SUPERIOR VISION

SUPERIOR VISION CORP. AND SUBSIDIARIES

HIPAA Security Rule Policies & Procedures

Last Revision Date: December 22, 2014

SUPERIOR VISION CORP.
AND SUBSIDIARIES
SECURITY POLICIES AND PROCEDURES

TABLE OF CONTENTS

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".

The confidentiality of individual protected health information ("PHI") has always been an important issue to the Company. The Company respects the privacy of PHI and has enacted procedures in accordance with 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. parts 160 and 164, subparts A and E (the "Privacy Rule"). In accordance with the HIPAA Security Regulations for the Protection of Electronic Protected Health Information promulgated at 45 C.F.R. parts 160, 162 and 164, subpart C, (the Security Rule"), covered entities (health plans, health care clearinghouses and health care providers transmitting PHI in electronic form in connection with a transaction covered under HIPAA) are required to: (a) protect the confidentiality, availability and integrity of electronic protected health information ("EPHI"); and (b) protect against reasonably anticipated threats or hazards to the security or integrity of EPHI. To further the Company's goals regarding the security of EPHI, these Security Policies and Procedures have been adopted to comply with the HIPAA Security Rule effective April 21, 2005, as amended by the HITECH Act effective September 23, 2009 and the Final Omnibus Rule September 23, 2013. The Company will update these Security Policies and Procedures, as applicable, to maintain compliance with these security laws.

APPLICABILITY

These Security Policies and Procedures apply to Superior Vision Corp. and its subsidiaries to the extent that such Security 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.

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" and has a direct customer relationship with its 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.

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. 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.

POLICY CROSSWALK

POLICY		STANDARD
Policy No. 1:	Security Officer Job Description	164.308(a)(2) Assigned Security Responsibility
Policy No. 2:	Information System Activity Review	164.308(a)(1) Security Management ▪ Information System Activity Review 164.312(a)(2) and 312(b) Audit Controls
Policy No. 3:	Access Management and Authentication	164.308(a)(3) Workforce Security ▪ Authorization and/or Supervision ▪ Workforce Clearance Procedures 164.308(a)(4) Information Access Management ▪ Access Authorization ▪ Access Establishment and Modification 164.308(a)(5) Security Awareness and Training ▪ Password Management 164.310(a)(2) Facility Access Controls ▪ Access Control and Validation Procedures 164.310(b) Workstation Use 164.312(a)(1) and (2) Access Controls ▪ Unique User Identification ▪ Emergency Access Procedure ▪ Automatic Log-off 164.312(c) Integrity ▪ Mechanism to Authenticate EPHI 164.312(d) Person or Entity Authentication

POLICY		STANDARD
Policy No. 4:	Security Incident Reporting and Response	164.308(a)(1) Security Management ▪ Sanction Policy 164.308(a)(6) Security Incident Procedures ▪ Response and Reporting
Policy No. 5:	Termination Procedures Related to Security Maintenance	164.308(a)(3) Workforce Security ▪ Termination Procedures 164.308(a)(4) Information Access Management ▪ Access Establishment and Modification
Policy No. 6:	Security Reminders and Staff Training	164.308(a)(5) Security Awareness and Training ▪ Security Reminders
Policy No. 7:	Acceptable Use Policy	164.308(a)(5) Security Awareness and Training ▪ Protection from Malicious Software 164.310(b) Workstation Use
Policy No. 8:	Facility Access Controls and Workstation Security	164.308(a)(5) Security Awareness and Training ▪ Protection from Malicious Software 164.310(a)(1) and (2) Facility Access Controls ▪ Facility Security Plan ▪ Access Control and Validation Procedures 164.310(c) Workstation Security 164.310(d) Device and Media Controls ▪ Accountability 164.312(a)(1) and (2) Access Control ▪ Emergency Access Procedure ▪ Automatic Log-off ▪ Encryption / Decryption 164.312(e)(1) Transmission Security ▪ Integrity Controls

POLICY	STANDARD
	▪ Optional – Encryption
Policy No. 9: Maintenance, Disposal and Re-Use of Equipment and Media	164.310(a)(1) and (2) Facility Access Controls ▪ Maintenance Records 164.310(d)(1) and (2) Device and Media Controls ▪ Disposal ▪ Media Re-Use
Policy No. 10: Contingency Plan	164.308(a)(7) Contingency Plan ▪ Data Back-up Plan ▪ Disaster Recovery Plan ▪ Emergency Mode Operation Plan ▪ Testing and Revision Procedures ▪ Application and Data Criticality Analysis 164.310(a)(1) and (2) Facility Access Controls ▪ Contingency Operations 164.310(d)(1) and (2) Device and Media Controls ▪ Data Back-up and Storage
Policy No. 11: Business Associates-EPHI	164.314(a)(2)(i)

QUESTIONS

Any questions regarding these Security Policies and Procedures should be directed to the Security Officer, Greg Pontius (800-243-1401, ext. 1430).

I. POSITION TITLE: Security Officer

II. JOB RESPONSIBILITIES:

- Maintain current knowledge of the HIPAA Security Rule, and any amendments to this Rule, through attendance at continuing education classes, seminars, online news services or other available means.
- Perform and/or oversee initial and periodic security assessments to monitor the existence, implementation and upkeep of adequate security measures.
- Implement periodic security review utilizing internal IT staff or external IT provider, as appropriate.
- Before any major change to facilities or operations (e.g., opening a new office or move of an existing office, implementation of new software system, new internet or data circuit carrier), determine if a new audit or security review is necessary, and if so, carry out that review.
- Draft, or oversee the drafting, of the Company's policies and procedures for implementation of the Security Rule and periodically review for any needed revisions.
- Oversee the implementation of the Company's policies and procedures.
- Develop and arrange for a HIPAA security training program for all staff members.
- Develop and arrange for a HIPAA security training program for all new employees.
- Oversee the addition of security provisions in existing business associate agreements and ensure that all new business associate agreements contain security provisions.
- Receive, arrange for investigation and response, and document all reported suspected or known security incidents.

- Report all security incidents that involve the unauthorized acquisition, access, use or disclosure of protected health information to the Privacy Officer for investigation of a potential breach subject to HIPAA Privacy Policy 32.
- Ensure that IT system logs are periodically reviewed in accordance with the Company's security policies.
- Serve as a security policy resource for all staff members.
- Oversee development and design of contingency plan.
- Provide periodic reports to management regarding the Company's security compliance and implementation efforts.

I. POLICY

It is the policy of the Company to periodically conduct internal reviews of IT system activity and log-on activity to prevent and/or detect suspected or known security incidents.

II. PURPOSE

It is the purpose of this Policy to describe the timing and extent of the audit procedures.

III. SCOPE

Most applications (including utility software on operating systems, data backup systems, etc.) have event logs that track all activity, whether as part of legitimate operations or as part of an unusual security event. There are certain IT products that are specifically designed to identify suspicious events and record pertinent data regarding them, including the date, time and certain other details. While it is not feasible to review all log entries at all times, this Policy applies to periodic targeted reviews of certain IT components and to more thorough review if any suspicious system activity is detected.

IV. PROCEDURE

A. Conducting Periodic Reviews

1. The Security Officer or his designee will ensure that all applicable logs from all applicable operating systems, services and applications are enabled and configured properly to record the date and time of events.

2. The Security Officer or his designee will periodically review, or arrange for review by the Company and/or it's IT vendors, the following information regarding IT system activity:

a. Overall system storage on server(s) and storage devices – (i) compare present amount of storage used to the previous amount of storage used, and note any significant increases or decreases; (ii) look for the addition of new user accounts to the system, especially any new administrator accounts since the last review; (iii) look for the addition of any new directories, software programs, icons, wallpapers, screensavers or shortcuts, especially on any server(s); (iv) look for any changes in procedures or applications as a result of any software application updates that, during the previous period, may have

been: (1) sent to the office via CD-ROM or other physical media to be installed locally; (2) downloaded from the vendor's website; (3) "pushed" from the vendor's website via an automatic update; or (4) remotely installed by the vendor, if the vendor has outside access into your system;

b. Data back-up system - note any significant increases or decreases in the time required to complete normal back-ups; check the back-up software log and the media itself to ensure the number of directories/ files and the volume of data being backed up seems reasonable and consistent with the previous review;

c. Workstations, laptops, PDAs and any media – (i) ensure that the location of all workstations, laptops, PDAs and any media are still known (particularly backup tapes and/or removable drives); (ii) ensure that all security measures are still in place such as periodic virus scanning and updates, firewall/VPN software, spam filtering, pop-up blocking, anti-malware, etc., as appropriate;

d. Security Incident Log and Maintenance Log – periodically review the logs looking for any trends or patterns in the areas of log-ins, email access, remote access, or user ID or password issues.

3. The Security Officer or his designee will ensure that the logs are maintained until the next cycle of review takes place.

B. Conducting Targeted Audits of Suspicious Log Activity

1. The Security Officer or his designee will review any unusual activity related to software applications and if a security incident is found to have occurred, follow the procedures in Policy No. 4, Security Incident Reporting and Response.

2. The following constitute unusual activity:

a. a fairly rapid drop-off in system performance or network speed;

b. a dramatic change in the time needed to complete a back-up or other operation; or

c. an unexplained or unexpected increase in system resources such as processor utilization or disk space.

I. POLICY

It is the policy of the Company to implement IT system security measures to ensure that only authorized individuals have access to EPHI, and to prevent unauthorized individuals from having access to EPHI.

II. PURPOSE

It is the purpose of this Policy to set forth security measures to ensure the following:

A. that access to the Company's IT system and EPHI by the Company's staff members is properly authorized;

B. that all of the Company's staff members have appropriate access to EPHI and to prevent those who do not have access to EPHI from obtaining such access;

C. that physical access to the Company's IT system containing EPHI is appropriately limited to authorized individuals;

D. that physical measures and a password management are implemented to protect the Company's IT system and related equipment from unauthorized use, and to ensure that access to EPHI is only available to those persons or programs that have been appropriately granted such access; and

E. that validation and authentication prompts are in place prior to access and use of EPHI.

F. that measures are in place to safeguard the transmission of data files containing EPHI to destinations outside of the Company's computer network.

III. SCOPE

This Policy applies to (a) each of the Company's staff members, including volunteers and trainees, (b) the Company's stationary and portable equipment used to store, receive or transmit EPHI (e.g., desktop workstations, servers, laptops, etc.), and (c) software applications used in any of the equipment listed in (b) above. This policy applies where indicated to remote access by, and home computers of, staff members.

IV. PROCEDURE

A. Determining Access Rights.

1. Staff members who work with EPHI or in locations where EPHI is available must be qualified to operate the IT system components to which they have been granted access. Prior to allowing a staff member to operate IT system component or access EPHI, the Security Officer or his designee will review each staff member's background and qualifications to determine whether the individual is capable of working with EPHI in a manner that will maintain the confidentiality of the EPHI and integrity of the IT system. If the Security Officer or his designee determines that the staff member is not qualified, the staff member will not receive access rights until receiving training on the particular IT system component in question and the Security Officer is satisfied that granting access rights to the staff member will not pose a security risk.

2. The Security Officer or his designee will grant access rights to the Company's IT system to each staff member based on job description and/or by a specific component of the Company's IT system. Staff members may not authorize their own access to EPHI or be granted authorization from anyone other than the Security Officer or his designee.

3. The Security Officer or his designee will ensure that each staff member has access to the IT system components and software necessary to perform the functions of his/her job, as described in the applicable job description. The access granted to each staff member by the Security Officer or his designee will be the "minimum necessary" required for the staff member's job.

4. If desired, the Security Officer or his designee may designate certain IT system components (e.g., certain workstations, software applications, etc.) as appropriate for certain staff members. Once designated, these IT system components may be accessed by authorized staff members as required by their job descriptions. The Security Officer or his designee will ensure that the designated IT system components are clearly defined and physically separate from other IT components so as to prevent unauthorized access to other IT system components for which the individual has not been granted access. The assignment of a staff member to an IT component will also be noted in the Inventory maintained pursuant to Policy No. 8 (Facility Access Controls and Workstation Security).

5. The Security Officer or his designee will maintain a Staff Access Log to log the date and type of access granted to each staff member.

6. Whenever a staff member terminates or changes jobs within the facility, the Security Officer or his designee will follow the procedures set forth in Policy No. 5 (Termination Procedures Related to Security Maintenance), including corresponding entries into the Staff Access Log.

7. The Security Officer or his designee will annually, or whenever the Company installs new IT components or significantly reorganizes the Company's staff duties, review all job descriptions and IT system components to determine whether it is necessary to terminate or modify staff members' rights of access to the Company's EPHI. If so, the Security Officer or his designee will make the modifications following the procedures in Policy No. 5 (Termination Procedures Related to Security Maintenance), as appropriate.

8. The Security Officer or his designee(s) will supervise all staff members who work with the Company's EPHI or are in a position to access EPHI to ensure that the staff members are working within the access rights granted to them. The Security Officer or his designee will also enforce the Company's Acceptable Use Policy, Policy No. 7, as it relates to the appropriate use of the Company's IT system and handling of EPHI. The Security Officer or his designee will direct staff members to communicate any concerns or questions regarding proper operation of IT system and/or the handling of EPHI to the Security Officer or his designee.

B. Controlling Access by Visitors.

1. All staff members will limit a visitor's physical access to the Company's IT system and the rooms or facilities in which such systems are housed, as provided in Policy No. 8, Facility Access Controls and Workstation Security.

2. To control, validate, and document access by vendors, repair personnel, and other non-staff members in any area used to house IT systems containing EPHI, the Company will log-in visitors and issue a Visitor badge. The Security Officer or his designee will escort vendors and repair personnel to and from areas housing IT system containing EPHI. After-hours visitor access is addressed in Policy No. 8, Facility Access Controls and Workstation Security.

3. The Security Officer and any executive officer of the Company are the only persons who may grant temporary access to the Company's IT system to vendors, repair persons and consultants. Whenever temporary access rights are

granted to a vendor, repair person or consultant, appropriate documentation will be maintained, including notation of when the temporary access is terminated.

C. Defining Appropriate Workstation Use/Password Management/Automatic Logoffs

1. To identify and track each staff member for the purpose of controlling and monitoring access to the Company's IT system, each staff member will be required to comply with the password management measures below. Every staff member accessing the Company's IT system components must have a unique user ID and password. When initially requesting access to any component of the Company's IT system that accesses, transmits, receives, or stores EPHI, a staff member will be required to supply his or her unique user identification and password to gain access.

2. Each staff member's password must meet the following requirements, unless otherwise determined by the Company:

   a. Must be a minimum of six - eight characters in length;

   b. Must incorporate at least one of the following characteristics:

      - Any lower case letters (a-z)
      - Any upper case letters (A-Z)
      - Any numbers (0-9)
      - Any punctuation or non-alphanumeric characters found on a standard ASCII keyboard

   c. Should not include easily guessed information such as personal information, names, pets, birth dates, etc.

3. Staff members will not allow another user or staff member to use their user ID or password and will ensure that their user ID is not documented, written, or otherwise exposed in an insecure manner.

4. If a staff member believes his/her user ID or password has been comprised, they must report the event to the Security Officer or his designee according to Policy No. 4, Security Incident Response and Reporting.

5. Staff members will change their password anytime the staff member believes his/her User ID or password has been compromised, or whenever directed by the Security Officer or his designee.

D. Validating and Authenticating Users

1. The Security Officer or his designee will ensure that all workstations and portable devices are configured as necessary to enable security mechanisms and automatic log-offs (if needed) and to require unique IDs and passwords. The Security Officer or his designee will also ensure that all applications used to store, receive and transmit EPHI require the use of unique user IDs and passwords.

2. The Security Officer or his designee will ensure that all workstations and portable devices employ inactivity timers or automatic log-off mechanisms (e.g., password protected screensaver that blacks out screen activity.). Except as provided below, these mechanisms must terminate a user session after a reasonable period of inactivity.

a. Servers, workstations or portable devices that access, transmit, receive, or store EPHI, and are located in locked or secure environments need not implement inactivity timers or automatic log-off mechanisms.

b. If a system that otherwise would require the use of an inactivity timer or automatic log-off mechanism does not support an inactivity timer or automatic log-off mechanism, the Security Officer or his designee will implement one of the following procedures:

i. The system will be upgraded to support the required inactivity timer or automatic log-off mechanism;

ii. The system will be moved into a secure environment; or

iii. All EPHI will be removed and relocated to a system that supports the required inactivity timer or automatic log-off mechanism.

c. When leaving a workstation or portable device for an extended period of time, such as at the end of the workday, staff members must lock or activate the system's automatic log-off mechanism or logout of all applications and database systems containing EPHI.

3. Staff members will report to the Security Officer any inadvertent transmission of EPHI by the staff member to an unintended person or entity, as well as report any responses to a transmission of EPHI that the staff member receives from an unknown or unintended person or entity.

4. The Security Officer or his designee will arrange for an annual review of systems, unless required sooner as a result of a security incident or other malfunction, to ensure that all security mechanisms are still enabled and functioning. All new workstations and portable devices will be properly configured prior to use.

E. Transmission of Data Files Containing EPHI

1. All data files containing EPHI must be secured before transmitting them outside of the Company's internal computer network.

    a. Eligibility and Encounter data files must be secured via PGP encryption, password protected ZIP files, or other customer supplied secure transport mechanisms. Whenever possible, User IDs and Passwords should be communicated verbally. However, if the situation calls for email communication, User IDs and Passwords must be sent in separate emails.

    b. Email attachments containing EPHI must be secured either through PGP encryption, password protected ZIP files, or other customer supplied secure transport mechanisms.

2. Unless approved by the Security Officer in advance, the only exceptions to that specified in item E.1 above is when a secure network connection has been established with the customer, or if a customer supplies access to a secure email system.

I. POLICY

It is the policy of the Company to implement reasonable measures to prevent security incidents. Nonetheless, the Company recognizes that, despite all reasonable measures, there may be instances in which a security incident will occur. It is the policy of the Company to encourage the reporting of any suspected or known events or incidents, to respond appropriately to any reported incidents or to any incidents detected through the monitoring of the IT system, to mitigate the harmful effects of known events or incidents (including the imposition of employee sanctions if necessary) and to document security incidents and their outcomes.

II. PURPOSE

The purpose of this Policy is to define a security incident, describe the circumstances that may indicate that a security incident has in fact or possibly occurred and outline the reporting, response, documentation and post-incident procedures. This Policy also describes the sanctions that may be imposed against any staff member whose actions have been in violation of the Company's security policies and have caused the Company's IT system to be vulnerable to external threats, as well as the mitigation to be considered by the Company as a result of a known security incident.

III. SCOPE

This Policy applies to "security incidents" as defined by the HIPAA Security Rule, i.e., attempted and successful instances of unauthorized access, use, disclosure, modification or destruction of EPHI or interference with IT system operations. It applies as well to any event or circumstance that, even on a temporary basis, makes the Company's system vulnerable to attack, including changes in the IT system or actions by staff members who either accidentally or intentionally fail to follow the established policies and procedures of the Company. A Security incident may also constitute a "breach" that is additionally subject to HIPAA Privacy Policy 32 (Breach Notification).

IV. PROCEDURE

A. Recognizing a Security Incident

1. The following circumstances may be indicative of a security incident, may cause a temporary lapse in security or may be a precursor to a potential security incident:

a. anti-virus software alerts regarding a virus, worm or other malicious code attack;

b. persistent intrusion attempts from any entity;

c. system slowdown;

d. data loss on one or more workstations, on the server(s) or on any hard drive or back-up tape;

e. server crash;

f. receipt of threatening email messages;

g. unusually slow access to the internet;

h. large number of bounced emails with suspicious content;

i. auditing configuration change in log;

j. server log entries showing use of a Web vulnerability scanner;

k. unusual deviation from normal network traffic flows;

l. a workstation, laptop or server processor whose CPU utilization is noticed to be abnormally high (e.g., 90% or more) for an extended period of time (more than a few minutes);

m. a change in user accounts (e.g., addition, deletion or modification of access rights or profiles);

n. absence of incoming or outgoing emails for an abnormally long period of time;

o. the unusual appearance of any new file, directory, software, icon, toolbar, shortcut, desktop wallpaper or screensaver;

p. any sudden or unusual problems with logging in using the normal ID and password;

q. the appearance of an unknown or unrecognized username or user log-in screen, other than what is normally expected;

r. the sudden change of your internet “home page,” or a scenario where multiple browser windows seem to open up on their own; or

s. any situation where you think someone’s user ID or password might have been compromised or shared with someone.

2. The following are security incidents regardless of the circumstances:

a. network or system intrusion by an unauthorized person;

b. theft or loss of any device that may contain EPHI, such as a laptop, PDA, cell phone, hard drive, back-up tape or drive, etc.;

c. any email that may contain EPHI, that are not transmitted using the Company's own internal mail server system;

d. any situation in which a staff member inadvertently transmits EPHI to an unintended person or entity;

e. any situation in which a staff member receives a response to a transmission of EPHI from an unknown or unintended person;

f. connection of any of the Company's IT components (including portable components) to any other network, including a home network or local "WIFI" hot spot, regardless of whether permanent or temporary; or

g. compromise of any user ID or password (e.g., sharing a password or user ID with any other internal or external entity).

3. In addition, violation of the security policies of the Company is a reportable security incident if the prohibited action creates a vulnerability in the IT system. Inappropriate usage of the network and/or internet by staff members will always constitute a reportable security incident.

B. Reporting Security Incidents

1. All staff members will promptly report any suspected or known security event or incident to the Security Officer and/or any executive officer of the Company, i.e., all staff members will report any of the signs, events or circumstances listed in A.1, A.2 or A.3. The Security Officer or his designee will, as deemed appropriate in his/her discretion, complete the incident report form attached to this Policy as Exhibit A. Self-reporting is highly encouraged.

2. The Security Officer or his designee will log each report into the Security Event/Incident Log. The Log may be maintained electronically, as long as no part of the log is overwritten during any running 6-year period. The log will require the following data, at a minimum: (a) the date and time of the event that is the subject of the report, if known; (b) the date and time of the report; (c) a description of the event; (d) a description of any steps taken to determine whether an incident has occurred; (e) a description of any steps taken to

eradicate the incident and recover from the incident; and (f) the outcome and any mitigation undertaken as a result of the incident.

C. Responding to the Security Incident

III. The Security Officer or his designee will oversee the investigation of all reported events or incidents, to include some or all of the following steps; investigation of certain events may only require the steps necessary to rule out an incident:

a. Determine whether a security incident has actually occurred, e.g., a detection device can give false positives or an event may not have resulted in a vulnerability. Assume that an incident has occurred until it is determined that it has not.

b. Determine if the incident can be handled and/or analyzed internally or will require the assistance of outside consultants and vendors. If an outside consultant is brought in, the subsequent steps will be taken in conjunction with the consultant.

c. Refer any incident that involves unauthorized acquisition, access, use or disclosure of protected health information to the Company Privacy Officer for further investigation of whether a breach has occurred that is subject to HIPAA Privacy Policy 32 (Breach Notification).

d. Determine the scope of the incident, such as which networks, systems or applications are affected, who or what originated the incident and how the incident is occurring (e.g., what tools or attack methods are being used, what vulnerabilities are being exploited, etc.)

e. Obtain the firewall log from the firewall vendor for the period of time in question. Review the firewall log, server and individual application logs, and mail exchange log to pinpoint any unusual activity, if possible.

f. Prioritize incidents if more than one incident has occurred and previous incidents have not been resolved. Consider the current and potential effect of the incident and the criticality of the affected resources.

g. Record all facts regarding the incident, documenting events, telephone conversations, and observed changes to files. Copy any error messages that the system provides.

IV. The Security Officer or his designee will, as soon as possible, notify affected staff members and, if necessary, management personnel, of any changes in use and access caused by the incident or the investigative process.

V. The Security Officer or his designee and consultants, as necessary, will contain the incident or the cause of the incident as soon as reasonably possible under the circumstances. Possible actions may include shutting down the system, disconnecting from a wired or wireless network, disconnecting a modem cable or disabling certain functions. The type of containment will vary for different types of incidents. The goal is to minimize the business impact of the incident.

VI. The Security Officer or his designee will take steps to restore systems following containment. See Policy No. 10, Contingency Plan. Recovery may include rebuilding systems, replacing compromised files with clean versions, installing patches, changing passwords, tightening perimeter security measures and employing higher levels of system logging or network monitoring.

D. Mitigating the Security Incident

If the Privacy Officer has determined that the incident constitutes a breach, i.e., that unauthorized acquisition, access, use or disclosure has occurred that compromises the security or privacy of protected health information, the Privacy Officer will take action in accordance with the HIPAA Privacy Policy 32 (Breach Notification). The Privacy Officer will notify the Security Officer of this finding for logging in the security incident log.

E. Learning from the Security Incident

The Security Officer or his designee will hold a “lessons learned” meeting with staff members as soon after a major incident as possible to review what occurred, what was done to intervene and how well the intervention worked. At the meeting, staff may discuss what they might do differently in a future similar incident, what prevention might work and what additional tools would make detection or investigation easier or quicker in a future incident.

F. Sanctions

The Company will impose appropriate sanctions against staff members for violation of the Company’s security policies, as well as violation of the Company’s privacy policies. Depending upon the nature and circumstance of the violation, the sanction may include a warning, suspension or termination of employment. The nature of the violation, the degree of harm caused by the

violation and the cooperation of the staff member will be considered in determining the type of sanction, if any, that will be imposed for any violation of this Policy. 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.

V. DOCUMENTATION

The Company will retain all documentation regarding an incident for a period of six (6) years after the incident occurred or was reported, whichever is earlier. The Human Resources Department will maintain a record, in a staff member's personnel file, of any sanctions imposed under this Policy.

EXHIBIT A
EVENT/INCIDENT REPORT FORM

Event/Incident Reported By: _____

Position:_____ Date of Report:_____

Date/Time of Event/Incident_____

Description of Event/Incident:_____
_____
_____
_____
_____
_____

OFFICE USE ONLY:

Reviewed By:_____ Date:_____

Referred to Privacy Officer for Breach Investigation: _____Yes _____ No

Incident Log Entry Date:_____

Investigation By:_____

Summary of Findings and Response:_____
_____
_____
_____
_____

Sanctions: _____ Yes _____ No

Date Incident Log Completed: _____

TERMINATION PROCEDURES RELATED TO SECURITY MAINTENANCE **POLICY: 5**

I. POLICY

It is the policy of the Company to ensure that the security of the Company's facilities and IT systems is maintained when a staff member's relationship with the Company terminates or is modified.

II. PURPOSE AND SCOPE

It is the purpose of this Policy to provide a checklist of actions to be taken when a staff member terminates or modifies his/her relationship with the Company. When the relationship is terminated the checklist in Section III.A should be added to any existing employee termination checklist and exit interview form used by the Company. When the relationship is modified, the checklist in Section III.B below should be added to any other procedures necessary to the modification in job duties. The termination checklist may also be used when a relationship with an outside consultant or vendor terminates.

III. PROCEDURE

A. TERMINATION CHECKLIST

The Security Officer and/or Human Resources department will ensure that the following steps are taken whenever a staff member's relationship with the Company is terminated (most of these steps should be taken at the time of termination or within the first 24 hours if possible):

1. Retrieve all keys, access cards or any other physical device that provides access to the facility or any workstation within the facility. If the staff member does not have all such items with him/her, consider accompanying the staff member to the location where such items are kept.

2. Retrieve any portable devices or media that contain or may contain EPHI, such as PDAs, laptops, cell phones, portable drives, memory cards, disks, CDs, back-up tapes, etc. If the staff member does not have all such items with him/her, consider accompanying the staff member to the location where such items are kept.

3. If the Company is terminating the staff member for cause, escort the staff member to his/her workstation to collect belongings and escort the staff member out of the facility to ensure that the staff member is unable to sabotage the operating system or remove any EPHI.

4. If the Company is terminating the staff member for cause, change facility locks or change facility access codes.

5. Overwrite or change the staff member's password in the operating system. Do not delete the staff member user ID at this time. Changing the password, without deleting the user ID, will allow the Company to retrieve business emails that require attention by other staff members. Continue in this mode until assured that no further business emails will be coming to the former staff member.

6. Send notice of the terminated relationship to key contacts who would normally have communicated with the former staff member.

7. Delete the staff member's user profile or account from any remote access terminal or dial-in server and take all other steps necessary to ensure that the former staff member cannot remotely access [Provider's] system or EPHI.

8. If the Company uses a document management system, move all of the former staff member's documents into another user name, such as "former employee," so that the documents can be retrieved after the staff member's user ID is deleted from the system.

9. After a reasonable waiting period and completion of the step in No. 8 above, delete the former staff member's user ID from the operating system.

10. Maintain all termination documentation for a period of six years (or longer, if required by law) after its creation.

11. Make appropriate entry into the Staff Access Log.

12. Test the effectiveness of the process for deleting user IDs on the operating system within one week of deletion.

B. JOB MODIFICATION CHECKLIST

The Security Officer and/or Human Resources department will ensure that the following steps are taken whenever a staff member's relationship with the Company is modified (i.e., a change in job classification that will require different access rights):

1. Discuss with the staff member the changes in access rights under the modified job classification.

2. Retrieve all keys, access cards or other physical devices that provide access to parts of the facility or any workstation that will no longer be accessed or used under the modified job classification.

3. Retrieve any portable devices or media, such as PDAs, laptops, cell phones, portable drives, memory cards, disks, CDs, back-up tapes, etc, that may contain EPHI that are not necessary to the modified job classification.

4. Send notice of the modified job duties to key contacts who would normally have communicated with the staff member under the former job classification.

5. Delete the staff member's user ID, if feasible, in programs to which the staff member no longer needs access under the modified job classification. Modify remote access to such programs as well.

6. Make appropriate entry into the Staff Access Log.

7. Add the staff member's user ID and password to programs to which the staff member will need access in modified job classification. Facilitate remote access as well if remote access in necessary to the job classification.

I. POLICY

It is the policy of the Company to provide training to each staff member, during new employee orientation and periodically thereafter, regarding the policies and procedures of the Company related to the confidentiality, availability and integrity of EPHI. In addition, the Company will maintain an ongoing system of security reminders regarding practical issues that point out the importance of good security practices. Those members of the staff who will use EPHI as part of their regular job duties may receive more detailed training than those who do not normally use EPHI.

II. PURPOSE

The purpose of this Policy is to outline the topics for training, differentiate among staff positions as to the type and extent of necessary training, provide suggested methods of training and provide a mechanism for documenting completed training.

III. SCOPE

This policy applies to the training of staff members only with respect to securing EPHI. It does not apply to other required training. The term "staff member" does not include vendors or consultants.

IV. PROCEDURES

A. PREPARING A TRAINING PROGRAM

1. All employees must receive training in the following areas related to the security of EPHI:

a. an overview of the HIPAA Security Rule;

b. an overview of the Company's general plan to meet the requirements of the Security Rule;

c. details about acceptable use of the Company's IT system and what is expected from each staff member (Policy No. 7);

d. details about facility access controls and workstation security (Policy No. 8);

e. guidance as to how to recognize a suspected security incident, as well as how and when to report a suspected or known security incident (Policy No. 4);

f. information regarding the Company's contingency plan (Policy No. 10);

g. details regarding the sanctions that the Company may use to enforce compliance with the Company's policies and procedures regarding the security of EPHI (Policy No. 4); and

h. information regarding workstation access and authorization procedures (Policy No. 3).

2. IT personnel will receive additional training in the following areas:

a. details regarding information system activity review (Policy No. 2); and

b. details regarding repair, maintenance, disposal and re-use of IT components and media that are used to store, receive or transmit EPHI (Policy No. 9);

3. The Security Officer and/or his designee will develop a training program. The training methodologies may include in-service classes, computerized training modules, individual review of the policies and procedures or any other methodology that is reasonably designed to inform staff members of their responsibilities related to the security of EPHI.

B. CONDUCTING TRAINING

1. The Human Resources department will develop a training schedule that will provide annual training to all staff members. The training will be mandatory.

2. The Human Resources department will ensure that above training is part of the new staff orientation program, with all training completed within a reasonable time after hire (within 10 business days for new hire dealing directly with EPHI; within 30 business days for new hire not dealing directly with EPHI).

3. Each staff member will be required to sign a Training Sign-in Sheet when attending a training session.

4. The Human Resources department will retain all Training Sign-In Sheets for a period of six (6) years from the date of the training.

5. Documentation of staff training for new hires may be combined with documentation of training under the HIPAA Privacy Rule.

C. DEVELOPING A SECURITY REMINDER SYSTEM

1. The Security Officer or his designee will establish a means of providing periodic security reminders to staff members. The Security Officer or his designee will use any method that will effectively communicate changes in law, new cases or incidents of interest, virus alerts and reminders about acceptable use, etc. to staff members, such as the internal email system, a newsletter, staff meetings, a memo, etc.

2. Staff members are encouraged to pass on to the Security Officer security-related information that may be of interest to other staff members.

3. Documentation of the security reminders will be retained for six years after they are shared with staff members.

I. POLICY

It is the policy of the Company to help ensure the security of the Company's IT system and the integrity of EPHI by clearly defining the acceptable uses of the Company's IT system by staff members and contractors. Adherence to this Policy will help the Company guard against internal and external attacks that deny authorized access or result in the loss, dissemination, or compromise of EPHI in the Company's possession.

II. PURPOSE

It is the purpose of this Policy to provide the Company's staff members with guidelines regarding acceptable uses of the Company's IT system, in order to avoid compromising the integrity of the IT system by inadvertent exposure to malicious software and other external attacks. This Policy also sets forth procedures for detecting and reporting malicious software. This Policy applies to all staff members of the Company.

III. SCOPE

The Company's IT system represents a significant financial asset and is integral to the Company's operations. All data, in any form, created or stored on or transmitted through the Company's IT system, is the property of the Company. Therefore, any document, file or data, whether in the form of text, audio, video, image or photo, or any email, voicemail or other message composed, sent, received, forwarded or stored on or passing through the Company's IT system is the property of the Company and is subject to this Policy.

IV. ACCEPTABLE USE GUIDELINES

A. DEFINING IT SYSTEM

For purposes of this Policy, "IT system" includes, but is not limited to, the following:

1. Any and all computer and network infrastructure provided and/or maintained by the Company, including desktop and laptop workstations, servers, routers, switches, hubs, firewalls, peripherals, electronic storage devices and related media, PDAs, printers, copiers, scanners, audio/video equipment and all similar devices, whether or not they are attached to the Company's network;

2. Any and all software applications (purchased or leased) and installed on the Company's computer IT system;

3. Internet resources, including the Company's web site, email system, intranet(s) or extranet(s); and

4. Any third-party IT system accessed by or through the Company's IT system (for example, a personal e-mail account on Yahoo! accessed through the Company's IT system is covered by this Policy).

B. USING THE IT SYSTEM APPROPRIATELY

1. General Rules. Staff members will follow these rules when using the Company's IT system, unless otherwise authorized by the Security Officer or any executive officer of the Company:

a. Do not use peer-to-peer file sharing programs such as Kazaa, Morpheus or Limewire;

b. Do not download free programs offered on the Internet, including "free" anti-virus software;

c. Do not click on pop-ups, including those that purport to fix a "problem" with the computer;

d. Do not defeat nor disable any security features at a workstation or on a portable device;

e. Do not access, or attempt to access, the directories of other staff members or any documents, emails files or other similar items that are addressed to other staff members without specific authorization;

f. Do not access websites, or generate, store or forward email or voicemail or files (including images, text, audio, video, etc.) which contain offensive, threatening or disruptive materials;

g. Do not gain unauthorized access to others' networks or IT system (frequently referred to as "hacking") to access content that is the intellectual property, copyrighted material and/or trade secrets of another organization;

h. Do not use another person's account or an alias to access the IT system and/or external networks or systems;

i. Do not generate or transmit any material, in any form, that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin or disability;

j. Do not generate bulk messages (frequently known as "SPAM"), or facilitate pyramid marketing, chain letters or the promotion of hoaxes; and

k. Do not conduct any activity on the IT system not specifically in furtherance of your job responsibilities for the Company.

2. Email Use. Staff members should restrict email usage to that which is required to complete the staff member's job responsibilities. Staff members should not assume confidentiality of messages transmitted via email or over the Internet on the Company's IT system. The Company reserves the right to monitor and/or inspect any employee's email usage. Staff members will not put the Company's authorization codes, credit card numbers, or similar items in email messages without the prior authorization of the Security Officer or an executive officer of the Company.

3. Internet Use. Staff members should restrict Internet use to business purposes only during working hours. All Internet usage is tracked and monitored by the IT Department. Any employee that violates this policy may be subject to disciplinary action, up to and including termination.

4. Installation of Hardware and Software. To prevent the introduction of malicious code and protect the integrity of the Company's IT system, staff members will obtain all hardware and software from the Company. Staff members may not install software without prior approval of the Security Officer or the Director, Information Technology.

5. Software Licenses. All software used on the Company's IT system is licensed and/or registered in the name of the Company. Staff members will abide by software copyright laws and will not obtain, install, duplicate or use software except as permitted by the Company's software licensing agreements.

C. USING PERSONAL EQUIPMENT

If a staff member remotely accesses the Company's IT system or voice mail system with a home computer or portable device, all EPHI that is temporarily stored on the staff member's computer or portable device will be removed immediately after use and not stored permanently. Personal equipment may not be directly connected or attached to the Company's IT system without the prior approval of the Security Officer. No staff member will use personal equipment, including cell phones, in the facility unless approved in advance by the Security Officer and/or an executive officer.

D. DETECTING AND REPORTING SUSPICIOUS EVENTS

1. If a staff member experiences any of the following events that may indicate the presence of malicious software and/or a security incident, the staff member will report it to the Security Officer and/or any executive officer of the Company:

a. anti-virus software alerts regarding a virus, worm or other malicious code attack;

b. persistent intrusion attempts from any entity;

c. system slowdown;

d. data loss on one or more workstations, on the server(s) or on any hard drive or back-up tape;

e. server crash;

f. receipt of threatening email messages;

g. unusually slow access to the internet;

h. large number of bounced emails with suspicious content;

i. auditing configuration change in log;

j. log entries showing use of a Web vulnerability scanner;

k. unusual deviation from normal network traffic flows;

l. a workstation, laptop or server processor whose CPU utilization is noticed to be abnormally high (e.g., 90% or more) for an extended period of time (more than a few minutes);

m. a change in user accounts (e.g., addition, deletion or modification of access rights or profiles;

n. absence of incoming or outgoing emails for an abnormally long period of time;

o. the unusual appearance of any new file, directory, software, icon, toolbar, shortcut, desktop wallpaper or screensaver;

p. any sudden or unusual problems with logging in using the normal ID and password;

q. the appearance of an unknown or unrecognized username or user log-in screen, other than what is normally expected;

r. the sudden change of your internet “home page,” or a scenario where multiple browser windows seem to open up on their own; or

s. any situation where you think someone’s user ID or password might have been compromised or shared with someone.

2. Staff members are encouraged to make good faith reports to the Security Officer and/or any executive officer of the Company regarding any instance in which they observe the inadvertent or intentional violation of this policy by other staff members. Staff members are also encouraged to self-report their own inadvertent violations of this Policy. The nature of the violation, the degree of harm caused by the violation and the cooperation of the staff member will be considered in determining the type of sanction, if any, which will be imposed for any violation of this Policy.

3. The Security Officer or his designee will investigate the event in accordance with Policy No. 4 regarding security incident reporting and response. The Company reserves and intends to exercise the right to review, audit, intercept, and access all data without the permission of the staff member on any workstation or Company provided portable device.

I. POLICY

It is the policy of the Company to limit access to the facility and to stationary and portable workstations to only those persons with appropriate authorization so as to prevent unauthorized physical access, tampering or theft.

II. PURPOSE

It is the purpose of this Policy to describe the security mechanisms and procedures that will be implemented to assure the physical security of the facility (or parts of the facility housing workstations or equipment, as well as the security of the equipment and workstations themselves that are used to store, receive or transmit EPHI.

III. SCOPE

This Policy applies to stationary equipment used to store, receive or transmit EPHI, as well as to portable equipment used to store, receive or transmit EPHI, such as laptops, PDAs, etc. This policy applies where indicated to remote access by and home computers of staff members.

IV. PROCEDURE

A. Securing the Facility

1. The Security Officer or his designee will ensure that the main entrance door to the Company's office facility has a lock or electronic security system in place that is used after regular business hours. After hours access will be restricted to only those staff members whose job duties require after hours access, as described in the job description for that position (see Policy No. 3.), and to authorized designees of the landlord. In the case of an emergency requiring after hours access by a vendor, the vendor will be accompanied by a staff member with appropriate access rights. The Company will not, if feasible, furnish IT vendors, other vendors or repair personnel with keys, access cards or access codes.

2. The Security Officer or his designee will ensure that any doors to the Company's office facilities have a lock or electronic security system for use during and after regular business hours.

3. The Security Officer or his designee will ensure that, to the extent that certain equipment, such as servers, are housed in one or more separate rooms within the facility, the entrance to the rooms will be locked or subject to an electronic security system after regular business hours to prevent unauthorized

access. The Security Officer will provide the key, access card or access code only to those staff members whose job duties require access to the room. The Security Officer will encourage use of the locks or security system during regular business hours to the extent feasible but will require use of the locks or security system at any time that authorized staff members are not present in the room(s).

4. To the extent that equipment and workstations used to store, receive or transmit EPHI are dispersed through the facility during regular business hours, the Security Officer or his designee will ensure that appropriate physical security measures are in place to protect the workstations, as described in Section B below.

5. Keys, access cards or access codes will be changed periodically as follows:

a. At any time that the Security Officer and/or executive management deem advisable;

b. Whenever a staff member is terminated for cause; or

c. In response to a suspected or known security incident involving physical security.

B. Securing Equipment and Workstations

1. The Security Officer or his designee will ensure that all accounts are password protected, and that system administrator access is only given to those few individuals who actually need it. The Security Officer and/or his designee(s) will use the system administrator account only when required; under normal use, the Security Officer and/or his designee(s) will use a non-system administrator account.

2. The Security Officer or his designee will ensure that security patches and anti-virus updates are regularly downloaded to the Company's server(s) and individual workstations.

3. The Security Officer or his designee will do the following to physically secure equipment and workstations used in the facility and safeguard portable equipment:

a. Prepare and maintain an inventory of (a) all equipment and workstations that store, receive or transmit EPHI, to include servers, workstations,

laptops, storage systems (including back-up tapes and other removable media), and (b) all software applications that are used to store, receive or transmit EPHI. The Security Officer or his designee will update the inventory as new equipment is added to or deleted from the IT system or as changes in staff occur. If portable equipment is not permanently in the possession of any one staff member but is shared among staff members, the Security Officer or his designee will develop a tracking system for such items.

b. Implement network perimeter security and access control with a firewall installed between the server(s) and the outside network. The firewall will be configured to meet the following minimum requirements:

(i) limit network access to only authorized staff members and entities;

(ii) limit network access to only legitimate or established connections;

(iii) secure console and management ports;

(iv) log failed access attempts; and

(v) be located in a physically secure room.

c. Install anti-virus software and spyware tools on the server(s) and on workstations.

d. Direct all staff members to position workstations in a manner to avoid inadvertent or intentional viewing by unauthorized staff members or third parties, such as vendors, repairpersons, and other visitors.

e. Enable screen saver and automatic log-off mechanisms on any workstation that is located in an area that may be viewed by unauthorized staff members or visitors.

f. Enable security features as appropriate on each workstation.

g. Restrict all remote access to the Company's network to a secure method of access, unless otherwise authorized by the Security Officer or any executive officer of the Company.

4. Staff members will take the following steps to secure equipment and workstations used outside the office, including home computers, PDAs, laptops and memory cards:

a. Lock all vehicles in which the Company's equipment and workstations are being transported.

b. Enable screensaver and automatic log-off mechanisms.

c. Enable appropriate security features, including features that lock the workstation after inactivity and require a secure password to reactivate.

d. Never leave the equipment or workstation unattended with EPHI in an accessible mode.

e. Use home computers only for the purpose of remote access so that EPHI is not stored on the home computer.

f. Regularly update security patches and anti-virus software (after consulting with IT staff to determine their applicability).

g. Not use PDAs, cell phones or memory cards for long term storage of EPHI; all EPHI should be purged every 30 days.

5. The following rules apply to staff members using remote access:

a. Use a unique ID and password for authentication purposes;

b. Never use any mechanism to bypass authorized remote access mechanisms;

c. Ensure that the remote workstation has up-to-date anti-virus software;

d. Never give password to another person.

6. The Security Officer or his designee will disable all unused or unnecessary equipment or workstations.

C. Securing Wireless Workstations

1. The Security Officer or his designee will consult with the Company's IT vendor regarding the appropriate encryption for all wireless devices to prevent external intrusion. All encryption mechanisms that are implemented must support a minimum of 128-bit encryption. The Security Officer or his designee will arrange to periodically test the effectiveness of the encryption by conducting a vulnerability scan.

2. The following rules apply to staff members using wireless devices:

a. Enable encryption at all times – minimum 128-bit.

b. Use a unique ID and password.

c. Never install or use an unmanaged, ad hoc or rogue wireless access point that is inside or outside the Company's firewall or network, unless otherwise authorized by the Security Officer or any executive officer of the Company.

D. Documenting Physical Safeguards

The Security Officer or his designee will record changes in locks, access cards or access codes.

I. POLICY

It is the policy of the Company to ensure that the security of EPHI is maintained during and after repairs, periodic maintenance or upgrades of the IT system and individual equipment used to store, receive and transmit EPHI. In addition, it is the policy of the Company to ensure that EPHI is effectively deleted or removed from IT equipment and media before disposal or re-use, either by the Company or by a third party.

II. PURPOSE

It is the purpose of this Policy to describe the procedures to be followed to secure EPHI whenever the IT system or any of its parts is repaired, maintained, upgraded, removed from use or re-used, either at the facility or elsewhere.

III. SCOPE

This Policy applies to repairs, maintenance or upgrade of any portion of the IT system that is used to store, receive or transmit EPHI. This Policy also applies to the disposal or re-use of IT equipment or media.

IV. PROCEDURE

A. Repairing and Maintaining the IT System

1. The Security Officer or his designee will establish and retain a log of all repairs, maintenance and upgrades to any component of the Company's IT system that is used to store, receive or transmit EPHI. The log will include, at a minimum, the date of service, the staff member or vendor performing the service, a brief description of the service and the IT system component(s) subject to the service and any actions taken to secure the IT system after the service. The log and file will be retained for six years from the date of service or date of creation, whichever is applicable.

2. The Security Officer or his designee will establish and maintain a Staff Access Log for the purpose of tracking the dates on which access rights to the IT system are granted, modified or terminated for staff members and documentation regarding access rights granted to visitors, including vendors, repair persons and consultants. The access logs will be retained for six years following any entry in the logs. (See also Policy No. 3, Access Management and Authentication.)

B. Removing EPHI Before Disposal or Re-use of IT Equipment and Media

1. Prior to disposing of or re-using any hard drive, disk, CD, flash drive, back-up tape/drive or other type of storage device or removable media, the Security Officer or his designee will ensure that a retrievable copy of the EPHI exists in the IT system.

2. Prior to disposing or re-using any hard drive, disk, CD, flash drive, back-up tape/drive or other type of storage device or removable media, the Security Officer or his designee will ensure the removal or deletion of EPHI. A typical delete and/or reformat is not sufficient, because deleted data can typically be recovered from hard drives. Measures to be considered include:

   a. disk wipers/scrubbers;

   b. physical or electronic destruction or defacement (such as degaussing);

   c. a system for overwriting; or

   d. any other mechanism that ensures that the data cannot be recovered.

Notwithstanding the foregoing, EPHI should not be deleted from a back-up tape/drive that will continue to be used in rotation and is stored and transported in a secured environment.

3. The Security Officer or his designee will periodically assess the effectiveness of the chosen data destruction or deletion mechanism used.

I. POLICY

It is the policy of the Company to have a contingency plan to ensure that EPHI is regularly backed up, is available in an emergency situation to those with authorization for access and is protected from unauthorized use or disclosure despite an emergency or disaster.

II. PURPOSE

The purpose of this policy is to outline the standard procedures for the following tasks:

A. Applications and Data Criticality Analysis to assess the relative criticality of specific IT systems applications and data in support of other Contingency Plan components.

B. Data Back-up to ensure that the Company will at all times be able to create and maintain exact copies of EPHI;

C. Disaster Recovery/Emergency Mode Operation to allow the Company to restore any loss of data in the event of a disaster or other emergency and to continue critical business processes for the protection of EPHI while operating in emergency operations mode; and

D. Testing and Revision to permit the Company to periodically test and revise the Contingency Plan as necessary.

III. SCOPE

This Policy applies whenever there is a disruption in any part of the IT system housing or using EPHI, such as a disruption caused by the malfunction of an IT component, by power outage, by natural disaster, by accidental user error, or from outside malicious threats and acts.

IV. RESPONSIBILITY

To ensure that decision-making authority during contingencies is uninterrupted, a Disaster Management Team has been established. The responsibilities and tasks to be carried out by the Disaster Management Team during a contingency operation is detailed in Section 3 – Recovery Teams and Responsibilities of the Company's Disaster Recovery Plan.

V. PROCEDURE

A. Data and Criticality Analysis.

1. The following is a list of the Company's IT components, in descending order of importance to key functions (more detailed information is included in Section 9 – Critical Systems/Services of the Company's Disaster Recovery Plan:

a. Hardware

(i) Telecommunications systems and Network components

(ii) Facsimile machine

(iii) Internet/online access

(iv) Servers for Mission Critical applications

(v) Data Back-up components

(vi) Computer workstations (in following order)

A. Workstations used to access EPHI

B. All remaining workstations

(vii) Printer(s)

(viii) Cellphones, PDAs and other devices not essential to the delivery of patient care or disaster recovery/emergency operations

b. Software

(i) Software necessary to perform Data Back-up

(ii) Patient record/health information software

(iii) All remaining software

2. The Security Officer or his designee will maintain a copy of all original software disks and CDs, along with license information, in a secure storage site. Data files sent to/from clients shall be actively retained for at least three years.

B. Data Back-up and Normal Operations.

1. The Security Officer or his designee will, on a daily basis, perform a full or partial tape back-up of the data maintained on the IT systems (the "Data Back-up"), using such tape rotation as determined by the Security Officer or his designee performing the Data Back-up.

2. The Security Officer or his designee will use a tape system in the Data Back-up that is of a type commonly used and accessible by hardware that is commonly available and typically used for this purpose (to facilitate recovery at an alternate site if necessary).

3. The Security Officer or his designee will maintain the back-up tape in a secure site each night (e.g. fireproof storage container under double lock and key) until the back-up tapes are transferred for storage to the Company's off-site storage vendor. Transfer of back-up tapes to off-site storage shall be made at least twice per week. All annual back-up tapes shall be retained at the off-site storage facility indefinitely, the last back-up tape of each month shall be retained at the off-site storage facility for one year, and daily and weekly back-up tapes shall be rotated every three weeks, or in accordance with such other tape rotation schedule determined by the Security Officer or his designee.

4. In the Security Officer's absence, the Chief Executive Officer of Superior Vision Corp. or his designee will determine who will assume responsibility for performing the Data Back-up. The Security Officer will determine all individuals to be trained in Data Back-up procedures, with re-training whenever Data Back-up procedures are modified.

5. On a daily basis, the Security Officer or his designee will verify that the Data Back-up is adequately backing up data by reviewing the corresponding logs on the IT systems.

6. At least quarterly, the Security Officer or his designee will verify and update as necessary the contact information for IT vendors, suppliers, repair persons and other individuals with whom the Company has service contracts related to IT systems (Appendix A). The Security Officer or his designee will also verify and update the Company's Emergency Response Team list. Copies of this information can be found in the Company's Disaster Recovery Plan.

7. In addition to the daily Data Back-up, the Security Officer or his designee will perform a Data Back-up immediately prior to any planned modification to or replacement of the IT system.

C. Disaster Recovery/Emergency Mode Operation.

The steps to be carried out by the Disaster Management Team in an emergency situation are described in the Company's Disaster Recovery Plan.

D. Testing and Revision

The Security Officer and/or his designee(s) will test/assess the Company's Contingency Plan no less frequently than annually. A list of tasks is included in Section 14 – Testing and Revisions of the Company's Disaster Recovery Plan.

POLICY 10 – Contingency Plan
Appendix A - Form

Contact Information for Hardware and Software

	Company	Address	Phone Number	Contact Person	Account No.
Computers					
Server(s)					
Telephones					
Printers					
Fax Machines					
Copiers					
Local Phone Service					
Long Distance Service					
Operating Software					
Office Management Software					
Miscellaneous Software					
Accounting/GL Software					

Contact Information for Vendors and Service Contractors

Company Name	Service Type	Address	Phone Number	Contact Person	Account No.

I. POLICY

The Company may disclose PHI to business associates of the Company when satisfactory assurances from the business associate have been received that the business associate will appropriately safeguard the information, and will require same from their subcontractors. In accordance with the Company's HIPAA Privacy Rule Policies and Procedures, the Company adopted a policy (Privacy Rule Policy 22) requiring a business associate of the Company that is not itself a covered entity to enter into a business associate agreement substantially in the form adopted by the Company. It is the policy of the Company that its form of business associate agreement comply with the Security Rule for those business associates that create, receive, maintain or transmit EPHI on behalf of the Company.

II. PURPOSE AND SCOPE

The purpose of this Policy is to give guidance on how the Company will comply with the HIPAA Privacy Rule and HIPAA Security Rule for those business associates that create, receive, maintain or transmit EPHI on behalf of the Company.

III. PROCEDURES

The Company will assess whether the business associate creates, receives, maintains or transmits EPHI on behalf of the Company. The business associate agreement for the Company's business associates with access to EPHI who are not otherwise covered entities will be in the form provided for in the Company's HIPAA Privacy Rule Policies & Procedures – Policy 22, Business Associates Agreement - Form.