure prior to the effective date of any revised Notice of Privacy Practices which it may be required to send to its insureds, if revision of the notice is necessary.

The Company will properly document and implement any changes to policies and procedures.

PURPOSE

The HIPAA Privacy Rule requires the implementation and maintenance of policies in written or electronic form. 45 CFR §164.530 (i) and (j).

This policy is designed to give guidance and ensure compliance with provisions of HIPAA requiring covered entities to implement and maintain documentation of policies, procedures, and other administrative documents.

PROCEDURES

The Company's policies have been reasonably designed to take into account the size and type of activities undertaken by the Company with respect to protected health information.

In implementing a change in these Privacy Policies and Procedures, the Company will:

Ensure that the policy or procedure, as revised to reflect a change in the Company's privacy practice, complies with the standards, requirements, and implementation specifications of the HIPAA Privacy Rule;

Document the policy or procedure as revised;

Revise any required Notice of Privacy Practices to state the changes in practice and make the revised Notice of Privacy Practices available to direct enrollees; and

Neither SVIP, SVT nor any other Subsidiary which in the future may have direct enrollees will implement a change in policy or procedure prior to the effective date of the revised Notice of Privacy Practices sent to such Subsidiary's direct enrollees.

The Company may change policies or procedures that do not affect the content of a Notice of Privacy Practices, provided that the policy or procedure complies with the HIPAA Privacy Rule and is documented as required in this policy.

The following documentation will be maintained in an organized manner that allows necessary availability, while also ensuring the security of information:

Policies and procedures related to the use or disclosure of PHI;

Forms for the consent to use or disclose PHI;

Forms for the authorization to use or disclose PHI;

Requests for the use or disclosure of PHI;

Agreements with business associates referring to the use or disclosure of PHI;

Notice of Privacy Practices, as applicable to a particular Subsidiary and any changes made thereto; and

Individual rights forms and requests.

Questions regarding this policy or knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer.

ADMINISTRATIVE REQUIREMENTS **POLICY: 5**

PRIVACY COMPLIANCE

PROTECTED HEALTH INFORMATION SAFEGUARDS

POLICY

The Company will put in place reasonably appropriate administrative, technical and physical safeguards to protect the privacy of PHI.

PURPOSE

The HIPAA Privacy Rule requires that covered entities have in place appropriate safeguards to protect PHI. 45 CFR § 164.530(c)(1). A covered entity must have reasonable safeguards and try to limit incidental use or disclosure of PHI. 45 CFR § 164.530(c)(2). However, the HIPAA Privacy Rule does not prohibit use or disclosure of PHI that is incident to a permitted use or disclosure when appropriate safeguards are in place and the minimum necessary standard is followed. 45 CFR § 164.502(a)(1)(iii).

This policy is designed to give guidance and ensure compliance with provisions of the HIPAA Privacy Rule requiring appropriate safeguards and incidental use or disclosure.

PROCEDURES

The Privacy Officer will coordinate with the Security Officer to review and implement appropriate safeguards for PHI, taking into account financial and administrative burdens of particular safeguards.

It is not expected that Company's safeguards guarantee the privacy of PHI from any and all potential risks.

The following are examples of appropriate safeguards:

A. INTERNAL SYSTEMS

Systems Access

- Employee access to the Company's internal systems is individually assigned based upon each employee's needs in order to carry out his/her job functions.
- Users are assigned system passwords, and each employee is required to keep his/her password confidential. Sharing of user accounts is considered a violation of the Company's security policies and is subject to appropriate disciplinary action.

The system access of terminated employees is discontinued immediately upon such termination.

System Change Control Process

A System Change/Problem Form must be completed in order to identify a problem and/or request changes to existing programs.

- The Company's Security Officer, or his designee, shall evaluate all System Change/Problem Forms to determine the feasibility of the change and required resources for implementing such change.

All approved systems changes will be performed, implemented and rigorously tested in a test environment prior to being made available to users.

All original source code shall be archived and documented.

B. **E**lectronic **D**ata

1. Eligibility Data

The Company receives member eligibility files from client health plans on physical media or electronically, via either encrypted and compressed files attached to e-mail or transmission to the Company's FTP site. Access to such files is limited to the Company's Chief Information Officer and other authorized personnel. Once such eligibility files are uploaded from physical media, the files are archived for a period of time in a secure area and are thereafter deleted and/or destroyed.

2. Encounter Data

The Subsidiaries administering vision and/or eye care benefits on behalf of their client health plans may provide the client health plan with encounter data specific to each client health plan's members. Such data is transmitted to each client health plan in a compressed, encrypted or other electronic format agreed upon between the Subsidiary and each client health plan.

3. Website

Participating providers and members enrolled may access the Company's website to obtain benefits, provider and eligibility information. In order to gain access to the website, providers and members must enter the authentication information required by the Company. The Company's privacy protocols with respect to the website restrict access to protected health information through this authentication process. The Company's website also incorporates the use of Secured Sockets Layer (SSL) encryption technology that safeguards data as it travels across the internet.

Company employees must also satisfy an authentication process in order to gain access to the website. Each employee's access level is individually assigned based upon his/her needs in order to carry out his/her job function.

C. **A**utomated **T**elephone **V**oice **R**esponse **U**nit (VRU)

Participating providers and members may access the Company's VRU to obtain benefits, provider and eligibility information, as applicable. In order to gain access to the VRU, Providers must enter their provider identification number(s). Members must enter their health plan identification number and date of birth. The Company's privacy protocols with respect to the VRU restrict access to protected health information through the authentication process described above.

D. **P**hysical **S**afeguards

1. Claims

The Company receives claims from participating providers via paper submissions and electronically through the Company's website. Electronic submissions are secured through the authentication process described above. Prior to processing, paper claims are held in a locked storage unit with access restricted to designated personnel. Subsequent to processing, paper claims are archived via an optical imaging process and are thereafter destroyed. All imaged claims are stored on a secure, dedicated file server, with access limited to those employees who need access to imaged claim(s) in order to perform their duties.

The Company retains a copy of all reimbursement checks, with such copies kept in a locked storage unit, with access limited to those employees who need such access in order to perform their duties.

2. Other Paper

Access to all non-claims documentation that contains PHI, is restricted to designated personnel with the need to access such information in order to carry out their job functions. Such documentation is stored commensurate with the nature of such information in accordance with the Company's policies and procedures regarding confidential information.

While the goal is never to use or disclose PHI unless permitted by the Privacy Rule or these Policies and Procedures, incidental use or disclosure of PHI by Company Workforce members is not strictly prohibited, provided an attempt is made to reasonably limit such incidental disclosures.

Examples of permissible incidental uses or disclosures of PHI, provided reasonable safeguards are in place, are as follows:

Company Workforce members may orally coordinate services in their offices.

Company Workforce members may discuss an enrollee's claims or health condition over the phone with the individual, a provider, or a family member.

When necessary for quick, effective and quality health care, Company Workforce members may engage in communications even if incidental use or disclosure of PHI will occur.

Questions regarding this policy may be directed to the Privacy Officer or Security Officer. Knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer.

ADMINISTRATIVE REQUIREMENTS **POLICY: 6**
PRIVACY COMPLIANCE
WORKFORCE MEMBERS
TRAINING

POLICY

The Company will train Company Workforce members regarding the Company Privacy Policies and Procedures. The Company Workforce members include all workforce members who must have access to PHI in order to carry out their duties as an employee of the Company. Training will be timely and will be based upon the information necessary and appropriate for the Company Workforce members to carry out their function for the Company. Appropriate documentation of training will be maintained.

PURPOSE

The HIPAA Privacy Rule requires covered entities to train all Company Workforce members on the policies and procedures of the entity. 45 CFR § 164.530(b)(1). For new workforce members, training will occur within a reasonable time after a new Company Workforce member begins working with the covered entity. Appropriate workforce members will be trained when there are changes to the policies and procedures. 45 CFR § 164.530(b)(2).

This policy is designed to give guidance and ensure compliance with provisions of the HIPAA Privacy Rule requiring appropriate training of Company Workforce members.

PROCEDURES

Company Workforce members will be trained in the appropriate use and disclosure of PHI as set forth in these Privacy Policies and Procedures. As deemed necessary by the Privacy Officer, annual retraining may be conducted.

The training will be based upon the information necessary and appropriate for the Company Workforce member to carry out the functions of the position. The Company will document all workforce training for a period of at least six (6) years from the date of Training.

The training timeline will be as follows:

Within 10 business days of hire - new Company Workforce members dealing directly with PHI.

Within 30 business days of hire – new Company Workforce members not dealing directly with PHI

Annual Refresher Training – appropriate Company Workforce members.

Questions regarding this policy or knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer.

ADMINISTRATIVE REQUIREMENTS **POLICY: 7**
PRIVACY COMPLIANCE
WORKFORCE MEMBERS
SANCTIONS

POLICY

The Company will impose appropriate sanctions against members of the Company Workforce who fail to comply with these Privacy Policies and Procedures.

The type of sanction applied will vary depending on the severity of the violation, whether the violation was intentional or unintentional, whether the violation indicates a pattern or practice of improper access, use or disclosure of PHI, and other appropriate factors.

Company Workforce members should be aware that violations of a severe nature may result in notification to law enforcement officials as well as regulatory, accreditation, and/ or licensure organizations.

The sanctions do not apply when members of the Company Workforce appropriately exercise their right to:

File a complaint with HHS; or

Testify, assist, or participate in an investigation, compliance review, proceeding, or hearing under Part C of Title XI; or

Oppose any act made unlawful by the HIPAA Privacy Rule; provided the person has a good faith belief that the act opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of protected health information in violation of the HIPAA Privacy Rule; or

Disclose PHI to an appropriate health oversight agency; public health authority; or an attorney retained by the individual for purposes of determining the individual's legal options with regard to the whistleblower activity.

PURPOSE

The HIPAA Privacy Rule requires that covered entities have and apply appropriate sanctions against Company Workforce members who violate the privacy policies and procedures, and that the covered entity maintain documentation of such sanctions. 45 CFR § 164.530(e). Further, the HIPAA Privacy Rule prohibits covered entities from engaging in intimidating or retaliatory acts against individuals or others in certain circumstances. 45 CFR § 164.530(g).

This policy is designed to give guidance and ensure compliance with all applicable laws and regulations related to sanctioning for violating the Company's Privacy Policies and Procedures.

PROCEDURES

Depending upon the nature and circumstances of the violation, Company Workforce member sanctions may include a warning, a suspension or termination of employment.

The Privacy Officer, in conjunction with the Human Resources department, is responsible for determining the severity of Company Workforce member sanctions.

All sanctioning of employees will be documented and retained for a period of at least six (6) years from the date of discipline or the date when the discipline was last in effect, whichever is later.

Questions regarding this policy or knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer.

ADMINISTRATIVE REQUIREMENTS **POLICY: 8**
PRIVACY COMPLIANCE
COMPLAINTS
GENERAL

POLICY

The Company will provide a process for individuals to make complaints concerning the Company's Privacy Policies and Procedures regarding the use or disclosure of protected health information, or the Company's compliance with such policies and procedures, as well as appeal the Company's decision regarding complaints.

Individuals will not be required to waive their rights to file a complaint with the Department of Health and Human Services as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

Individuals or others will not be intimidated, threatened, coerced, discriminated against or have other retaliatory action taken against them for asserting their rights under the HIPAA Privacy Rule. This will include filing of complaints or appeals, testifying, assisting, participating in an investigation or compliance matter, or opposing in good faith and in a reasonable manner any act that is unlawful under the HIPAA Privacy Rule. An individual or other person or entity opposing any act will not release protected health information in violation of the HIPAA Privacy Rule.

PURPOSE

The HIPAA Privacy Rule requires covered entities to have a mechanism for receiving complaints from individuals regarding the covered entity's compliance with the privacy policies and procedures, and for documenting complaints and their disposition. 45 CFR § 164.530(d).

This policy is designed to give guidance and ensure compliance with all applicable laws and regulations related to filing complaints and appeals with the Company regarding alleged violations of the Company's Privacy Policies and Procedures.

PROCEDURE

The Company will accept complaints about any aspect of its practices regarding protected health information. See Policy 9 (Administrative Requirements – Privacy Compliance – Complaints – Procedures). Examples include individuals who believe that protected health information relating to them has been used or disclosed improperly; a workforce member of the Company has improperly handled the information; or that they have wrongfully been denied access to or opportunity to amend the information.

The Privacy Officer will be the designated contact for individuals to file complaints regarding all Subsidiaries unless any of the Subsidiaries designate a different person as the contact for individuals to file complaints. See Policy 3 – Privacy Officer Designation for the Privacy Officer contact information.

The Company provides the following anonymous reporting mechanism to its workforce members for HIPAA Privacy Rule and other compliance questions and reporting: http://intranet.blockvision.com/suggest (enter user ID - BVEMPLOYEE and password - EYEZONLY)

The Company will document all complaints and appeals received, if any, and their disposition, for a period of at least six (6) years from the date of the complaint's or appeal's creation or the date when it last was in effect, whichever is later.

Questions regarding this policy or knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer.

ADMINISTRATIVE REQUIREMENTS **POLICY: 9**
PRIVACY COMPLIANCE
COMPLAINTS/APPEALS
PROCEDURES

POLICY

The Company will promptly investigate and resolve all complaints filed about the Company's Privacy Policies and Procedures regarding the use or disclosure of protected health information, or its compliance with such policies and procedures, as well as appeals of the Company's decision regarding a complaint.

PURPOSE

The HIPAA Privacy Rule requires covered entities to have a process for receiving complaints from individuals regarding the covered entity's compliance with the privacy policies and procedures, and for documenting complaints and their disposition. 45 CFR § 164.530(d).

This policy is designed to give guidance and ensure compliance with all applicable laws and regulations related to filing complaints and appeals with the Company regarding alleged violations of the Company's Privacy Policies and Procedures.

PROCEDURE

Any complaints concerning violation of the HIPAA Privacy Rule or the Company's Privacy Policies and Procedures must be documented in writing. See Administrative Requirements – Privacy Compliance – Complaints – Complaint Form. Complaints will be investigated thoroughly and resolved promptly. Appropriate corrective action will be taken to ensure future compliance. Complete documentation must be maintained for future reference and audit. The Company will gather as much information as possible about the complaint in question. The Privacy Officer may investigate the complaint or may designate an investigator.

The following information will be collected on the Individual Complaint Form:

date and time the complaint was reported; name of the complaining party and contact phone number (unless person wants to remain anonymous); nature of the alleged violation; identification of the individual(s) suspected

to be involved; and date and time of the incident or event giving rise to the complaint.

The Privacy Officer will coordinate the investigation until the complaint is resolved. The designated investigator(s) will carry out an investigation appropriate for the circumstances of the complaint. Where appropriate, legal counsel may be consulted. The investigative process will be documented on the Complaint Investigation Form.

The designated investigator(s) will:

Gather and analyze the relevant facts by reviewing necessary documents and conducting interviews;

If additional information is needed to proceed and the name of the complainant is known, contact the complainant for more information;

If the complaint does not merit further investigation, the analysis of the supporting facts which led to such conclusion will be documented.

Upon completion of the investigation, complete the Complaint Investigation Form.

The Privacy Officer will review the results and recommendations with the designated investigator(s). A copy of the results and recommendations will be forwarded to the Company's Compliance Committee. The disciplinary or corrective actions should then be implemented as directed. The resolution of the complaint should be logged on the Complaint Investigation Form.

Corrective actions to be taken:

Employees or other workforce members who have violated the HIPAA Privacy Rule, or Company Privacy Policies and Procedures will be subject to corrective action, up to and including discharge, see Policy 7 (Administrative Requirements – Privacy Compliance – Workforce Members – Sanctions);

Business Associates who have violated the HIPAA Privacy Rule, or Company policies or procedures will be asked to correct the violation. If a business associate fails to do so, The Company may seek to terminate the agreement with the business associate, if feasible, or if not feasible, report the business associate to the Department of Health and Human Services.

Mitigation of the harmful effects of any impermissible acquisition, access, use or disclosure of protected health information, to the extent practicable, will be taken by Company. See Policy 10 (Administrative Requirements – Privacy Compliance – Mitigation of Violation) and Policy 32 (Administrative Requirements – Breach Notification).

A complainant who is not satisfied with the Company's decision regarding his/her complaint may appeal such decision, in writing. The Privacy Officer will appoint an Appeal Committee to review each appeal, with members of the committee selected based upon the nature of the alleged violation. The Appeal Committee will review all information gathered as part of the complaint process, as described above, as well as any information submitted by the appellant and/or his/her representative as part of the appeal process. The Company will send the appellant a letter notifying him/her of the Company's determination regarding the appeal.

The Company will document all complaints and appeals received, if any, and their disposition, for a period of at least six (6) years.

Questions regarding this policy or knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer.

INDIVIDUAL COMPLAINT FORM

Member Name:_____ Member #:_____

Address: _____Phone #: _____

Name of Person Reporting: _____

If other than member above:

Relationship to member: _____

Phone #:_____

Address: _____

Date Received: _____ Time Received:_____ Received By_____

Report Received: ___In Person ___ Telephone ___ Mail (please attach)

Specifics of Report (include date and time of incident and names of individuals involved):

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

COMPLAINT INVESTIGATION FORM

Member Name:_____ Member #:_____

Name of Investigator(s):_____
_____

Date of Complaint: _____ (attach completed Individual Complaint Form)

Individuals Interviewed (include date/time and attach written statements):

Documents Reviewed):

Summary and Conclusions of Investigation (attach additional pages if necessary):
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Recommended Sanctions, Corrective or Disciplinary Action (if any):

_____
_____
_____
_____
_____
_____
_____
_____

Recommended Mitigation Steps (to the extent practicable):

_____
_____
_____
_____
_____

Corrective Action Taken: (include action taken and date of action):

_____
_____
_____
_____
_____

_____ _____
Investigator Signature Date

_____ _____
Investigator Signature Date

_____ _____
Privacy Officer Signature Date

ADMINISTRATIVE REQUIREMENTS **POLICY: 10**
PRIVACY COMPLIANCE
MITIGATION OF VIOLATION

POLICY

The Company will mitigate, to the extent practicable, any harmful effects of a use or disclosure of protected health information that violates these Privacy Policies and Procedures or the HIPAA Privacy Rule.

PURPOSE

The HIPAA Privacy Rule requires covered entities to mitigate, if practical, the impermissible acquisition, access, use or disclosure of protected health information by the covered entity or a business associate of the covered entity. 45 CFR 164.530(f). This mitigation may include written notification to the victims of the impermissible act(s) if the act(s) compromises the security or privacy of the protected health information. See Policy 32 (Administrative Requirements – Breach Notification). 45 CFR 164.404.

This policy provides guidance to ensure compliance with the HIPAA Privacy Rule regarding the mitigation of inappropriate acquisition, access, use or disclosure of protected health information.

PROCEDURE

Any workforce member or business associate that in good faith suspects that protected health information has been used or disclosed in violation of these Privacy Policies and Procedures or the HIPAA Privacy Rule will utilize the complaint procedures included in these Privacy Policies and Procedures. See Policy 8 (Administrative Requirements – Privacy Compliance – Complaints - General).

The Company will document all steps taken to mitigate an impermissible use or disclosure of protected health information, if any, for a period of at least six (6) years from the date the mitigation or the date when mitigation steps were last in effect, whichever is later.

Questions regarding this policy or knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer.

NOTICE OF PRIVACY PRACTICES **POLICY: 11**

CONTENT OF NOTICE OF PRIVACY PRACTICES

GENERAL

POLICY

Any Subsidiary that is a health plan under HIPAA and has direct enrollees will have a Notice of Privacy Practices that notifies individuals regarding the use or disclosure of their protected health information, their rights with respect to such uses or disclosures, and such Subsidiary's legal duties under the HIPAA Privacy Rule.

The content of the Notice of Privacy Practices will be in compliance with the HIPAA Privacy Rule and will comply with these Privacy Policies and Procedures.

PURPOSE

The HIPAA Privacy Rule requires that notice be given to individuals, except for inmates, of the use and disclosure of protected health information as well as the individual's rights and the health plan's legal duties with respect to use and disclosure of protected health information. 45 CFR 164.520.

This policy provides guidance to ensure compliance with the HIPAA Privacy Rule by a Subsidiary that is a health plan with direct enrollees regarding the content of the Notice of Privacy Practices of such Subsidiary.

PROCEDURES

Notice given to an individual regarding the use and disclosure of protected health information must be written in plain language and contain the statement prominently displayed: "*THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY*."

The Notice must contain descriptions in sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required by the HIPAA Privacy Rule and other applicable laws, including:

A description and at least one example, of the types of uses and disclosures that the Subsidiary is permitted by law to make for each of the following purposes: treatment, payment, and health care operations.

A description of each of the other purposes for which the Subsidiary is permitted or required by the HIPAA Privacy Rule to use or disclose protected health information without the individual's written authorization.

Information on when the Subsidiary will disclose protected health information without the individual's authorization including uses and disclosures required by law.

If a use or disclosure described is prohibited or materially limited by other laws, the description of the use or disclosure must reflect the more stringent law.

The Notice must also contain the following statements or information:

A statement indicating that other uses and disclosures will be made only with the individual's written authorization and that the individual may revoke such authorization as permitted by the individual's rights under HIPAA;

A statement that all communications about health-related products or services for which the covered entity receives financial remuneration in exchange for making the communication from or on behalf of a third party whose product or service is being described are marketing and require an authorization;

A statement that sales of medical information (subject to certain exceptions under HIPAA) require an authorization;

A statement of the individual's rights with respect to his or her protected health information and a brief description of how the individual may exercise those rights;

The right to request restrictions on certain uses and disclosures of protected health information;

A statement that genetic information will not be used or disclosed for underwriting purposes.

A statement that the Subsidiary is not required to agree to a requested restriction;

The individual's right to receive confidential communications of protected health information, as applicable;

A statement and a brief description of how the individual may exercise his/her right to inspect, copy, amend, and receive an accounting of Disclosures of protected health information;

A statement and a brief description of how the individual may exercise his/her right to obtain a paper copy of the Notice of Privacy Practices from the Subsidiary if the individual has agreed to receive the Notice electronically;

A statement that the Subsidiary is required by law to maintain the privacy of protected health information and is required to provide individuals with

notice of the Subsidiary's legal duties and privacy practices with respect to protected health information;

A statement that the Subsidiary is required to abide by the terms of the Notice that is currently in effect;

A statement that the covered entity is required to notify affected individuals in the event of a breach (see Policy 32);

A statement indicating that, for protected health information that it created or received prior to issuing a revised Notice, the Subsidiary reserves the right to change the terms of its Notice and to make the new Notice provisions effective for all protected health information that it maintains;

A statement that the Subsidiary will promptly revise and distribute its Notice whenever there is a material change to the uses or disclosures, the individual's rights, the covered entity's legal duties, or other privacy practices stated in the Notice, and how it will provide individuals with the revised Notice;

A statement that individuals may complain to the Subsidiary and to the Department of Health and Human Services if they believe their privacy rights have been violated;

A brief description of how an individual may file a complaint with the Subsidiary;

A statement that the individual will not be retaliated against for filing a complaint;

The name, or title, and telephone number of a person or office of the Subsidiary to contact for further information concerning the Notice of Privacy Practices;

The date on which the Notice is first in effect, which is not to be earlier than the date on which the Notice is printed or otherwise published.

If the Subsidiary chooses to apply and describe more limited uses or disclosure in its Notice than required under the HIPAA Privacy Rule, then it will ensure that it does not include in the Notice a limitation affecting its right to make a use or disclosure that is required by law or permitted to avert a serious threat to health and safety.

The Subsidiary will promptly revise and redistribute its Notice whenever there is a material change to the uses or disclosures, the individual's rights, the Subsidiary's legal duties, or other privacy practices stated in the notice.

The Subsidiary will not implement a material change to any term of the Notice of Privacy Practices prior to the effective date of the Notice of Privacy Practices in which such material change is reflected, except when required by law.

Upon making a change to a Subsidiary's Notice of Privacy Practices or these Privacy Policies and Procedures, due to a change in applicable law, the Company will use the notice revision date as the new effective date. However, the Company may change policies or procedures that do not affect the content of the Subsidiary's Notice of Privacy Practices, provided that the policy or procedure complies with the HIPAA Privacy Rule and is documented as required in this policy.

Questions regarding this policy or knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer.

NOTICE OF PRIVACY PRACTICES **POLICY: 12**
PROVISION OF NOTICE
GENERAL

POLICY

Any Subsidiary that is a health plan under HIPAA that has direct enrollees will provide a formal Notice of Privacy Practices to the individuals that are its direct enrollees regarding the use or disclosure of protected health information as required by the HIPAA Privacy Rule.

The Subsidiary's provision of the Notice of Privacy Practices given to such individuals regarding the use and disclosure of protected health information will comply with these Privacy Policies and Procedures.

PURPOSE

The HIPAA Privacy Rule requires that notice be given to individuals, except for inmates, of the use and disclosure of protected health information as well as the individual's rights and a covered health plan's legal duties with respect to protected health information. 45 CFR § 164.520(a)(1).

This policy provides guidance to ensure compliance with the HIPAA Privacy Rule regarding the provision of the Notice of Privacy Practices to individuals by a covered "health plan" Subsidiary that has direct enrollees.

PROCEDURES

The Notice of Privacy Practices will be provided to individuals with whom the Subsidiary has a direct enrollment relationship, and/or to the group through which the individual is enrolled, as follows:

At the time of enrollment to the named insured for all individuals who are new enrollees;

Upon request of any enrollee;

Within 60 days of a material revision of the Notice of Privacy Practices;

No less frequently than once every three years, the Subsidiary must notify the named insured for all enrollees of the availability of the Notice and how to obtain the Notice;

Automatically and contemporaneously for electronic notices, when the response is to the individual's enrollment and the enrollment is electronic.

The individual who is the recipient of an electronic Notice retains the right to obtain a paper copy of the Notice from the Subsidiary upon request.

The Subsidiary will prominently post the Notice of Privacy Practices on its web site that provides information about its customer services or benefits, and will make the notice available electronically through the web site.

When providing the Notice of Privacy Practices to the group through which the individual is enrolled or to an individual by e-mail, the Subsidiary will:

Ensure that the group on behalf of the individual or the individual has agreed to electronic Notice and such agreement has not been withdrawn;

Provide a paper copy of the Notice to the group on behalf of the individual or the individual if the Subsidiary knows that an e-mail transmission of the electronic notice has failed.

The Subsidiary will document compliance with and maintain the Notice of Privacy Practices by retaining copies of the notices issued by the Subsidiary for a period of at least 6 years from the date of its creation or the date when it last was in effect, whichever is later.

Questions regarding this policy or knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer.

NOTICE OF PRIVACY PRACTICES
PROVISION OF NOTICE
FORM

[Covered Entity Name]NOTICE OF PRIVACY PRACTICES

Last Revision Date: September 23, 2013

THIS NOTICE DESCRIBES:

(1) HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED; AND

(2) HOW YOU CAN GET ACCESS TO THIS INFORMATION.

PLEASE REVIEW IT CAREFULLY.

CONTACT INFORMATION

If you have any questions about his notice, please contact:

Name: _____
Address: _____
Telephone: _____

OUR DUTIES REGARDING YOUR MEDICAL INFORMATION

We understand that medical information about you and your health is personal. We are committed to protecting medical information about you.

This notice will tell you about the ways in which we may use and disclose medical information about you. We also describe your rights and certain obligations that we have regarding the use and disclosure of your medical information.

We are required by law to:

Make sure that medical information identifying you is kept private;

Give you this notice of our legal duties and privacy practices with respect to medical information about you; and

Follow the terms of our notice that is currently in effect.

We are also required by law to notify affected individuals following a breach of their unsecured medical information in accordance with applicable law.

HOW WE MAY USE & DISCLOSE MEDICAL INFORMATION ABOUT YOU.

The following categories describe different ways that we use and disclose medical information. For each category of uses or disclosures, we will explain what we mean and try to give some examples. Not every use or disclosure in a category will be listed. However, all of the ways we are permitted to use and disclose information will fall within one of the categories.

- **For Treatment.** We may use medical information about you to arrange for the provision of optometric treatment or services to you. We may disclose medical information about you to optometrists, doctors, technicians, or other personnel who are involved in rendering services to you. We also may disclose medical information about you to people who may be involved in or pay for your optometric care, such as family members.
- **For Payment.** We may use and disclose medical information about you so that the treatment and services you receive from health care providers may be billed by them to us and so that payment may be made by us to those providers and collected from you, other insurance companies or third parties. For example, we may receive information from your optometrist about an eye examination you received at such optometrist's office so that we may pay your optometrist for the exam. We may also talk to your optometrist prior to your receiving an eye examination to verify your eligibility for such services in order to determine whether we will cover the services.
- **For Health Care Operations.** We may use and disclose medical information about you for our health care operations. These uses and disclosures are necessary to operate our business and to make sure that all of the individuals enrolled with our plan receive quality care. For example, we may use medical information to review the services rendered by a participating provider to evaluate the performance of the provider in caring for you. We may also combine medical information about many people covered by the plan to evaluate and/or make changes to the benefits covered by the plan. We may also disclose medical information to health plan sponsors (usually employers) for purposes of administering the plan.
- **Health-Related Benefits and Services.** We may use and disclose medical information to tell you about health-related benefits or services that may be of interest to you. We will not seek or accept direct or indirect payment from a third party for communicating to you about these benefits or services without first obtaining your written permission.

- **Marketing.** We will not use or disclose medical information for marketing purposes, except that we may use or disclose medical information about you when we have face-to-face conversations with you about products or services that may be beneficial to you. We will not seek or accept direct or indirect payment from a third party in exchange for communicating to you about these products or services without first obtaining your written permission.
- **Sale**. We will not sell to any third party the right to use, access or disclose your medical information without your written permission except as specifically permitted by law.
- **As Required By Law.** We will disclose medical information about you when required to do so by federal, state or local law. For example, we may disclose medical information about you to a health oversight agency for activities authorized by law or we may disclose medical information about you in response to a court or administrative order or in connection with a legal proceeding (such as a subpoena or a discovery request).

OTHER USES OF MEDICAL INFORMATION

Other uses and disclosures of medical information not permitted by this notice or the laws that apply to us will be made only with your written permission. If you provide us permission to use or disclose medical information about you, you may revoke that permission, in writing, at any time. If you revoke your permission, we will no longer use or disclose medical information about you for the reasons covered by your written permission. You understand that we are unable to take back any disclosures we have already made with your permission.

We will not use or disclose your genetic information for underwriting purposes.

YOUR RIGHTS REGARDING MEDICAL INFORMATION ABOUT YOU.

You have the following rights regarding medical information we maintain about you:

- **Right to Request Restrictions.** You have the right to request a restriction or limitation on the medical information we use or disclose about you for treatment, payment or health care operations. You also have the right to request a limit on the medical information we disclose about you to someone who is involved in your care or the payment for your care, like a family member or friend. We are not required to agree to your request. If we do agree, we will comply with your request unless the information is needed to provide you emergency treatment.

  To request restrictions, you must make your request in writing to the contact person/office first set forth above.

A Request for Limitation Form for making your request will be provided upon request. In your request, you must tell us (1) what information you want to limit; (2) whether you want to limit our use, disclosure or both; and (3) to whom you want the limits to apply, for example, disclosures to your spouse.

- **Right to Request Confidential Communications.** You have the right to request that we communicate with you about medical matters in a certain way or at a certain location. For example, you can ask that we only contact you at work or by mail**.**

  To request confidential communications, you must make your request in writing to the contact person/office first set forth above. A Request for Confidential Communication Form for making your request will be provided upon request. We will not ask you the reason for your request. We will accommodate all reasonable requests. Your request must specify how or where you wish to be contacted, and must contain a statement to the effect that you could be endangered if we disclose all or part of your medical information in a certain way or at a certain location.

- **Right to Inspect and Copy.** You have the right to inspect and copy medical information that may be used to make decisions about your care. Usually, this includes medical and billing records, but does not include information compiled in anticipation of a legal proceeding.

  To inspect and copy (including an electronic copy) medical information that may be used to make decisions about you, you must submit your request in writing to the contact person/office first set forth above.

  A Request for Access Form for making your request will be provided upon request. If you request a copy of the information, we may charge a fee for the costs of copying, matting or other supplies associated with your request and will provide you with access and/or copies within 30 days.

  We may deny your request to inspect and copy in certain very limited circumstances. If you are denied access to medical information, you may request that the denial be reviewed. A licensed health care professional of our choosing will review your request and the denial. The person conducting the review will not be the person who denied your request. We will comply with the outcome of the review.

- **Right to Amend.** If you feel that medical information we have about you is incorrect or incomplete, you may ask us to amend the information. You have the right to request an amendment for as long as the information is kept by or for us.

  To request an amendment, your request must be made in writing and submitted to the contact person/office first set forth above. In addition, you must provide a reason that supports your request. A Request to Amend Form for making your request will be provided upon request.

We may deny your request for an amendment if it is not in writing or if it does not include a reason to support the request. In addition, we may deny your request if you ask us to amend information that:

- Was not created by us, unless the person or entity that created the information is no longer available to make the amendment;
- Is not part of the medical information kept by or for the plan;
- Is not part of the information which you would be permitted to inspect and copy; or
- Is accurate and complete.

➢ **Right to an Accounting of Disclosures.** You have the right to request an "accounting of disclosures." except for certain disclosures that do not require an accounting such as disclosures to carry out treatment, payment and health care operations, disclosures about you to you, and disclosures incident to a permitted or required use and disclosure. This accounting is a list of the disclosures of medical information about you that we have made.

To request this list of disclosures, you must submit your request in writing to the contact person/office first set forth above. A Request for Accounting of Disclosures Form for making your request will be provided upon request. Your request must state a time period which may not be longer than six years. Your request should indicate in what form you want the list (for example, on paper or electronically). The first list you request within a 12 month period will be free. For additional lists, we may charge you for the costs of providing the list. We will notify you of the cost involved and you may choose to withdraw or modify your request at that time before any costs are incurred.

➢ **Right to a Paper Copy of This Notice.** You have the right to a paper copy of this Notice. You may ask us to give you a copy of this Notice at any time. Even if you have agreed to receive this Notice electronically, you are still entitled to a paper copy of this Notice.

You may obtain a copy of this Notice at our Website, www.visionplans.com

To obtain a paper copy of this Notice, contact the contact person/office first set forth above.

➢ **Right to Notification of Unauthorized Use or Disclosure.** You have the right to receive written notification of any use or disclosure of your medical information that is not in accordance with this Notice of Privacy Practices and compromises the security or privacy of your medical information. We will provide notice as soon as reasonably possible but no later than 60 days after our discovery of the breach of the security or privacy of your medical information.

CHANGES TO THIS NOTICE

We reserve the right to change this Notice. We reserve the right to make the revised or changed Notice effective for medical information we already have about you as well as any information we receive in the future. We will post a copy of the current Notice at our Website. The Notice will contain on the first page, in the top center, the effective date.

COMPLAINTS

If you believe your privacy rights have been violated, you may file a complaint with us or with the Secretary of the Department of Health and Human Services. To file a complaint with us Company, submit the complaint in writing to:

Name: _____
Address: _____
Telephone: _____

All complaints must be submitted in writing. An Individual Complaint Form for making your request will be provided upon request. You will not be penalized for filing a complaint.

PROTECTED HEALTH INFORMATION ("PHI") **POLICY: 13**
IDENTIFYING PHI

POLICY

The Company will treat as PHI any individually identifiable health information, including demographic information collected from an individual, transmitted or maintained in any form or medium, that:

Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

Relates to either: (1) the past, present, or future physical or mental health or condition or genetics of an individual; (2) the provision of health care to an individual; or the past, present, or (3) future payment for the provision of health care to an individual; and

That identifies the individual; or

With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Routine health information meeting the above definition will be automatically designated as protected health information immediately upon its creation or receipt by Company.

PHI does not include the individually identifiable health information of individuals who have been dead for fifty (50) years. In addition, the PHI of a decedent may be disclosed to family members who were involved in the care of the decedent prior to his/her death, unless doing so is inconsistent with any express request of the decedent known to the disclosing entity.

The Company will comply with the HIPAA Privacy Rule and all applicable laws, regulations, policies, and procedures when maintaining, using, and disclosing protected health information.

PURPOSE

The HIPAA Privacy Rule protects the privacy of protected health information. 45 CFR § 164.502(a)(1).

This policy is designed to give guidance on how to properly identify and secure protected health information, as required by the HIPAA Privacy Rule.

PROCEDURES

The following information maintained or received by the Company will be designated as protected health information:

Benefit information, including eligibility data;

Reimbursement/claims information, including encounter data; and

Medical and other clinical records.

The following information maintained by Company will not be designated as protected health information:

Quality Assurance Program records, other than medical or clinical records;

Employment records regarding Company employees; and

Education records protected by the Family Educational Rights and Privacy Act ("FERPA").

In the event the nature of a record is unclear, the Privacy Officer, will be responsible for determining whether the information should be designated as protected health information.

Questions regarding this policy or knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer.

PROTECTED HEALTH INFORMATION ("PHI") **POLICY: 14**
DE-IDENTIFICATION OF PHI

POLICY

The Company may create de-identified information from protected health information. De-identification of information will be performed with appropriate administrative and technical processes only under the close supervision of the person designated by the Privacy Officer. The appointed person will have appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable. Methods of reidentification shall be secured.

De-identified information is not subject to the HIPAA Privacy Rules and may be used or disclosed without authorization. However, de-identified information will not be disclosed if those Company Workforce members creating or disclosing the information, or any other Company Workforce members, have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

PURPOSE

The HIPAA Privacy Rules allow the Company to use or disclose protected health information to a business associate for the purpose of creating de-identified information. 45 CFR § 164.502(d). Information is considered to be de-identified information when it has been stripped of any elements that may identify the individual, such as name, birth date, or social security number. 45 CFR § 164.514(a-c).

This policy is designed to give guidance on how the Company will create, use or disclose de-identified information.

PROCEDURES

The Privacy Officer will make decisions as to whether protected health information should be de-identified. The reason for de-identification will be documented and maintained.

All de-identification will be done under the supervision of the appointed person who will have appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable. The technological process for removing identifying elements from protected health information will be established by the appointed individual. The appointed person will document the methods and results used to determine that the risk of identification is very small following the de-identification of the individually identifiable health information.

In order to create de-identified information all individually identifying elements specified in the applicable Privacy Rule will be removed (ie. names, all elements of dates, social security numbers, health plan identification numbers, etc.).

If any of the required identifiers are not removed, then the information will only be disclosed if the appointed person documents the methods and results used to determine that the risk of identification is very small following the de-identification of the individually identifiable health information.

The code or other means of record identification used to re-identify information will not be derived from or related to information about the individual and should not otherwise be capable of being translated so as to identify the individual.

Questions regarding this policy or knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer.

PROTECTED HEALTH INFORMATION ("PHI") **POLICY: 15**
USE OR DISCLOSURE OF PHI
GENERAL

POLICY

Protected health information will be used or disclosed only as permitted by these Privacy Policies and Procedures and HIPAA Privacy Rule.

Once it has been determined that the requested use or disclosure of protected health information is permissible, all Company Workforce members will follow the procedures established by these Privacy Policies and Procedures.

PURPOSE

This policy is designed to give guidance on how Company Workforce members will disclose protected health information once it has been determined that the use or disclosure is permissible.

PROCEDURES

All proposed uses or disclosures of protected health information pursuant to these Privacy Policies and Procedures must be reviewed only by Company Workforce members having received appropriate training on the Company's Privacy Policies and Procedures and with the appropriate level of access. See Policy 6 (Privacy Compliance – Workforce Members – Training); and Policy 16 (Protected Health Information – Use of Disclosure of PHI – Minimum Necessary).

Company Workforce members will follow appropriate policies and procedures for verifying the identity and authority of individuals requesting use or disclosure of protected health information, See Policy 25 (Protected Health Information – Use or Disclosure of PHI – Identity Verification of PHI Requester).

Once it is determined that use or disclosure is appropriate, Company personnel with appropriate access clearance will access the individual's protected health information using proper access and authorization procedures.

The requested protected health information will be delivered to the requesting individual in a secure and confidential manner, such that the information cannot be accessed by other persons who do not have appropriate access clearance to the information.

The request and delivery of the protected health information will be appropriately documented by Company personnel.

Questions regarding this policy or knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer.

PROTECTED HEALTH INFORMATION ("PHI") **POLICY: 16**
USE OR DISCLOSURE OF PHI
MINIMUM NECESSARY

POLICY

Company Workforce members will follow proper procedures to ensure that only the minimum amount of protected health information necessary to accomplish the specific purpose of a use or disclosure of protected health information is actually used or disclosed.

Company Workforce members will request only the minimum amount of protected health information necessary to accomplish the specific purpose of the request.

This policy does not apply to the following uses or disclosures:

Disclosure to or requests by a health care provider for treatment, See Policy 17 (Protected Health Information – Use or Disclosure of PHI – Treatment, Payment and Health Care Operations);

Uses or disclosure made to the individual who is the subject of the information, See Policy 26 (Individual Rights – Access to PHI - General);

Uses or disclosure pursuant to an authorization, See Policy 18 (Protected Health Information – Use or Disclosure of PHI – Authorization - General);

Disclosure made to the HHS; and

Uses or disclosures required by law, See Policy 24 (Protected Health Information – Use or Disclosure of PHI – Required by Law).

Uses or disclosures required for compliance with 45 CFR Subchapter C.

PURPOSE

The HIPAA Privacy Rule requires covered entities to ensure that the appropriate steps are taken to disclose only the minimum amount of protected health information necessary to accomplish the particular use or disclosure. 45 CFR. §164.502(b), 164.514(d).

This policy is designed to give guidance on how Company Workforce members will comply with the minimum necessary requirements for the use or disclosure of protected health information.

PROCEDURES

The Company will maintain levels of access to protected health information for Company Workforce members for that required on a routine and recurring basis to appropriately accomplish their duties and responsibilities.

Access to protected health information will be reasonably limited to that described above through reasonable administrative, technical and physical safeguards established by the Privacy Officer in conjunction with the Security Officer. See Policy 5 (Administrative Requirements – Privacy Compliance – Protected Health Information Safeguards).

Requests for disclosures of protected health information, other than the listed levels of access identified above, will be reviewed on a case-by-case basis in accordance with criteria listed in the policy. An entire medical record will only be used or disclosed when the entire medical record is reasonably necessary to accomplish the purpose of the use, disclosure, or request.

The following criteria will be used in limiting the amount of protected health information requested, used, or disclosed by Company Workforce members:

What is the purpose of the use or disclosure?

Can a limited amount of PHI be disclosed?

Is there any risk of improper use or disclosure?

Company Workforce members may reasonably rely on requests by:

Public health and law enforcement agencies if the official represents that the information requested is the minimum necessary for the stated purpose;

Other covered entities if the covered entity represents that the information requested is the minimum necessary for the stated purpose; or

By a professional who is a member of the Company Workforce, for the purpose of providing professional services to the Company, if the professional represents that the information requested is the minimum necessary for the stated purpose.

A business associate of the Company if the business associate has agreed to appropriately safeguard the information.

Any use or disclosure under this policy and procedure will be in compliance with Policy 15 (Protected Health Information – Use or Disclosure of PHI – General).

Questions regarding this policy or knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer.

PROTECTED HEALTH INFORMATION ("PHI") **POLICY: 17**
USE OR DISCLOSURE OF PHI
TREATMENT, PAYMENT AND HEALTH CARE OPERATIONS

POLICY

The Company will comply with the requirements set forth in the HIPAA Privacy Rule to use or disclose protected health information for treatment, payment, or health care operations.

PURPOSE

The HIPAA Privacy Rule permits a covered entity to use and disclose protected health information for treatment, payment, and health care operations, subject to certain limitations. 45 CFR § 164.506.

This policy is designed to give guidance on how Company Workforce members will comply with the requirements for the use or disclosure of protected health information for treatment, payment, and health care operations.

PROCEDURE

The terms treatment, payment, and health care operations, as well as health care provider and covered entity have specific meanings that must be understood before use or disclosure pursuant to this policy.

The term "treatment" is defined in 45 CFR § 164.501, a copy of which is referenced at the end of these Privacy Policies and Procedures.

The term "payment" is defined in 45 CFR § 164.501, a copy of which is referenced at the end of these Privacy Policies and Procedures.

The term "health care operations" is defined in 45 CFR § 164.501, a copy of which is referenced at the end of these Privacy Policies and Procedures.

The term "covered entity" is defined in 45 CFR § 160.103, a copy of which is referenced at the end of these Privacy Policies and Procedures.

The term "health plan" is defined in 45 CFR § 160.103, a copy of which is referenced at the end of these Privacy Policies and Procedures.

The term “health care provider” is defined in 45 CFR § 160.103, a copy of which is referenced at the end of these Privacy Policies and Procedures.

Use or disclosure of protected health information for treatment, payment, or health care operations without authorization from an individual may occur under the following circumstances:

For the Company’s own treatment, payment, or health care operations;

For treatment activities of any health care provider;

For the payment activities of another covered entity or health care provider, as long as the recipient of the PHI is that covered entity or health care provider;

To another covered entity, for the other covered entity’s health care operations, if:

Both covered entities have or had a relationship with the individual; and

The purpose of the disclosure is for:

Conducting quality assessment and improvement activities, including: (1) outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; (2) population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and individuals with information about treatment alternatives; and related functions that do not include treatment; or

Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care

professionals, accreditation, certification, licensing, or credentialing activities; or

Health care fraud and abuse detection or compliance.

Any use or disclosure under this policy and procedure will be in compliance with Policy 15 (Protected Health Information – Use or Disclosure of PHI – General).

The Company will not use or disclose genetic information for underwriting purposes.

Questions regarding this policy or knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer.

PROTECTED HEALTH INFORMATION ("PHI") **POLICY: 18**
USE OR DISCLOSURE OF PHI
AUTHORIZATION
GENERAL

POLICY

The Company will comply with the requirements set forth in the HIPAA Privacy Rule to request authorization to use or disclose protected health information where the use or disclosure is not permitted by the HIPAA Privacy Rule or these Policies and Procedures.

To the extent that the activities of the Company constitute that of a covered entity, the Company will not condition the provision to an individual of treatment, payment, or eligibility for benefits on the provision of an authorization. Additionally, any Subsidiary that has direct enrollees will not condition enrollment in the Subsidiary's health plan on the provision of an authorization, except in limited circumstances for underwriting or risk rating determinations or certain enrollment or eligibility determinations. See Policy 19 (Protected Health Information- Use or Disclosure of PHI – Conditioning Enrollment or Eligibility).

PURPOSE

The HIPAA Privacy Rules require a covered entity to obtain authorization to use or disclose protected health information for all uses and disclosures not explicitly permitted under the HIPAA Privacy Rules. 45 CFR § 164.508.

Specifically, the following are some examples of uses and disclosures a covered entity may not make of medical information **without** authorization:

- **Marketing activities.** A covered entity may use or disclose medical information when it has face-to-face conversations with the individual about products or services that may be beneficial to him/her. It may not seek or accept direct or indirect payment from a third party in exchange for communicating to such individual about these products or services without first obtaining the individual's written permission.
- **Sale of health information.** A covered entity may not sell medical information without the applicable individual's authorization (except as specifically permitted by HIPAA).

This policy is designed to give guidance on how Company Workforce members will comply with the requirements for authorization to use or disclose protected health information.

PROCEDURE

All required authorizations will be obtained on the Company Authorization Form, or another authorization satisfying the HIPAA Privacy Rule requirements. The Company Authorization Form must be completely filled out and signed to be valid.

To be deemed a valid authorization, the following requirements must be satisfied.

The authorization will be written in plain language.

Any authorization initiated by the Company for the use or disclosure of protected health information will contain the following:

A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;

A description of each purpose of the requested use or disclosure;

The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;

The name or other specific identification of the person(s), or class of persons, to whom the Company may make the requested use or disclosure;

An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure;

Statement of the individual's right to revoke the authorization in writing and the exceptions to the right to revoke;

A description of how the individual may revoke the authorization in writing;

A statement that information used or disclosed pursuant to the authorization may be subject to redisclosure by the recipient and no longer protected by 45 CFR Part 164;

The signature of the individual; (or signature of personal representative with a description of the personal representative's authority to act for the individual and documentation of verification of that identify); and the date of the signature;

A statement that the individual may refuse to sign the authorization;

For marketing uses or disclosures, if applicable, a statement that the use or disclosure of the requested information will result in direct or indirect remuneration to the Company from a third party;

If applicable, a statement that the health plan will not condition treatment, payment, enrollment in the health plan, or eligibility for benefits on the individual's providing authorization for the requested use or disclosure, except for the health plan's eligibility or enrollment determination relating to an individual or for its underwriting or risk rating determinations.

In addition, as part of the authorization process, the Company will provide individuals with any facts they need to make an informed decision as to whether to allow disclosure of the information.

The Company will document and retain the signed authorization for a period of at least six (6) years from the date of its creation or the date when it last was in effect, whichever is later.

The Company will provide the individual with a copy of the signed authorization. The authorization will not be combined with another document to create a compound authorization, unless allowed by the HIPAA Privacy Rule and authorized by the Privacy Officer.

Any use or disclosure under this policy and procedure will be in compliance with Policy 15 (Protected Health Information – Use or Disclosure of PHI – General).

Questions regarding this policy or knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer.

PROTECTED HEALTH INFORMATION ("PHI") **POLICY: 19**

USE OR DISCLOSURE OF PHI

AUTHORIZATION

CONDITIONING ENROLLMENT OR ELIGIBILITY

POLICY

A Subsidiary with direct enrollees may, if deemed necessary within its judgment, condition enrollment or eligibility on obtaining an authorization prior to the individual's enrollment in the Company only as allowed by the HIPAA Privacy Rule.

PURPOSE

The HIPAA Privacy Rule does not allow a health plan to condition payment or the provision of treatment to an individual on the individual signing an authorization to use or disclose protected health information, except where the authorization is sought for certain eligibility or enrollment determinations. 45 CFR § 164.508(b)(4).

This policy is designed to give guidance on how Company Workforce members for a Subsidiary that has direct enrollees will comply with the requirements for authorization to use or disclose protected health information if such authorization is required.

PROCEDURE

All requests for disclosures of protected health information that require authorization will be directed to the Privacy Officer.

The Privacy Officer, in close consultation with the management of the Subsidiary directly enrolling the individual and the requesting party, will determine the nature of the request, and whether it is necessary to condition enrollment or eligibility determinations on obtaining the authorization. Such health plan Subsidiary may condition enrollment or eligibility for benefits on provision of an authorization requested by the Subsidiary prior to enrollment if the authorization is sought for eligibility of benefits or enrollment determinations for that individual or for the Subsidiary's underwriting or risk rating determinations.

If such conditions are determined necessary, then the Subsidiary will inform the individual and/or third-party, including the reason for the conditioning of enrollment or eligibility.

Any use or disclosure under this policy and procedure will be in compliance with Policy 15 (Protected Health Information – Use or Disclosure of PHI – General).

Questions regarding this policy or knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer.

PROTECTED HEALTH INFORMATION ("PHI") **POLICY: 20**
USE OR DISCLOSURE OF PHI
AUTHORIZATION
REVOCATION

POLICY

The Company will allow an individual to revoke an authorization to use or disclose their protected health information, as required by the HIPAA Privacy Rule.

The Company will take all necessary steps to honor and comply with an individual revocation of an authorization to use or disclose protected health information, unless stated otherwise in this policy.

PURPOSE

The HIPAA Privacy Rule requires covered entities to allow individuals to revoke their authorization to use or disclose protected health information. 45 CFR. § 164.508(b)(5).

This policy is designed to give guidance on how Company Workforce members will comply with the requirements allowing for revocation of authorization to use or disclose protected health information.

PROCEDURE

The Company will permit an individual to revoke authorization except in situations where:

The Company has taken action in reliance on the authorization;

The authorization was obtained as a condition of obtaining insurance coverage and other law provides the insurer with the right to contest a claim under the insurance policy or to contest the insurance policy.

The Company will not impose a time restriction on when an individual may revoke authorization to use or disclose their protected health information.

The Company will require individuals to request the revocation of authorization to use or disclose protected health information in writing.

Any use or disclosure under this policy and procedure will be in compliance with Policy 15 (Protected Health Information – Use or Disclosure of PHI – General).

Questions regarding this policy or knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer.

PROTECTED HEALTH INFORMATION ("PHI") **POLICY: 21**
USE OR DISCLOSURE OF PHI
AUTHORIZATION
INVALID AUTHORIZATION

POLICY

The Company prohibits the use of an invalid authorization to use or disclose protected health information.

PURPOSE

The HIPAA Privacy Rule does not permit covered entities to use or disclose protected health information pursuant to an authorization unless the authorization is valid. 45 CFR. § 164.508(b)(2).

This policy is designed to give guidance on how Company Workforce members will comply with the prohibition against use or disclosure of protected health information under an invalid authorization and to address how an authorization could be defective.

PROCEDURE

The Company will invalidate an authorization and cease disclosing protected health information pursuant to the authorization upon the following events:

The expiration date has passed or the expiration event is known by the Company to have occurred;

All of the required elements of the authorization have not been filled out completely, as applicable;

The authorization has been revoked;

The authorization lacks any of the required elements required for the intended use or disclosure, See Policy 18 (Protected Health Information – Use or Disclosure of PHI – Authorization – General);

The authorization is inappropriately combined with any other document to create a compound authorization.

If any material information in the authorization is known by the Company to be false.

Any use or disclosure under this policy and procedure will be in compliance with Policy 15 (Protected Health Information – Use or Disclosure of PHI – General).

Questions regarding this policy or knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer.

PROTECTED HEALTH INFORMATION ("PHI")
USE OR DISCLOSURE OF PHI
AUTHORIZATION
AUTHORIZATION FORM

AUTHORIZATION TO USE AND DISCLOSE MEDICAL INFORMATION

By signing this form you are authorizing _____("Company") to disclose (list information to be disclosed):_____
_____
_____.
to: (list persons to receive information)"_____
_____
_____

for the purpose of (list purpose of use or disclosure):_____
_____
_____

Right to Revoke Authorization. You have the right to revoke this authorization, in writing, except to the extent that we have already used or disclosed your medical information in reliance on your authorization, or if this authorization is obtained as a condition of obtaining health insurance coverage, other law provides the insurer with the right to contest action under the policy or the policy itself. To revoke your authorization, send a written request for revocation to _____ (Privacy Officer or Contact Person) at the following address: _____.

Your Medical Information May Be Re-Disclosed. When your medical information is used or disclosed pursuant to this authorization, it may be subject to re-disclosure by a person who receives your medical information. This re-disclosure may not be protected by the applicable privacy laws.

Right to Inspect and Copy Your Medical Information. You have the right to inspect and copy your medical information which is in our designated record sets. To inspect and copy such information, you must submit your request in writing to _____ (Privacy Officer or Contact Person) at the following address: _____.

You Are Not Required to Sign this Authorization. Your authorization is voluntary and you may refuse to sign this authorization. We will not require you to sign this form in order to obtain treatment or payment, except as otherwise provided on this Authorization.

Expiration Date. This authorization expires _____ (insert date or event upon which authorization expires).

_____ _____
Signature Individual Name

_____ _____
Date Authority to act for individual

THIS FORM IS IN DUPLICATE. The top Copy is for the Company's records, and the bottom Copy is for your records.

PROTECTED HEALTH INFORMATION ("PHI") **POLICY: 22**
USE OR DISCLOSURE OF PHI
BUSINESS ASSOCIATES
GENERAL

POLICY

The Company may disclose protected health information to business associates of the Company when satisfactory assurances have been received from the business associate. In order to obtain satisfactory assurances that protected health information will be safeguarded, any business associate of the Company that is not itself a covered entity will be required to enter into an appropriate written business associate agreement with Company that meets the requirements of the HIPAA Privacy Rule. Business associates of the Company also may create or receive PHI on the Company's behalf if satisfactory assurances are obtained by the Company.

PURPOSE

The HIPAA Privacy Rule allows covered entities to disclose protected health information to business associates and allows business associates to create protected health information provided satisfactory assurances are obtained through the use of a written business associate agreement. 45 CFR § 164.502(e), 164.504(e). Depending on the nature of the activities performed by a particular Subsidiary, the Subsidiary may itself be a covered entity under the HIPAA Privacy Rules, or may be a business associate of another covered entity for which it provides payment or health care operation services. In its capacity as a business associate of another covered entity, a Subsidiary may be requested to sign a business associate agreement with the covered entity obligating the Subsidiary to ensure its compliance, and compliance by its subcontractors, with the HIPAA Privacy Rule.

This policy is designed to give guidance on how protected health information will be disclosed to business associates and how satisfactory assurances will be obtained by the Company regarding safeguarding of protected health information by business associates and other subcontractors of the Company.

PROCEDURE

The term "business associate" is defined in 45 CFR § 164.501. A third-party

subcontractor that provides services to one or more Subsidiaries or performs or assists in performing a function or activity on behalf of the Company that involves the access to, use and/or disclosure of PHI will be requested to sign a business associate agreement so that the Company can either comply with the HIPAA Privacy Rule regarding business associates if such Subsidiary is itself a "covered entity" or can obtain satisfactory assurances that its third-party subcontractors will safeguard the use and disclosure of PHI in accordance with the HIPAA Privacy Rule, HIPAA Security Rule and HITECH. Business associates are subject to enforcement of the applicable HIPAA requirements by the United States Department of Health and Human Services. SVC will enter into a business associate agreement on behalf of itself and the Subsidiaries if the business associate or third-party service provider is engaged to provide services to more than one Subsidiary involving the access to and/or use and disclosure of PHI. For example, the Company's IT consultants, actuaries and accountants will sign a single business associate agreement with SVC on behalf of itself and the Subsidiaries. If a Subsidiary has a direct service relationship with a business associate and that business associate only provides services to such Subsidiary, only the Subsidiary will enter into the business associate agreement.

All business associates of the Company who are not otherwise covered entities will be required to enter into a business associate agreement prior to the disclosure by the Company of any protected health information. If a health care provider does nothing more than act as a provider, the health care provider is not a business associate and will not be required to sign a business associate agreement.

A list of all current Company business associates will be maintained, including the name of the business associate and the date of the business associate agreement.

No workforce member may enter into a service contract on behalf of the Company without first contacting the Privacy Officer to evaluate whether a business associate agreement, or equivalent terms, are required to be part of the service agreement.

The Privacy Officer or his/her designee will be responsible for negotiating appropriate terms to the business associate agreements for all business associates of the Company. Copies of all signed business associate agreements will be maintained by the Company for a period of at least six (6) years from the date of creation or the date when last in effect, whichever is later.

Once an appropriate business associate agreement has been finalized, protected health information may be disclosed to the business associate, as permitted by these Privacy Policies and Procedures and the HIPAA Privacy Rule . Any use or disclosure under this policy and procedure will be in compliance with Policy 15 (Protected Health Information – Use or Disclosure of PHI – General).

Questions regarding this policy or knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer.

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("BAA") to be effective _____, 200_ or such earlier date that BA had access to Protected Health Information/Confidential Information of SVC (the "Effective Date") is made and entered into by and among Superior Vision Corp. and its Subsidiaries (Superior Vision Corp. and its Subsidiaries are hereinafter collectively referred to as "SVC"), having a place of business at 939 Elkridge Landing Road, Suite 200, Linthicum, Maryland 21090, and _____("Business Associate" or "BA"), having a principal place of business at _____.

RECITALS:

WHEREAS, BA provides services to SVC or performs or assists in performing a function or activity on behalf of SVC that involves the access to, use and/or disclosure of Protected Health Information (as defined in 45 C.F.R. 164.501, as may be from time to time updated, amended or revised); and

WHEREAS, the parties wish to enter into this BAA in order to ensure compliance with the requirements regarding the use and/or disclosure of Protected Health Information as required by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the federal Standards for Privacy of Individually Identifiable Health Information promulgated thereunder at 45 C.F.R. part 160 and part 164, Subparts A and E (the "Privacy Rule"), as may be required under the "Security Rule" and the "Transactions Rule" 45 C.F.R. Part 160, 164, subparts A, C and E, and Part 162, and as may be required under the Health Information Technology for Economic and Clinical Health Act ("HITECH") in the American Recovery and Reinvestment Act of 2009 ("ARRA") and its implementing regulations in 45 C.F.R. Part 164, subpart D ("HITECH Rule") and in the Final HIPAA/HITECH Omnibus Rule;

WHEREAS, the parties recognize they are both subject to enforcement of the applicable HIPAA requirements by the United States Department of Health and Human Services.

NOW THEREFORE, for and in consideration of the representations, warranties and covenants contained herein, and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the parties hereto agree as follows:

I. DEFINITION OF TERMS

Terms used, but not otherwise defined, in this BAA shall have the same meaning

as those terms in the Privacy Rule, the Security Rule, the Transactions Rule or the HITECH Rule. For purposes hereof, the term "Subsidiaries" means the corporations or other entities now or hereafter owned or controlled directly or indirectly by Superior Vision Corp., including, without limitation, the following: Superior Vision Holdings, Inc.; Superior Vision Services, Inc.; Superior Vision Insurance, Inc.; Superior Vision Benefit Management,, Inc.; Block Vision of Texas, Inc. d/b/a/ Superior Vision of Texas; UVC Independent Practice Association, Inc.; Superior Vision Insurance Plan of Wisconsin, Inc.;; Vision 21 Managed Eye Care of Tampa Bay, Inc. d/b/a Eye Specialists; and Superior Vision of New Jersey, Inc.

II. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE

1. Permitted Uses and Disclosures of Protected Health Information. Except as otherwise limited in this BAA, or in any agreement between BA and SVC pursuant to which BA provides services to or performs or assists in performing a function or activity on behalf of SVC (the "Services Agreement"), BA may use and/or disclose Protected Health Information to perform the functions, activities or services for or on behalf of SVC as contemplated by the Services Agreement, provided that such use and/or disclosure would not violate the Privacy Rule or the Security Rule if done by SVC or the minimum necessary policies and procedures of SVC. Except as otherwise limited by this BAA, BA may use Protected Health Information for the proper management and administration of BA or to carry out the legal responsibilities of BA and as Required by Law.

2. Responsibilities of Business Associate With Respect to Protected Health Information. With regard to the use and/or disclosure of Protected Health Information, BA hereby agrees to the following:

(a) BA agrees to not use and/or disclose Protected Health Information other than as permitted or required by this BAA, the Services Agreement or as Required By Law.

(b) BA agrees to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information to prevent use or disclosure of Protected Health Information other than as provided for by this BAA.

(c) BA agrees to report to SVC and must require its subcontractors to report to BA (and then provide such reports to SVC), in writing and within two (2) business days, any acquisition, access, use or disclosure of Protected Health Information not provided for by this BAA of which it becomes aware, including any security incident of which BA becomes aware.

(d) BA agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by BA on behalf of SVC, agrees to the same restrictions and conditions that apply through this BAA to BA with respect to such information, including the reasonable and appropriate safeguards implementation requirement in accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2).

(e) BA agrees to provide access, at the request of SVC, and in the time and manner designated by SVC, to Protected Health Information in a Designated Record Set, to SVC or, as directed by SVC, to an Individual in order to meet the requirements under 45 C.F.R. 164.524. This provision shall be applicable only if BA has Protected Health Information in a Designated Record Set**.**

(f) BA agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that SVC directs or agrees to pursuant to 45 C.F.R. 164.526 at the request of SVC or an Individual, and in the time and manner directed by SVC. This provision shall be applicable only if BA has Protected Health Information in a Designated Record Set.

(g) BA agrees to make internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information received from, or created or received by BA on behalf of, SVC available to SVC or to the Secretary of the Department of Health and Human Services or his/her designee (the "Secretary"), in the time and manner designated by SVC or the Secretary, for purposes of the Secretary determining SVC's compliance with the Privacy Rule and the Security Rule.

(h) BA agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for SVC to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. 164.528, as modified by HITECH for electronic health records.

(i) BA agrees to provide to SVC, in the time and manner directed by SVC, information collected in accordance with Section II(2)(h) of this BAA, to permit SVC to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with C.F.R. 164.528, as modified by HITECH for electronic health records.

(j) BA shall request, use and/or disclose only the minimum amount of Protected Health Information, necessary to accomplish the purpose of the request, use or disclosure. BA shall comply with 45 CFR §§ 164.502(b) and 164.514(d).

(k) BA shall not directly or indirectly receive remuneration in exchange for any Protected Health Information as prohibited by 45 CFR § 164.502(a)(5)(ii).

(l) BA shall not make or cause to be made any communication about a product or service that is prohibited by 45 CFR §§ 164.501 and 164.508(a)(3).

3. Use and Disclosure in Connection with Standard Transactions. If BA conducts Standard Transactions (as defined in 45 C.F.R. Part 162) for or on behalf of SVC, BA will comply, and will require each subcontractor or agent involved with the conduct of such Standard Transactions to comply with each applicable requirement of 45 C.F.R. Part 162. BA will not enter into, or permit its subcontractors or agents to enter into, any agreement in connection with the conduct of Standard Transactions for or on behalf of SVC that: (i) changes the definition, data condition, or use of a data element or segment in a Standard Transaction; (ii) adds any data elements or segments to the maximum defined data set; (iii) uses any code or data element that is marked “not used” in the Standard Transactions implementation specification or is not in the Standard Transactions implementation specification; or (iv) changes the meaning or intent of the Standard Transactions implementation specification.

4. Security Rule Requirements. BA understands that it is independently required by law to comply with the Security Rule. It agrees that it will (a) implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of Electronic Protected Health Information that it creates, receives, maintains, or transmits on behalf of SVC; (b) report to SVC any acquisition, access, use or disclosure of protected health information, including all Security Incidents, of which it becomes aware in accordance with Section II.2(c) above; and (c) ensure that any agent, including a subcontractor, to whom it provides Electronic Protected Health Information agrees in writing to comply with the Security Rule by entering into a business associate agreement with BA that complies with the

requirements for business associate agreements under HIPAA and HITECH and, in accordance therewith, agrees to implement reasonable and appropriate safeguards to protect such Electronic Protected Health Information.

III. OBLIGATIONS OF SVC

1. If deemed applicable by SVC, SVC shall:

(a) notify BA of any limitation(s) in any notice of privacy practices of SVC in accordance with 45 C.F.R. 164.520 to the extent that such limitation(s) may affect BA's use or disclosure of Protected Health Information.

(b) notify BA of any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, to the extent that such changes may affect BA's use or disclosure of Protected Health Information.

(c) notify BA of any restriction to the use or disclosure of Protected Health Information that SVC has agreed to in accordance with 45 C.F.R. 164.522, to the extent that such restriction may affect BA's use or disclosure of Protected Health Information.

2. SVC shall not request BA to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by SVC.

IV. TERM AND TERMINATION

(a) Term. The term of this BAA shall be effective as of the Effective Date and shall terminate when all of the Protected Health Information provided by SVC to BA, or created or received by BA on behalf of SVC, is destroyed or returned to SVC, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such Protected Health Information in accordance with Section IV. (c) below.

(b) Termination for Cause. Upon SVC's knowledge of a material breach by BA, SVC shall, at its sole option, do any of the following:

(1) terminate the Services Agreement and this BAA; provided, however, that BA shall have the opportunity to cure the breach or end the violation within fifteen (15) days of receipt of SVC's notice of breach and neither the Services Agreement nor this BAA shall terminate if BAA cures the breach or ends the violation, to SVC's satisfaction, within such fifteen (15) day period;

(2) immediately terminate the Services Agreement and this BAA if BA has breached a material term of this BAA and cure is not possible; or

(3) if neither termination nor cure is feasible, SVC may report the

violation to the Secretary.

(c) Effect of Termination.

(1) Except as provided in paragraph (2) of this Section IV.(c), upon termination of this BAA or the Services Agreement for any reason, BA shall return or destroy all Protected Health Information received from SVC, or created or received by BA on behalf of SVC. This Section IV. (c) (1) shall apply to Protected Health Information that is in the possession of subcontractors or agents of BA. BA shall retain no copies of Protected Health Information.

(2) In the event that BA determines that returning or destroying Protected Health Information is infeasible, BA shall provide in writing to SVC notification of the conditions that make return or destruction infeasible. Upon SVC's determination that return or destruction of Protected Health Information is infeasible, BA shall extend the protections of this BAA to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as BA maintains such Protected Health Information.

V. MITIGATION

SVC and BA shall cooperate and coordinate in an effort to mitigate any harmful effects from a violation of this BAA or from any incident of improper acquisition, access, use or disclosure of protected health information. BA shall not undertake any mitigation efforts without consultation with SVC.

VI. LIABILITY AND INDEMNIFICATION

Each party shall be solely liable for any violations of the Privacy, Security or HITECH Rules by its employees, agents or representatives. Any party in violation shall indemnify and hold the party not in violation harmless from any fines and penalties that are assessed by any regulatory authorities against the party not in violation as a result of the acts or omissions of the party in violation. In addition, the party in violation shall be liable for the costs and expenses (including reasonable attorneys' fees) related to any required notifications and other mitigation directed to individuals affected by the violation.

VII. CONFIDENTIALITY AND OWNERSHIP OF CONFIDENTIAL INFORMATION

(a) Confidentiality. Each party agrees: (1) to hold the other party's (the "Disclosing Party's") proprietary and confidential information (the "Confidential Information") in strict confidence, (2) to treat the Confidential Information with at least the same care and precaution as the party receiving such Confidential Information (the "Receiving Party") affords to its most confidential, valuable and secret information, (3)

not to disclose or use any Confidential Information for any purpose other than to fulfill the Receiving Party's obligations under this Agreement or to carry out the Services, (4) except as required by applicable law, not to release or disclose the Confidential Information to any third party without the prior written consent of the Disclosing Party, and (5) to return to the Disclosing Party all copies of any written or tangible Confidential Information upon termination of this Agreement. Notwithstanding the foregoing, the Receiving Party shall have no confidentiality obligation with respect to any information received from the Disclosing Party which (1) was known to the Receiving Party prior to disclosure by the Disclosing Party, (2) is lawfully obtained by the Receiving Party from a third party under no obligation of confidentiality, (3) is or becomes generally known or available other than by the Receiving Party's unauthorized disclosure, or (4) is independently developed by the Receiving Party.

(b) Ownership of Confidential Information. The parties agree that no ownership or similar rights in the Confidential Information are conferred pursuant to this Agreement.

(c) Equitable Relief. The parties agree that remedies available at law for a breach or threatened breach of this Section VII would be inadequate to protect the interests of the parties hereunder in the Confidential Information and, in recognition of this fact, it is agreed that a party shall be entitled to seek equitable relief (including, without limitation, equitable relief in the form of specific performance, a temporary restraining order, or a temporary or permanent injunction), without posting bond or other security. No remedy herein conferred is intended to be exclusive of any other remedy, and each and every such remedy shall be cumulative and shall be in addition to any other remedy available to such party.

VIII. MISCELLANEOUS

1. Regulatory References. A reference in this BAA to a section of the Privacy Rule, Security Rule, HITECH or other HIPAA standard means the section as in effect or as amended.

2. Amendment. BA and SVC agree to take such action as is necessary to amend this BAA from time to time as is necessary for SVC to comply with the requirements of the Privacy Rule, the Security Rule and HIPAA. Additionally, SVC may amend this BAA upon thirty (30) days written notice to BA and the amendment shall automatically be made a part of this BAA unless BA provides written objection to such amendment within such notice period.

3. Survival. The respective rights and obligations of BA under Section IV. (c) of this BAA regarding effect of termination shall survive the termination of this BAA and/or the Services Agreement. Additionally, the provisions of Section VI of this BAA

regarding indemnification and the provisions of Section VIII.6 of this BAA regarding construction of this BAA as a general confidentiality agreement shall survive the termination of this BAA and/or the Services Agreement.

4. Interpretation. Any ambiguity in this BAA shall be resolved to permit SVC to comply with the Privacy Rule and other applicable HIPAA standards.

5. Effect of BAA on Services Agreement. This BAA amends the Services Agreement. Except as amended by this BAA, the terms and provisions of the Services Agreement shall remain in full force and effect.

6. Confidentiality Agreement. BA agrees that the terms and conditions of this BAA shall be construed as a general confidentiality agreement that is binding upon BA even if it is determined that BA is not a business associate of SVC as that term is used in the Privacy Rule.

7. Notices. Any notice or other communication required or permitted to be given under this BAA shall be sent to the parties at their respective addresses set forth above, or to such other address designated by a party from time to time in accordance with this Section VIII. 7.

8. No Offshore PHI. No Protected Health Information will be used, accessed, received, processed, transferred, handled, or stored by BA or any employee, agent or subcontractor of BA outside of the United States and United States territories.

9. Counterparts. This Agreement may be executed in counterparts and forwarded by facsimile or electronic transmission by the parties.

IN WITNESS WHEREOF, the parties have caused this Business Associate Agreement to be signed by their duly authorized representatives.

Superior Vision Corp. on behalf of itself and its Subsidiaries	**Business Associate:**
	_____ **[print complete name]**
By: _____	By: _____
Name:	Name:
Title:	Title:
	_____ **[print title if BA is not an individual]**

PROTECTED HEALTH INFORMATION ("PHI") **POLICY: 23**
USE OR DISCLOSURE OF PHI
INVOLVEMENT IN THE INDIVIDUAL'S CARE AND NOTIFICATION

POLICY.

The Company may disclose to a family member, other relative, close personal friend, or any other person identified by the individual, protected health information that is directly relevant to such person's involvement with the individual's care or payment for the individual's health care.

The Company may use or disclose an individual's protected health information to notify, or assist in the notification of, a family member, a personal representative of the individual, or another person responsible for the care of the individual, of the individual's location or general condition.

PURPOSE

Subject to an individual's right to object, the HIPAA Privacy Rule permits a covered entity to use or disclose protected health information to an individual's family member or others involved in the individual's care in order to ensure quality care, or to notify family members or others of the individual's location, general condition or death. 45 CFR § 164.510(b).

This policy is designed to give guidance on when protected health information may be disclosed to family members, relatives, friends or others identified by the individual.

PROCEDURES

The Company will seek agreement from an individual to disclose his or her protected health information relevant to that individual's care to the individual's identified family member, friend, or any other person identified by the individual.

If necessary given the condition of the individual or critical circumstances involved, the Company may reasonably infer from the circumstances, based on the exercise of professional judgment, that the individual does not object to the disclosure of health information relevant to the individual's care or payment for care, to the individual's family member, friend, or any other person identified by the individual.

In the event that the individual is not present for, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the Company may, in the exercise of professional judgment, determine whether the disclosure is in the

best interests of the individual and, if so, disclose only the protected health information that is directly relevant to the person's involvement with the individual's health care.

Company Workforce members may use professional judgment and their experience with common practice to make reasonable inferences of an individual's best interest in allowing a person to act on behalf of the individual to obtain claim forms, explanation of benefits, or other similar forms of protected health information.

Company Workforce members will exercise professional judgment in determining that disclosing protected health information pursuant to the applicable policies and procedures herein, when the individual is present or when the individual is not present, will interfere with the ability to respond to the emergency circumstances.

Any use or disclosure under this policy and procedure will be in compliance with Policy 15 (Protected Health Information – Use or Disclosure of PHI – General).

Questions regarding this policy or knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer.

PROTECTED HEALTH INFORMATION ("PHI") **POLICY: 24**
USE OR DISCLOSURE OF PHI
REQUIRED BY LAW

POLICY

The Company may use or disclose protected health information to the extent that the use or disclosure is required by federal, state or local law and is limited to the requirements of such law.

In the event that two or more laws or regulations governing the same use or disclosure conflict, the Company will comply with the more restrictive laws or regulations.

PURPOSE

The HIPAA Privacy Rule permits a covered entity to use or disclose protected health information without the written authorization of the individual or the opportunity for the individual to agree or object to the extent that such use or disclosure is required by law so long as the use or disclosure complies with and is limited to the relevant requirements of such law. 45 CFR § 164.512(a).

This policy is designed to give guidance and ensure compliance with relevant laws and regulations when using or disclosing protected health information as required by law.

PROCEDURES

The Company may use or disclose protected health information to the extent that such use or disclosure is required by law including, but not limited to, disclosures relating to the following: public health activities by public health authorities; victims of abuse, neglect, or domestic violence; health oversight activities by health oversight agencies; judicial or administrative proceedings; law enforcement purposes; decedents; cadaveric organ, eye or tissue donation; research purposes; to avert serious threat to health or safety; or specialized government functions or other requests.

When disclosing protected health information in accordance with the above circumstances, the Company will comply with the HIPAA requirements applicable to such disclosure.

Any use or disclosure under this policy and procedure will be in compliance with Policy 15 (Protected Health Information – Use or Disclosure of PHI – General).

Questions regarding this policy or knowledge of a violation or potential violation of this policy must be reported directly to Privacy Officer.

PROTECTED HEALTH INFORMATION ("PHI") **POLICY: 25**
USE OR DISCLOSURE OF PHI
IDENTITY VERIFICATION OF PHI REQUESTER

POLICY

The Company will take necessary steps to verify the identity and legal authority of persons requesting disclosure of protected health information.

PURPOSE

The HIPAA Privacy Rule requires covered entities to ensure that the appropriate steps are taken to verify the identity and authority of persons requesting protected health information. 45 CFR §164.514(h)

This policy provides guidance and ensures compliance with applicable laws when using or disclosing protected health information.

PROCEDURES

If the identity or authority of a person requesting PHI is not known to the Company, the Company will obtain documentation, statements or representations from such person to verify his/her/its identity and authority receiving disclosure of protected health information. Company Workforce members may rely on the following, if such reliance is reasonable under the circumstances, when disclosing protected health information:

Documentation, statements, or representations that, on their face, meet the applicable requirements for a disclosure of protected health information;

If the request is by a public official, presentation of an agency identification badge, other official credentials, or other proof of government status if the request is made in person, or if the request is in writing, the request is on the appropriate government letterhead;

If the disclosure is to a person acting on behalf of a public official, evidence that the person is acting under the government's authority, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official;

If the disclosure is to a public official or person acting on behalf a public official, the Company may rely on a written statement of the legal authority under which the information is requested, or if a written statement would be impracticable, an oral statement of such legal authority. Additionally,

If a request that is made pursuant to a warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal that is presumed to constitute legal authority the Company may rely thereon.

Company Workforce members may rely on the exercise of professional judgment in making the following uses or disclosures of protected health information:

A use or disclosure to others in the involvement in the individual's care, or acting on a good faith belief in making a disclosure to avert a serious threat to health or safety.

Company Workforce members receiving a request from an individual or entity for use or disclosure of protected health information will determine whether the identity of the requesting person is known to the Company.

In the event that the identity and legal authority of an individual or entity requesting protected health information cannot be verified, personnel will refrain from disclosing the requested information and report the case to the Privacy Officer in a timely manner.

Personnel will report any discrepancies in the verification of the identity or legal authority of an individual or entity requesting protected health information to the Privacy Officer in a timely manner.

Any use or disclosure under this policy and procedure will be in compliance with Policy 15 (Protected Health Information – Use or Disclosure of PHI – General).

Questions regarding this policy or knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer.

PROTECTED HEALTH INFORMATION ("PHI") **POLICY: 26**

INDIVIDUAL RIGHTS

ACCESS TO PHI

GENERAL

POLICY

The Company will give individual's the right of access to inspect and obtain a copy of their protected health information in a designated record set in accordance with the HIPAA Privacy Rule.

PURPOSE

The HIPAA Privacy Rule permits an individual to request to see and copy his or her own protected health information. 45 CFR § 164.524. The Company does not have to give an individual information that is not in the "designated record set", nor is Company required to provide access to protected health information in certain circumstances set forth in this Policy and Procedure.

This policy provides guidance and ensures compliance with applicable laws when providing individuals with access to their protected health information.

PROCEDURE

General

The phrase "designated record set" is defined in 45 CFR § 164.501, a copy of which is referenced at the end of the policies and procedures.

The Company will document and retain the following for a period of at least six (6) years from the date of its creation or the date when it last was in effect, whichever is later:

Designated record sets that are subject to access by individuals; and

The title of persons responsible for receiving and processing requests for access to protected health information.

Any use or disclosure under this policy and procedure will be in compliance with Policy 15 (Protected Health Information – Use or Disclosure of PHI – General).

Questions regarding this policy or knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer.

Providing Access

The Company will allow an individual to access, inspect, and/or obtain a copy of their protected health information that is maintained in a designated record set in a timely and professional manner. A request for access must be in writing. A Request for Access Form may be used by the individual to request access, inspect, and/or obtain a copy of their protected health information.

Upon receipt of a request for access PHI, the Privacy Officer or his/her designee shall be responsible for responding to the request. The Response to Request for Access Form shall be used to respond to any requests.

Action on a request for access must be taken no later than 30 days after the request is made.

If the Company cannot take action on a request for access to protected health information within the time periods above; the Company may extend the time required by 30 days with notice to the individual within the original timeframe.

In instances where the protected health information is in more than one record set, or at more than one location, the Company will only produce the protected health information once in response to a request for access.

If the Company does not maintain the protected health information, but the Company is aware of where the requested information is maintained, the Company will inform the individual where to direct the request for access.

The Company will provide the individual with access to the protected health information in the form or format requested by the individual, if it is readily producible in such form or format. If the requested format is not readily producible, then the Company will provide the individual with access to the protected health information in an electronic form or, at the option of the individual, a readable hard copy form or such other form as agreed to by the Company and the individual.

If requested by the individual, the Company will arrange with the individual for a convenient time and place to inspect or obtain a copy of the protected health information, or mailing of protected health information, within the specified time period. See Policy 27 (Protected Health Information – Individual Rights – Confidential Communication of PHI).

A summary of the requested protected health information will be provided in lieu of access to the information only when the individual agrees in advance to a summary, and to any related fees imposed.

An explanation of the requested protected health information to which access has been provided will accompany the access only when the individual agrees in advance to a summary, and to any related fees imposed.

Any fees imposed on the individual for a copy of the protected health information or a summary or explanation of such information will:

Be collected by the Company prior to providing access to protected health information;

Be reasonable and cost-based;

Will be only for the cost of the following:

Copying, including the cost of supplies for and labor of copying, the protected health information requested by the individual;

Postage, when the individual has requested the copy, or the summary or explanation, be mailed; and

Preparing an explanation or summary of the protected health information.

Denying Access

A denial of access will be issued and will not be subject to review in the following circumstances:

The protected health information is:

Not maintained in the Company designated record set;

Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; or

Subject to the Clinical Laboratory Improvements Amendments of 1988, 42 USC §263a, to the extent the provision of access to the individual would be prohibited by law; or exempt from the Clinical Laboratory Improvements Amendments of 1988, pursuant to 42 CPR §493.3(a)(2).

The protected health information is contained in records that are subject to the Privacy Act, 5 USC §552a, and the denial of access under the Privacy Act would meet the requirements of that law;

The protected health information was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

A denial of access will be issued and will be subject to review, upon request by the individual, only in the following circumstances:

A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;

The protected health information makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or

The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

In denying access in whole or in part, to the extent possible, the Company will give the individual access to any other protected health information requested, after excluding the protected health information that was denied. When denying an individual access to protected health information, the denial will be on the Response to Request for Access Form

Review of Access Denial

The Company will provide for review of a denial of access to protected health information when requested by the individual, if review of the denial is authorized by this Policy and Procedure (see above).

All denial reviews will be conducted by a licensed health care professional who is designated by the Privacy Officer on a case-by-case basis and who did not participate in the original decision to deny access.

The Privacy Officer will promptly refer a request for review to the designated reviewing official.

The designated reviewing official will determine, within a reasonable period of time, whether or not to deny the access requested based on the applicable standards set forth in this Policy and Procedure (see above).

The Privacy Officer will promptly provide written notice to the individual of the determination of the designated reviewing official and take other action as required to carry out the designated reviewing official's determination.

PROTECTED HEALTH INFORMATION ("PHI")
INDIVIDUAL RIGHTS
ACCESS TO PHI
REQUEST FOR ACCESS - FORM

REQUEST TO ACCESS HEALTH INFORMATION

I request access to health information regarding _____ (insert individual name) that is maintained by _____ (the "Company") in a "designated record set" in accordance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

A "designated record set" includes information such as medical records; billing records; enrollment, payment, claims adjudication and health plan case or medical management record systems; or records used to make decisions about individuals.

I understand that this request does not apply to certain health information, including: (1) information that is not held in the designated record set; (2) information compiled in reasonable anticipation of or for litigation; and (3) other information not subject to the right to access information under HIPAA.

I am requesting the following health information (include dates, where applicable):

_____

_____

_____

_____

I request access to the information in the following format (check one box only):

Electronic (via _____)

Paper (in person review only)	Paper (in person review and copies)	Other _____
Paper (copies only)	Summary Format (extra fees will be assessed)	_____ _____

Would you like any copies requested to be mailed to you? Yes No

The fee for copies will be cost-based, including the cost of supplies and labor. Postage will be charged for any copies or summary of information that you request be mailed to you. Finally, a charge for preparation of the summary of health information will be charged if you request access in that format. By signing below you are agreeing to pay the appropriate fees prior to your receipt of the requested information.

Company has 30 days to respond to this request, and if an extension is requested, the response time is 60 days.

_____ Individual Name

_____ Personal Representative Name (If applicable)

_____ Signature

_____ Relationship to Individual (If applicable)

_____ Date

_____ Mailing Address

_____ City, State, Zip

_____ **Email**

Please submit this completed form to:

_____(Privacy Officer)
_____(Mailing address)

RESPONSE TO REQUEST TO INSPECT HEALTH INFORMATION

On _____ (insert date) you submitted a request to _____ (the "Company") to access protected health information regarding _____ (insert individual name). This letter is a response to your request.

Your request is granted. Access will be granted in the following format(s):

The designated record set will be available for review as follows: _____

Copies of the designated record set will be provided. The fee for copies is $_____.

Summary of health information will be provided in accordance with your request. The fee for the summary is $_____*[state the fee]*.

An extension of time to respond is needed. Your request was received on _____. A delay in providing the information is necessary for the following reason(s): *[state the basis for delay]* _____ _____.

A response will be provided by _____ *[list date no more than 60 days from the date of the request].*

Your request is denied. Your request was received on _____. Your request is denied for the following reason [state the basis for the denial]: _____ _____.

You may file a complaint regarding this decision with the Company or the U.S. Department of Health and Human Services. If you file a complaint with the Company, please file it in writing to:

_____(Privacy Officer)
_____(Mailing address)

An Individual Complaint Form for making your complaint will be provided upon request.

In certain cases you are entitled to appeal the denial of access. You are entitled to an appeal if access was denied because in the opinion of a licensed health care professional, granting access is likely to endanger the life or physical safety of you or another person. If you appeal, your appeal will be reviewed by a licensed health care designated professional who did not participate in the original decision. The appeal and notice of the appeal decision will be conducted promptly. An appeal may be initiated by filing an Individual Complaint Form with the Privacy Officer.

PROTECTED HEALTH INFORMATION ("PHI") **POLICY: 27**
INDIVIDUAL RIGHTS
CONFIDENTIAL COMMUNICATION OF PHI
GENERAL

POLICY

The Company will accommodate reasonable requests by individuals to receive confidential communications of their protected health information through alternative means or at alternative locations, only when the disclosure of all or part of that information could endanger the individual.

PURPOSE

The HIPAA Privacy Rule requires a health plan to allow individuals to make reasonable requests, and must accommodate those reasonable requests, to receive communications of protected health information by alternative means or at alternative locations if the individual clearly states that the disclosure of all or part of that information could endanger the individual. 45 CFR § 164.522(b).

This policy provides guidance and ensures compliance with applicable laws to address reasonable requests for confidential communication of protected health information.

PROCEDURE

The Company will allow an individual to make reasonable requests for confidential communication of protected health information through alternative means or at alternative locations if the individual clearly states that the disclosure of all or part of that information could endanger the individual. A Request for Confidential Communication Form may be used by the individual to request restrictions. Upon receipt of a request for confidential communication of protected health information, the Privacy Officer or his/her designee will be responsible for responding to the request. The Response to Request for Confidential Communication Form will be used to respond to any requests.

The Company will require individuals to make a request for a confidential communication in writing.

The request for confidential communication of protected health information will clearly state that the disclosure of all or part of that information could endanger the individual.

When applicable, the Company will condition the provision of a reasonable accommodation on receiving information as to how payment, if any, will be handled, and specification of an alternative address or other method of contact.

The requested alternative means or location will be reviewed on a case-by-case basis to determine if the request is reasonable.

Any use or disclosure under this policy and procedure will be in compliance with Policy 15 (Protected Health Information – Use or Disclosure of PHI – General).

Questions regarding this policy or knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer.

PROTECTED HEALTH INFORMATION ("PHI")
INDIVIDUAL RIGHTS
CONFIDENTIAL COMMUNICATION OF PHI
REQUEST FOR CONFIDENTIAL COMMUNICATION – FORM

REQUEST FOR CONFIDENTIAL COMMUNICATION OF HEALTH INFORMATION

I am hereby stating that disclosure of the identified protected health information regarding _____ (insert individual's name) could endanger the individual. Therefore, I am requesting that the identified protected health information be communicated in the following manner or location (describe alternative means or location):_____

This request applies only to the following protected health information (include dates, where applicable):

I understand that I may be responsible for any additional costs associated with the confidential communication request. This request for confidential communication would expire: _____(insert date).

_____	_____
Individual Name	Personal Representative Name (If applicable)
_____	_____
Signature	Relationship to Individual (If applicable)
_____	_____
Date	Mailing Address
	_____
	City, State, Zip

Please submit this completed form to:
_____(Privacy Officer)
_____(Mailing address)

RESPONSE TO REQUEST FOR CONFIDENTIAL COMMUNICATION OF HEALTH INFORMATION

On _____ (insert date) you submitted a request to_____ (the "Company") for confidential communications of protected health information regarding _____(insert individual's name). In that request you stated that communication of protected health information could endanger _____ (insert individual's name). This letter is a response to your request.

□ Your request is granted. Per your request the Company will accommodate the following confidential communication request (check applicable box(es):

□ Alternate means of communication to be used:
_____
_____

□ Alternate communication location to be used:
_____
_____

□ Your request is contingent upon the Company receiving information regarding how you intend to pay the additional cost associated with the confidential communication request. The additional costs that must be paid in advance by you are: $_____. Please contact the Company to make arrangements for payment of these costs.

□ This request will apply to only the following protected health information:_____
_____

□ This request will expire: _____ (insert date)

□ Your request is denied. Your request is denied for the following reason (state the basis for the denial): _____
_____
_____

PROTECTED HEALTH INFORMATION ("PHI") **POLICY: 28**
INDIVIDUAL RIGHTS
LIMITATION ON PHI USE AND DISCLOSURE
GENERAL

POLICY

The Company will allow an individual to request restrictions on the use and disclosure of their protected health information.

PURPOSE

The HIPAA Privacy Rule requires that covered entities provide an individual with the right to request restrictions to the use and disclosure of his or her protected health information. 45 CFR § 164.522(a). Agreement to the restrictions is not required, except under limited circumstances. If the covered entity agrees to the restrictions they must be honored until the restriction is terminated. This provision does not apply to health care provided to an individual on an emergency basis.

This policy provides guidance and ensures compliance with applicable laws when an individual requests restrictions on use or disclosure of protected health information.

PROCEDURE

Company will allow an individual to request restrictions on the use or disclosure of protected health information. A Request for Limitation Form may be used by the individual to request restrictions. Upon receipt of a request for a limitation on the on the use or disclosure of protected health information, the Privacy Officer or his/her designee will be responsible for responding to the request. The Response to Request for Limitation Form will be used to respond to any requests.

The Company is not required by the HIPAA Privacy Rule to agree to any requested restrictions, except when the individual requests a Company provider to restrict disclosure of claims information to a health plan and the individual has already paid the provider in full out of pocket.

If the Company agrees to a restriction, the Company may not violate such restriction, unless otherwise specified in these Privacy Policies and Procedures.

The Company is not required to honor an individual's restriction request when the individual who requested the restriction is in need of emergency treatment and the restricted protected health information is needed to provide the emergency treatment, provided that:

If restricted protected health information is disclosed to a health care provider for emergency treatment, the Company will request that such health care provider not further use or disclose the information.

If the Company agrees to an individual's requested restriction, the restriction does not apply to uses and disclosures :

To an individual accessing their own protected health information, See Policy 26 (Protected Health Information – Individual Rights – Access to PHI – General);

To an individual requesting an accounting of their own protected health information, See Policy 30 (Protected Health Information – Individual Rights – Accounting of PHI Disclosures – General); or

Required By Law, See Policy 24 (Protected Health Information – Use or Disclosure of PHI – Required By Law).

The Company may terminate its agreement to a restriction if:

The individual agrees to or requests the termination in writing;

The individual orally agrees to the termination and the oral agreement is documented;

The Company informs the individual that it is terminating its agreement to a restriction. This termination is only effective with respect to protected health information created or received after the Company has so informed the individual.

The Company will document and retain the restriction for a period of at least six (6) years from the date of creation or the date when last in effect, whichever is later.

Questions regarding this policy or knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer.

PROTECTED HEALTH INFORMATION ("PHI")
INDIVIDUAL RIGHTS
LIMITATION ON PHI USE AND DISCLOSURE
REQUEST FOR LIMITATION – FORM

REQUEST FOR LIMITATION ON USE OR DISCLOSURE OF HEALTH INFORMATION

I request that the use or disclosure of protected health information regarding _____ (insert individual name) by _____ ("Company") for payment or health care operations, or disclosure to family members, relatives, close personal friends, or other person identified by the individual, be restricted in the following manner: (describe requested restriction):_____
_____

This request applies only to the following protected health information (include dates, where applicable):

I understand that Company is not required to agree to this restriction, unless my request involves only the restriction of claims information to my insurer and I have already paid the Company provider in full out of pocket. This requested restriction would expire: _____(insert date).

_____ Individual Name

_____ Signature

_____ Date

_____ Personal Representative Name (If applicable)

_____ Relationship to Individual (If applicable)

_____ Mailing Address

_____ City, State, Zip

Please submit this completed form to:
_____(Privacy Officer)
_____(Mailing address)

PROTECTED HEALTH INFORMATION ("PHI")
INDIVIDUAL RIGHTS
LIMITATION ON PHI USE AND DISCLOSURE
RESPONSE TO REQUEST FOR LIMITATION - FORM

RESPONSE TO REQUEST FOR LIMITATION ON USE OR DISCLOSURE OF HEALTH INFORMATION

On _____ (insert date) you submitted a request to _____ (the "Company") for limitation on the use of disclosure of protected health information regarding _____ (insert individual name). This letter is a response to your request.

□ Your request is granted. Per your request the Company will limit the use or disclosure of protected health information as follows: (check applicable box(es):

□ Use or Disclosure for Payment:
_____
_____

□ Use or Disclosure for Health Care Operations:
_____
_____

□ Disclosure to family members, relatives, close personal friends or others identified by individual:
_____
_____

□ This request will apply to only the following protected health information:_____
_____

□ This request will expire: _____ (insert date)

Despite the agreed upon restrictions, the Company may use or disclose protected health information as necessary for emergency treatment of the individual. In an emergency circumstance the Company will ask the health care provider not further use or disclose the information.
The Company's agreement to the above restrictions may be terminated by the individual or the Company at any time, but any such termination will only apply to uses or disclosures occurring after the termination of the restriction.

□ Your request is denied. Your request is denied for the following reason (state the basis for the denial): _____

PROTECTED HEALTH INFORMATION ("PHI") **POLICY: 29**
INDIVIDUAL RIGHTS
AMENDMENT OF PHI

POLICY

The Company will allow an individual to request an amendment to their protected health information or a record about the individual in a designated record set for as long as the information is maintained in the designated record set.

PURPOSE

The HIPAA Privacy Rule provides individuals with the right to request an amendment or correction to their protected health information. 45 CFR § 164.526. Covered entities have the right to deny the request to amend or correct protected health information.

This policy provides guidance and ensures compliance with applicable laws to address requests to amend protected health information maintained by Company.

PROCEDURE

General

The phrase "designated record set" is defined in 45 CFR § 164.501, a copy of which is referenced at the end of these policies and procedures.

The Company will document and retain the title of persons responsible for receiving and processing requests for amendment of protected health information for a period of at least six (6) years from the date of its creation or the date when it last was in effect, whichever is later.

The Company will allow an individual to request amendment of protected health information. A Request for Amendment Form may be used by the individual to request restrictions. Upon receipt of a request for amendment of protected health information, the Privacy Officer or his/her designee will be responsible for responding to the request. The Privacy Officer will consult with a designated health care professional regarding the request. The Response to Request for Amendment Form will be used to respond to any requests.

Individuals must document the reason(s) to support the requested amendment.

The Company will respond to the individual no later than 60 days after receipt of a request.

The time period for the action by the Company will be extended by no more than 30 days.

If the time period for the action is extended, the Company will, within 30 days after receipt of the request, provide the individual with a written statement of the reasons for the delay and the date by which the Company will complete the action on the request.

The time period for action will not be extended more than once.

Approval of Amendment

Upon approval of a requested amendment, the Company will:

Inform the individual on the Response to Request for Amendment Form, in a timely manner;

Make the appropriate amendment or append the amendment to the original record.

Provide the Amendment Notification Agreement Form to the individual to obtain the individual's identification of and agreement to have the Company notify the relevant persons of the amendment;

Make reasonable efforts to inform and provide the amendment within a reasonable time to persons identified by the individual as needing the amendment;

Make reasonable efforts to inform and provide the amendment within a reasonable time to persons, including business associates that we know have the affected protected health information and that may have relied, or could foreseeably rely, on such information to the detriment of the individual.

In the event that a covered entity notifies the Company of an amendment to an individual's protected health information, the Company will make the appropriate amendment or append the amendment to the original record.

Denial of Amendment

An individual's request for amendment may be denied if the requested protected health information or record:

Was not created by the Company, unless the originator is no longer able to act;

Is not part of the designated record set;

Would not be available for inspection under the requirements for individual rights to access protected health information, see Policy 26 (Protected Health Information – Individual Rights – Access to PHI – General); or

Is accurate and complete.

When denying an individual's request for amendment of protected health information, the denial will be on the Response to Request for Amendment Form.

Response to Denial

An individual has the right to file a written statement disagreeing with the denial of amendment. The statement of disagreement will be limited to five (5) single-sided 8-1/2 x 11 pages. The statement of disagreement should be filed with the Privacy Officer within 60 days of the notice of denial. The Company may prepare a rebuttal statement to the statement of disagreement. If a rebuttal statement is prepared, the individual will be provided with a copy. If a statement of disagreement is filed with the Company, the request for amendment, denial, statement of disagreement and any rebuttal prepared by the Company will be part of any future authorized disclosure of the protected health information.

If an individual does not submit a statement of disagreement, the individual may request that the request for amendment and the denial of amendment be provided with any future disclosures of the protected health information that was the subject of the request. The appended information will not be disclosed unless the individual requested such disclosure.

For recordkeeping purposes, the Company will append to the disputed record or protected health information any request for amendment, denial, statement of disagreement and any rebuttal prepared by the Company. Disclosure of the appended information will only occur as set forth above.

Complaints

An individual may file a complaint regarding a denial with the Company or the U.S. Department of Health and Human Services. See Policy 8 (Administrative Requirements – Privacy Compliance – Complaints – General).

Questions regarding this policy or knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer.

PROTECTED HEALTH INFORMATION ("PHI")
INDIVIDUAL RIGHTS
AMENDMENT OF PHI
REQUEST FOR AMENDMENT – FORM

REQUEST TO AMEND HEALTH INFORMATION

I request to amend the protected health information about me in the designated record set(s) maintained by _____ (the "Company") in accordance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

A "designated record set" includes information such as medical records; billing records; enrollment, payment, claims adjudication and health plan case or medical management record systems; or records used to make decisions about individuals.

I am requesting that the following health information be amended (include dates if applicable): _____
_____
_____
_____

I am making the request to amend for the following reason(s): _____
_____
_____

I understand that if the protected health information was not created by the Company, the Company is not required to honor my request, unless the person or entity that created the information is no longer available to make the amendment. For example, if the information I wish to amend is in a medical report created by a health care provider, I must ask that health care provider to amend the report. I also understand that if the information is not part of the designated record set, is not part of the information which you would be permitted to inspect and copy, or is already accurate and complete, I cannot amend the information.

I understand that the Company may refuse my request for amendment. I understand that the Company will respond to my request within 60 days.

_____	_____
Individual Name	Personal Representative Name (If applicable)
_____	_____
Signature	Relationship to Individual (If applicable)
_____	_____
Date	Mailing Address
	_____
	City, State, Zip

Please submit this completed form to:
_____(Privacy Officer)
_____(Mailing address)

PROTECTED HEALTH INFORMATION ("PHI")
INDIVIDUAL RIGHTS
AMENDMENT OF PHI
RESPONSE TO REQUEST FOR AMENDMENT – FORM

RESPONSE TO REQUEST TO AMEND HEALTH INFORMATION

On _____ you submitted a request to _____ (the "Company") to amend protected health information in accordance with the Health Insurance Portability and Accountability Act ("HIPAA"). This letter is a response to your request (check applicable box).

□ Your request is granted. The appropriate amendment to the designated record set will be made. You must provide the names of any person(s) who should be provided with the amended information on the enclosed Amendment Notification Agreement. A reasonable effort will be made in a timely fashion to inform these individuals, or any individuals that are known to have relied or could have relied on the information.

□ An extension of time to respond is needed. Your request was received on _____. A delay in providing the a response is necessary for the following reason(s): *[state the basis for delay]* _____ _____.
A response will be provided by _____ *[list date no more than 60 days from the date of the request].*

□ Your request is denied. Your request was received on _____. Your request is denied for the following reason [state the basis for the denial]: _____ _____.

You have the right to file a written statement disagreeing with the denial of amendment. The statement of disagreement must be limited to five (5) single-sided 8-1/2 x 11 pages. The statement of disagreement should be filed within 60 days of this notice with:
_____(Privacy Officer)
_____(Mailing address)

We have the right to prepare a rebuttal statement to your statement of disagreement. If a rebuttal statement is prepared, you will receive a copy.

If you do not submit a statement of disagreement, you may request that your request for amendment and this denial of amendment be provided with any future disclosures of

protected health information that is the subject of this request.

You may file a complaint regarding this decision with Company or the U.S. Department of Health and Human Services. If you file a complaint with Company, please file it in writing to:

_____(Privacy Officer)
_____(Mailing address)

An Individual Complaint Form for making your complaint will be provided upon request.

PROTECTED HEALTH INFORMATION ("PHI")
INDIVIDUAL RIGHTS
AMENDMENT OF PHI
AMENDMENT – NOTIFICATION AGREEMENT-FORM

AMENDMENT OF HEALTH INFORMATION NOTIFICATION AGREEMENT

I hereby authorize _____ (the "Company") to notify the following persons (include address information) of the amendment of my protected health information approved on _____ (insert date of approval):

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

_____ _____
Individual Name Personal Representative Name (If applicable)

_____ _____
Signature Relationship to Individual (If applicable)

_____
Date

Please submit this completed form to:
_____(Privacy Officer)
_____(Mailing address)

PROTECTED HEALTH INFORMATION ("PHI") **POLICY: 30**
INDIVIDUAL RIGHTS
ACCOUNTING OF PHI DISCLOSURES
GENERAL

POLICY

The Company will allow individuals to receive an accounting of instances where protected health information about them is disclosed, except for disclosures for the following purposes:

To carry out treatment, payment and health care operations (unless the Company uses or maintains an electronic health record with respect to protected health information);

To the individuals of protected health information about them;

Incident to a use or disclosure permitted by the HIPAA Privacy Rule;

Pursuant to a valid authorization;

To persons involved in the individual's care or other notification purposes;

For national security or intelligence purposes;

As part of a limited data set; or

To correctional institutions or law enforcement officials.

The Company will utilize a disclosure log for documenting and maintaining an accounting of when individuals' protected health information has been disclosed for purposes other than those listed above for which the individual does not have the right to an accounting.

PURPOSE

HIPAA requires that individuals have a right to receive an accounting of various instances when protected health information about them is disclosed by a covered entity, subject to certain time-limited exceptions for disclosures to law enforcement and oversight agencies. 45 CFR § 164.528.

This policy provides guidance and ensures compliance with applicable laws to address the accounting of instances when protected health information has been used or disclosed for purposes not excepted by the HIPAA Privacy Rule, as amended by HITECH.

PROCEDURE

Except for disclosures for which an accounting is not required under the HIPAA Privacy Rule, as amended by HITECH, the Company will allow an individual to obtain an accounting of instances when their protected health information has been disclosed. A Request for Accounting Form may be used by the individual to request restrictions. Upon receipt of a request for accounting of disclosures, the Privacy Officer or his/her designee will be responsible for responding to the request. The Response to Request for Accounting Form will be used to respond to any requests.

The Company will allow an individual to receive an accounting of disclosures made by the Company of protected health information maintained in paper medical records in the six (6) years prior to the date on which the accounting is requested. The Company will allow an individual to receive an accounting of disclosures made by the Company of protected health information maintained in electronic health records in the three (3) year period prior to the date on which the accounting is requested.

The Company must temporarily suspend the right of an individual to receive and accounting of disclosures to a health oversight agency or law enforcement official, for:

The time period specified by the agency or official if the agency or official provides the Company with a written statement that providing the accounting would impede the agency or official activities and specifies a time limit for the suspension; or

No longer that thirty (30) days if the agency or official provides the Company with an oral statement that providing the accounting would impede the agency or official activities, which is documented by the Company.

The accounting will be in writing on the Response to Request for Accounting Form and the Accounting of Disclosures Form and will include disclosures made to or by business associates of the Company.

Each accounting of a disclosure will include the following:

The date of disclosure;

The name of the entity or person who received the protected health information and, if known, the address of such entity or person;

A brief description of the protected health information disclosed; and

A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure; or in lieu of such statement

A copy of the individual's written authorization to use or disclose the protected health information, or

A copy of a written request for a disclosure required by the HHS Secretary to investigate or determine the covered entity's compliance with applicable laws and regulations.

The Company will act on the individual's request for an accounting not later than 60 days after receipt of the request on the Response to Request for Accounting by:

Providing the individual with the accounting requested, or

Extending the time to provide the accounting by no more than 30 days.

In the event that the Company extends the time to provide the accounting, within 60 days after receipt of the request, it will provide the individual with the Response to Request for Accounting of Disclosures Form stating the reasons for the delay and the date by which the covered entity will provide the accounting. The Company will not extend the time to provide the accounting more than once.

The first accounting to an individual in any 12 month period will be without charge. Any fee imposed by the Company for each subsequent request for an accounting by the same individual within the 12 month period will be cost-based. Upon imposing a fee the Company will inform the individual in advance of the fee and provide the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

The Company will document and retain the following for a period of at least six (6) years, or from the date of its creation or the date when it last was in effect, whichever is later:

The information required to be included in an accounting;

The written accounting that is provided to the individual;

The title of the persons or officer responsible for receiving and processing requests for an accounting by individual.

Questions regarding this policy or knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer.

PROTECTED HEALTH INFORMATION ("PHI")
INDIVIDUAL RIGHTS
ACCOUNTING OF PHI DISCLOSURES
REQUEST FOR ACCOUNTING – FORM

REQUEST FOR ACCOUNTING OF PROTECTED HEALTH INFORMATION DISCLOSURES

I request an accounting of the protected health information disclosures regarding _____ (insert individual name) by _____ (the " Company").

Please note: the maximum time frame that can be requested is six (6) years prior to the date of your request. I would like an accounting of all disclosures for the following time frame.

From: _____ To: _____

There is no charge for the first accounting request in a 12-month period. For subsequent requests in the same 12-month period, the charge is $_____. I agree to pay this fee if this is not my first accounting request in the 12-month period.

I understand the accounting I have requested will be provided to me within 60 days unless I am notified in writing that an extension of up to 30 days is needed.

_____ _____
Individual Name Personal Representative Name (If applicable)

_____ _____
Signature Relationship to Individual (If applicable)

_____ _____
Date Mailing Address

_____
City, State, Zip

Please submit this completed form to:
_____(Privacy Officer)
_____(Mailing address)

PROTECTED HEALTH INFORMATION ("PHI")

INDIVIDUAL RIGHTS
ACCOUNTING OF PHI DISCLOSURES
RESPONSE TO REQUEST FOR ACCOUNTING – FORM

RESPONSE TO REQUEST FOR ACCOUNTING OF PROTECTED HEALTH INFORMATION DISCLOSURES

On _____ (insert date) you submitted a request to _____ (the "Company") for an accounting of protected health information disclosures regarding _____ (insert individual name). This letter is a response to your request (check applicable box(es).

□ Your request is granted.

- □ The Accounting of Disclosures of Protected Health Information is attached.
- □ The fee for the Accounting of Disclosures of Protected Health Information is $_____. Please forward payment to Company.

□ An extension of time to respond is needed. Your request was received on _____. A delay in providing the information is necessary for the following reason(s): *[state the basis for delay]* _____ _____.
A response will be provided by _____ *[list date no more than 90 days from the date of the request].*

□ Your request is denied in part. Your right to receive an accounting of disclosures to a health oversight agency or law enforcement official has been suspended until _____ (insert date) by _____ (insert agency name).

PROTECTED HEALTH INFORMATION ("PHI")
INDIVIDUAL RIGHTS
ACCOUNTING OF PHI DISCLOSURES
ACCOUNTING OF PHI DISCLOSURES – FORM

ACCOUNTING OF DISCLOSURES OF PROTECTED HEALTH INFORMATION

PROTECTED HEALTH INFORMATION DISCLOSURE LOG

Individual Name: **Enrollee Identification No:**

Date Received	Name of Requestor	Address (If Known)	Auth Type	Purpose of Disclosure	PHI/Information Disclosed	Date Disclosed	Disclosed By:

(Use the above section as a complete record or to record those disclosures made w/o an authorization)

REQUESTS FOR ACCOUNTING OF DISCLOSURES

Requested By (Individual/Legal Rep)	Date Requested	Date Range Requested	Staff Member Completing Request	Date Provided

(Use the above section to document accounting requests when a copy of this disclosure log is provided to the individual requesting the accounting)

PROTECTED HEALTH INFORMATION ("PHI") **POLICY 32**
BREACH NOTIFICATION POLICY

POLICY.

It is the policy of the Company to identify and respond to incidents involving the unauthorized acquisition, access, use or disclosure of protected health information ("PHI") in violation of the HIPAA Privacy Rule. Any incident that compromises the security or privacy of PHI is a breach subject to this Policy. An incident compromises the security or privacy of PHI if it poses significant risk for financial, reputational, or other harm to the individual (harm threshold). Business associates that access, maintain, modify, record, store, destroy, or otherwise hold, use or disclose protected health information ("PHI") are required to notify Company of any incident that may be a breach.

PURPOSE

This policy is designed to give guidance as to whether a breach has occurred and the process for notification of affected individuals of any breach. It is the intent of this Policy to minimize risk and ensure prompt and appropriate action is taken should such a breach occur.

PROCEDURES

All incidents involving confirmed or suspected unauthorized acquisition, access, use or disclosure of protected health information will be immediately reported to the Company's Security Officer or Privacy Officer. If reported to the Security Officer, the Security Officer will notify the Privacy Officer. As a BA, the Company will immediately report the incident to the covered entity(ies) involved.

Because all incidents will be a Privacy Rule violation, regardless of whether constituting a breach subject to this policy, the Privacy Officer will process the incident in accordance with Policy 9 (Administrative Requirements – Complaints/Appeals) and Policy 10 (Administrative Requirements – Mitigation). The procedures in this Policy are in addition to the procedures in those policies.

The Privacy Officer will work with the Privacy Officer of the covered entity(ies) involved, if any, to determine whether a breach has occurred by analyzing the following:

Risk Assessment. A breach is presumed to have occurred if there is an impermissible acquisition, access, use of disclosure of PHI unless the Privacy Officer determines there is a low probability that the PHI has been compromised. In determining whether a breach has occurred, the Privacy Officer will consider the following four factors: (i) the nature and extent of PHI involved, (ii) who impermissibly used the PHI or to whom the PHI was impermissibly disclosed, (iii) whether the PHI was actually acquired or viewed, and (iv) the extent to which the risk to the PHI has been mitigated.

Exception Determination. The Privacy Officer can find that an exception to the breach definition applies if any of the following are true:

(a) There was an unintentional acquisition, access or use of PHI by a member of the Company's workforce or a member of a BA's workforce while doing business on behalf of the Company and there was no further disclosure (e.g., wrong employee of business associate receives billing information from Company employee, notifies sender and deletes the information)
(b) There was an Inadvertent disclosure of PHI by a workforce member to another "similarly situated" workforce member that does not result in further use or disclosure (e.g., Company sends claims information to wrong provider)
(c) There is the reasonable belief that an unauthorized recipient of the PHI would not be able to retain the information (e.g., a billing statement was sent to the wrong patient but is returned to the Company as undeliverable).

If the Privacy Officer and covered entity(ies) determine that a breach has occurred, notification must be sent to the affected individuals within 60 days from the date the Company, its BAs or the covered entity(ies), became aware of the incident or should have reasonably become aware of the incident. [Note: the 60-day period does NOT begin upon determination of whether a breach has occurred.] Notification delays are acceptable only if they impede a criminal investigation or cause damage to national security.

The Privacy Officer will coordinate with any covered entity involved to arrange for notification to be mailed to each individual affected by the breach by first class mail to the last known address of each individual or via email if the individual previously authorized contact via email. If the situation is urgent, contact by telephone is acceptable.

(a) If the individual is a minor or deemed "incompetent", notice should be sent to a parent or personal representative.
(b) If the individual is deceased, the next-of-kin or personal representative must be notified to the extent the information is known.

(c) If sufficient contact information is outdated or unavailable for less than 10 individuals, the Company may alternatively notify the individuals via email if they have that information. Similarly, if the Company has the individuals' phone number, but no email address, the Company may notify the individuals via telephone.
(d) If sufficient contact information is outdated or unavailable for 10 or more individuals, the Company must alternatively post a conspicuous notice on the home page of its web sites for 90 days or on major print or broadcast media in the area where the affected individuals reside. In addition, a toll free number must be made available to the individuals for at least 90 days.

If more than 500 individuals are affected in one state or jurisdiction, the Company or the covered entity(ies) will notify a prominent media outlet serving that state or jurisdiction. This notice should be provided simultaneously with written notice, but no later than 60 days from discovery. This notice must contain the same information as the written notice. This notice is in addition to the written notice to the individual.

If more than 500 individuals are affected and these individuals reside in several states with no one state having more than 500 individuals affected, media notice is not required.

If the Company, as a business associate, has more than 500 individuals affected with more than one covered entity involved, but no one covered entity has more than 500 individuals affected, media notice is not required.

If less than 500 individuals are affected, the Company will report, or will assist the covered entity(ies), if requested, in reporting all breaches to the DHHS in an annual report due by February 28 of the calendar year following the breaches being discovered.

If more than 500 individuals are affected by any one breach, the Company will report, or will assist the covered entity(ies), if requested, in reporting the breaches to DHHS concurrently with written notice to the individuals. DHHS will post on its web site all covered entities who submit reports of breaches involving more than 500 individuals.

Written notice to affected individuals under this Policy must include the following data elements:

(a) A brief description of the circumstance of the breach.
(b) Description of the type of PHI breached
(c) Steps the individuals should take to protect themselves from potential harm resulting from the breach.

(d) A description of the investigation, mitigation, and protection against further breaches.
(e) Contact procedures – Toll free number, email address, website, or postal address.

State laws that are more protective of the privacy rights of affected individuals in the event of a breach will preempt and/or may add additional notification requirements to those contained in this Policy. The Privacy Officer will notify legal counsel of any need to research state breach notification laws.

The Privacy Officer or his/her designee will document the investigation of any potential breach on the Breach Investigation and Notification Form following this Policy. All documentation shall be maintained for no less than six (6) years following the creation of the documentation. The Privacy Officer will notify the Compliance Committee of the results of this investigation.

The Company shall impose appropriate sanctions against any workforce member who fail to comply with the privacy policies and procedures of the Company and the requirements of this Policy.

PROTECTED HEALTH INFORMATION ("PHI")
BREACH NOTIFICATION POLICY
BREACH INVESTIGATION AND RESPONSE FORM

BREACH INVESTIGATION AND RESPONSE FORM

Date of Discovery of Potential Breach:_____ Date of Referral:_____

Name of Investigator(s):_____

Description of Potential Breach:_____

Covered Entity(ies) Involved:_____

- Is the potential breach a HIPAA Privacy Rule Violation? [ ] Yes [ ] No. If yes, go to next question.
- Does an exception to the breach notification rule apply? [ ] Yes [ ] No. If no, go to next question.
- Is there significant risk of financial, reputational or other harm from the potential breach? [ ] Yes [ ] No. If yes, a breach has occurred and notification to affected individuals is required.

Date of Mailing Written Notice to Affected Individuals:_____
(Attach copy of letter)

For Breaches Affecting 500 or More individuals in One State:

Date of Notification of Media Outlet (Attach Copy):_____

Date of Notification of DHHS (Attach Copy):_____

For Breaches Affecting Less than 500 Individuals:

Date Breach entered into Security Incident Log:_____

Recommended Sanctions:_____

Signature of Investigator(s):_____ Date:_____

Signature of Privacy Officer:_____ Date:_____

APPENDIX 1:

HIPAA COMBINED REGULATION TEXT

Combined Regulation Text (Transactions and Code Set Standards, Identifier Standards, Privacy Rule, Security Rule, Enforcement Rule, Breach Notification Rule) Link:

http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/index.html

HIPAA/HITECH Final Omnibus Rule Link:

http://www.hhs.gov/ocr/privacy/hipaa/administrative/omnibus/index.html