VILLAGE OF BLOOMINGDALE
HIPAA AND HITECH PRIVACY AND SECURITY POLICY
UPDATED 07/01/2017

1.0 PURPOSE

The purpose of this Policy is to:

1.1 Outline and document the HIPAA and HITECH compliance processes for internal and external use.

1.2 Provide a reference manual for internal compliance and training.

2.0 SCOPE

This Policy represents the efforts performed to ensure compliance with HIPAA and the HITECH Act. All employees who have access to PHI must be trained in and comply with this Policy.

Group Health Plan (GHP) means an employer sponsored arrangement that includes indemnity and self-funded health plans that offer; medical benefits including HMO coverage, long term care plans, dental, vision, flexible spending accounts (FSA), health reimbursement accounts (HRA), and other plans that may provide or pay for medical care such as some EAP plans and wellness plans.

Protected Health Information (PHI) means information that is created or received for the purpose of GHP administration including:

- Information that relates to the past, present, or future physical or mental health or condition of a Participant; and,
- The provision of health care to a Participant; or the past, present, or future payment for the provision of health care to a Participant; and that identifies the Participant.

The test is whether there is a reasonable basis to believe the information can be used to identify the Participant. PHI includes information of persons living or deceased. Even GHP enrollment data for the purpose of setting up tax advantaged accounts or processing continuation services is considered PHI.

3.0 GENERAL POLICIES

3.1 No Waiver of Privacy Rights. No Participant will be required to waive his or her privacy rights under the Privacy Rule as a condition of treatment, payment, enrollment or eligibility in any employer sponsored GHP. Privacy rights waivers are not enforceable and will not be accepted.

3.2 Privacy/Security Officer and Contact Person. This Officer will be responsible for the development and implementation of policies and procedures relating to privacy and security, including but not limited to this Privacy Policy. This Officer or his/her designee will also serve as the contact person for Participants who have questions, concerns, or any complaints regarding PHI.

3.3 Workforce Training. All employees who have access to PHI will be trained on these policies and procedures. Training sessions will be held to achieve the goal that all employees be trained within 30 days of the date of first access to PHI. Each employee will be required to acknowledge that they have been trained on and will comply with this Privacy and Security Policy.

3.4 Sanctions for Violations of Privacy Policy. Sanctions for using or disclosing PHI in violation of this Policy will be imposed in accordance with applicable discipline policy, up to and including termination.

3.5 Prohibition On Sale Of PHI. There is no selling PHI in any manner for any purpose, including the sale or exchange of or PHI for any form of trade or compensation. All Employees are strictly prohibited from arranging for or providing any PHI for sale, for any purpose whatsoever.

4.0 DESIGNATED RECORD SETS

There are two categories of PHI created, obtained and maintained for GHP administration. This PHI is defined as the Designated Record Set for the purposes this Policy.

4.1 Enrollment and disenrollment data including Participant elections and demographics for administering employer sponsored GHPs.

4.2 Limited claims information submitted by a Participant or obtained from other sources for the purposes of adjudicating an appeal from an adverse benefit determination made by the insurer, Third Party Administrator, or Service Provider.

5.0 PARTICIPANT RIGHTS UNDER HIPAA AND HITECH

The Privacy Officer will respond to participant requests as follows. The Privacy Officer can charge a reasonable fee for providing this assistance:

5.1 Right To Inspect And Copy PHI. Within thirty (30) days of receiving a written request from the Participant, the Privacy Officer will make PHI maintained in Designated Record Set available to the Participant, in a reasonable time and manner. A reasonable fee for the costs of copying, mailing, or other supplies associated with the request will be charged. The request may be denied in certain limited circumstances related to the wellbeing of the Participant. If you are denied access to your medical information, you may request that the denial be reviewed by submitting a written request to the Privacy Officer identified below.

5.2 Amendment of PHI. The Privacy Officer will make reasonable amendments to PHI when the PHI is created or maintained by the GHP or a Service Provider that is not itself considered a Covered Entity. The Privacy Officer will communicate any approval or denial of an amendment of PHI maintained by the Privacy Officer or a Service Provider to the Participant. An example of an unreasonable request would be for the Privacy Officer to alter a medical record received, the Participant would be advised to ask the medical provider who created the record for such amendment.

5.3 Accounting of Disclosures. The Privacy Officer will make available to the Participant the information required to provide an accounting of disclosures. The Privacy Officer will prepare and deliver any such accounting requested.

The accounting will not include (1) disclosures for purposes of treatment, payment, or health care operations; (2) disclosures made to a Participant; (3) disclosures made pursuant to a Participant's authorization; (4) disclosures made to friends or family in a Participant's presence or because of an emergency; (5) disclosures for national security purposes; and (6) disclosures incidental to otherwise permissible disclosures. To request this list or accounting of disclosures,

the Participant must submit a request in writing to the Privacy Officer. A Participant's request must state the time period the accounting covers, which may not be longer than six years before the date of the request. A Participant's request should indicate in what form a Participant wants the list (for example, paper or electronic). The first list a Participant requests within a 12-month period will be provided free of charge. For additional lists, the Employer may charge a Participant for the costs of providing the list. The Privacy Officer will notify a Participant of the cost involved and a Participant may choose to withdraw or modify the request at that time before any costs are incurred.

5.4 The Right To Restrict The Use And Request Confidential Communications. A Participant has the right to request a restriction of uses and disclosures of their PHI. A Participant also has the right to restrict communication of their PHI if the Participant informs the Privacy Officer that communicating the information may endanger the Participant. Requests will be deemed unreasonable if they limit the access and use that is necessary for GHP administration.

If the Privacy Officer agrees to the request for a restriction, the Privacy Officer will not use or disclose the PHI in violation of the restriction, except when needed for emergency treatment, at the written request of the Participant (by authorization), or when the use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law.

The Privacy Officer may terminate its agreement to a restriction, if the Participant agrees to or requests the termination in writing; or, the Privacy Officer informs the Participant that it is terminating its agreement to a restriction. The termination is only effective with respect to PHI created or received after the Participant is informed.

5.5 Requests for Alternative Communication Means or Locations. Participants may request to receive communications regarding their PHI by alternative means or at alternative locations. For example, Participants may ask to be called only at work rather than at home. These requests will be honored if, in the sole discretion of the Privacy Officer, the requests are reasonable. However, the Privacy Officer will accommodate such a request if the Participant clearly provides information that the disclosure of all or part of that information could endanger the Participant. All such requests should be forwarded to the Privacy Officer when received.

5.6 Right to receive a HIPAA Privacy Notice. That provides a clear, user friendly explanation:

- the uses and disclosures of PHI
- the individual's HIPAA rights, and
- the GHPs legal duties with respect to the PHI.

The Employer is charged with providing a notice on the PHI that will be obtained for GHP administrative purposes and how that PHI will be used.

- An Employer must make its notice available to any person who asks for it,
- On an ongoing basis at the time of enrollment, and

- An Employer must prominently post and make available its notice on any web site it maintains that provides information about its customer services or benefits.

There is Employer discretion regarding how to deliver the Notice. Special or separate mailings are not required. The Notice may be included with other written materials that are mailed to the Participants, or included with an SPD or with enrollment materials.

The Notice can be provided by email, if the recipient has agreed to receive an electronic notice and that agreement has not been withdrawn. If it is discovered that the email transmission has failed, the Notice must be provided by a paper copy. Additional materials may be included in the email.

6.0 COMPLAINT PROCEDURES

6.1 Complaints. A Participant can file a complaint regarding the Privacy Rule or any matter described in this Privacy Policy with the Privacy Officer by sending a written description of the facts and circumstances and the acts that are the subject of the complaint to:

Attn: Privacy Officer
VILLAGE OF BLOOMINGDALE
201 S Bloomingdale Rd
Bloomingdale, IL 60108

All complaints will be forwarded to the Privacy Officer. The Privacy Officer is responsible for any response and taking necessary actions to change this complaint process or this Privacy Policy. No response from the Privacy Officer is required. A copy of this complaint procedure will be provided to the Participant.

No Employee will intimidate, threaten, coerce, discriminate against, or take other retaliatory action against Participants for exercising their rights, filing a complaint, participating in an investigation, or opposing any improper practice under the Privacy Policy or the federal Privacy Rule.

6.2 Complaints made to the Secretary. A Participant may file a complaint to the Secretary of Health and Human Services. The Employer will cooperate with an investigation by permitting access to information requested by the investigator.

A complaint to the Secretary must be made in writing, must name the entity against whom the complaint is lodged, must describe the wrongful acts or omissions and must be filed within 180 days of the time that the Participant became aware of, or should have become aware of the violation. Complaints may include violations of the Privacy Policy and Security Policy.

The U.S. Department of Health and Human Services
Privacy Rule Complaint
200 Independence Avenue, S.W.
Washington, D.C. 20201
Telephone: 202-619-0257, Toll Free: 1-877-696-6775

7.0 DOCUMENTATION

The Privacy Officer will ensure that privacy files are maintained for a period of 6 years from the date of the event as described below, or when appropriate for 6 years after the end of the Plan Year in which the document was created. The Plan Sponsor will destroy PHI that is 7 years old on a calendar basis to meet the various requirements.

7.1 Training. A copy of training materials used and the employee's acknowledgement that the employee was trained on this Policy, and they acknowledged they would comply with this Policy.

7.2 Disclosures. Including documentation of authorizations and authorized disclosures. The Privacy Officer will not document disclosures of Summary Health Information as defined above, or routine Disclosures of minimum necessary data to a Business Associate.

7.3 Complaints. Any complaint made regarding this Policy, any response, and actions taken to resolve the complaint, if any.

7.4 Inadvertent Disclosure of PHI. The Privacy Officer will document any unauthorized disclosure of PHI. All incidents need to be reviewed by the Privacy Officer to determine whether this constitutes a Breach of insecure PHI. Any questions should be referred to the Privacy Officer.

7.5 Security Incidents. See the Incident Policy below.

7.6 HIPAA Privacy Notice Distribution. A copy of the Notice distributed with documentation of the method used. The documentation should specifically show who received the notice. Examples: mailed notices can be shown by retaining a copy of the addressed postmarked envelope, email notices can be shown by retaining a copy of the email with attachments, provided with the SPD will be shown by your efforts to document the SPD delivery.

7.7 Requests for Participant Rights. Written requests for HIPAA rights, the written response if any, and the resolution of the request are documented.

7.8 Plan Document Amendment. Retain a copy of the Plan Document Amendment including future updates needed.

8.0 BUSINESS ASSOCIATES

8.1 Business Associates. A Business Associate is an entity or person who: 1) Performs or assists in performing a GHP function or activity involving the use and disclosure of PHI (including claims processing or administration; data analysis, underwriting, etc.); or 2) Provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services, where

the performance of such services involves giving the Service Provider access to PHI. A Business Associate is required to enter an agreement with the Covered Entity that HIPAA compliance is in force. Business Associates will only use and disclose protected health information consistent with this Policy.

8.2 Contracts With Business Associates. The Employer may disclose PHI to a Business Associate and allow the Business Associate to create or receive PHI on its behalf. However, prior to doing so, the Employer must first obtain assurances from the Business Associate that it will appropriately safeguard the information. This assurance is in the form of a Business Associate Contract.

9.0 DISCLOSURES

No Disclosure of PHI for Non-Health GHP Purposes. PHI may not be used or disclosed for any purpose except as defined and limited in this Policy. PHI may not be used or disclosed for the payment or operations of "non-health" benefits (e.g., disability, worker's compensation, life insurance, etc.), unless the Participant has provided an authorization.

IMPORTANT NOTE: All transmissions of PHI are sent or received in a secure environment. The level of security will depend on the nature of the data. Enrollment and Disenrollment data that includes Social Security Numbers will be encrypted, sent in a secure email environment where available. Enrollment and disenrollment data that does not include Social Security Numbers is password protected where the password is sent under a separate cover.

Disclosure can be made to anyone designated as a personal representative, or attorney-in-fact by the Participant. The Participant must provide a written notice/authorization and supporting documents such as a power of attorney. The Employer will not disclose information to a personal representative if there is a reasonable belief that the Employee has been, or may be, subjected to domestic violence, abuse, or neglect by such person; or treating such person as a personal representative could endanger the Participant.

Complying With the "**Minimum Necessary**" Standard. PHI disclosures are limited to the "minimum necessary" data to accomplish the purpose for the disclosure. The "minimum necessary" standard does not apply to the following:

- uses or disclosures made to the Participant upon request;
- uses or disclosures made pursuant to a valid authorization; or,
- disclosures required by law or regulation made pursuant to a valid subpoena or request from a governmental entity.

Minimum Necessary is further defined for enrollment purposes as the name, GHP elections, effective and termination of coverage dates, demographics required to identify the individual, and balance data for account balance purposes.

9.1 Routine Disclosures. Routine disclosures insurers, Third Party Administrator, and Service Providers for the purpose of GHP administration can be made without prior participant authorization. The transmissions will comply with the Minimum Necessary Rule and be limited to

enrollment/disenrollment data and monetary account balance information for the purpose of making enrollment changes.

9.2 Disclosures of Summary Health Information. Summary health information may be disclosed without prior participant authorization. This information does not provide a reasonable basis to believe that it can be used to identify an individual. Summary health information must have the following 18 identifiers redacted:

- names;
- geographic subdivisions smaller than a state, aggregated to the level of a five-digit ZIP code;
- dates (except year) directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age (ages and elements may be aggregated into a single category of age 90 or older);
- telephone numbers;
- fax numbers;
- e-mail addresses;
- Social Security numbers;
- medical record numbers;
- GHP beneficiary numbers;
- account numbers;
- certificate/license numbers;
- vehicle identifiers and serial numbers, including license plate numbers;
- device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) addresses;
- biometric identifiers, including finger and voice prints;
- full face photographic images and any comparable images; and
- any other unique identifying number, characteristic. Disclosures of summary health information must be pre-approved by the Privacy Officer.

9.3 Plan Certification. In order for the insurer, Third Party Administrator or Service Provider to release any PHI to the Employer other than the minimum necessary information defined above, the Employer must certify that their Plan Documents have been amended to comply with the Privacy Rule and that they agree to comply. This is typically when the TPA or Service Provider are not under contract to resolve appeals and send detailed medical information to your office for consideration. The Employer must certify to:

- Not to use or further disclose protected health information ("PHI") other than as permitted or required by this Plan Document, or as required by law,
- Ensure that any subcontractors or Business Associates agree to the same restrictions,
- Not use or disclose PHI for employment related actions,
- Report to the GHP any use or disclosure that is inconsistent with this Plan Document or the federal Privacy Rule,
- Make the PHI information accessible to the Participants,
- Allow Participants to amend their PHI,
- Provide an accounting of its disclosures of PHI as required by the Privacy Rule,

- Make its practices available to the Secretary for determining compliance,
- Return and destroy all PHI when no longer needed, if feasible, and
- Establish adequate firewalls.

9.4 Disclosures to Federal Regulators. The Employer is required to make disclosures at the request of the Secretary of Health and Human Services, or its designee, for purposes of enforcement of the Privacy Rule. These disclosures are made without Participant authorization.

9.5 Disclosures Pursuant to an Authorization. PHI may be disclosed by Participant authorization to the Participant or as directed by the Participant. Any issue related to a disclosure and the well-being of the Participant, or another person named in the PHI, should be brought to the Privacy Officer prior to making the disclosure. All uses and disclosures made pursuant to a signed authorization must be consistent with the terms and conditions of the authorization.

An Authorization is a separate form, have a note that it can be revoked at any time, identify the person who is the subject of the PHI, identify the person(s) that can receive the PHI, the purpose of the request, have an expiration date, and a statement that the GHP will not condition claims payment on the signing of the authorization.

10.0 UNAUTHORIZED DISCLOSURE INCIDENT RESPONSE POLICY (NON BREACH)

10.1 Scope And Purpose

This Unauthorized Disclosure Incident Response Policy describes actions taken regarding an unauthorized disclosure of PHI, a disclosure that does not otherwise comply with the Disclosure Section of this Policy provided above, either by an Employee of the Employer or Business Associate. Participant, Media and HHS notices not required unless it is determined that the disclosure constitutes a Breach as determined below.

10.2 Reporting To Privacy Officer

All such unauthorized disclosures will be reported as soon as reasonably possible to the Privacy Officer. Each Employee reporting an unauthorized disclosure will also report the event to their Director/Manager.

10.2 Mitigation

The Privacy Officer will mitigate, to the extent possible, any harmful effects for an unauthorized disclosure. The Privacy Officer will inquire that the unauthorized recipient of the PHI confirms that they have immediately destroyed the data without further disclosure. Email or other confirmation will be retained as part of the Incident Documentation. Mitigation may include additional options as determined by the Privacy Officer such as ID Theft monitoring services.

11.0 BREACH DETERMINATION

A “Breach” under the HITECH Act is an unauthorized transmission of unsecure PHI. The Privacy Officer will review the facts and circumstances to make the Breach determination. This will include a two step analysis as described below:

11.1 Step One:

Determine whether the three exclusions below apply. The following unauthorized disclosures are *not* a Breach:

- Any unintentional acquisition, access, or use of PHI, if it was made in good faith and within the scope of authority and does not result in further use or disclosure.
- Any inadvertent disclosure to a person authorized to access PHI at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed
- A disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

11.2 Step Two:

If an unauthorized disclosure does not fit one of the exclusions above, then the unauthorized disclosure is presumed to be a Breach unless it can be demonstrated that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

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

12.0 BREACH NOTICES

12.1 When the Privacy Officer determines that an unauthorized disclosure of PHI is a Breach then notices have to be sent to the Participants whose PHI was compromised. The Notice will include the facts related to the disclosure, mitigation that has been completed.

12.2 Non-Breach Notices.

When the Privacy Officer determines that the unauthorized disclosure is not a Breach there is no notice sent to the Participants.

12.3 Breach Notices. When the Privacy Officer determines that the unauthorized disclosure is a Breach, a notice will be provided to the Participants without undue delay and in no case longer than 60 days. A Breach shall be treated as discovered as of the first day on which such Breach is known, or, by exercising reasonable diligence would have been known. Knowledge of a Breach exists when the Breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the Breach, who is a workforce member or agent.

The Privacy Officer will communicate the facts and circumstances that caused the Breach, the mitigation effort and response, the number of participants that were affected and the data that was disclosed. The notice will include:

- Description Event
- Date of Event (if known)
- Date of the Discovery
- Number of individuals affected
- The types of unsecured PHI that were involved (such as the name, Social Security Number, date of birth, home address, account number or disability code of the affected individuals)
- Description of the steps Business Associate has taking to investigate, mitigate losses related to and protect against any further disclosures or Breaches
- Contact information for affected individuals to ask questions or learn additional information: Name and Title, Address, E-mail address, Telephone Number

12.4 Documentation.

The Privacy Officer will maintain a file of each unauthorized disclosure that is made that is not in compliance with this Privacy Policy as soon as the there is an awareness of the disclosure. The record will contain a description of the PHI disclosed, to whom it was disclosed, when the Participant was notified of the disclosure, an explanation of any action taken to mitigate the damages that the disclosure created, and a description of any action that was taken regarding the error.

12.5 Notice to the Media and Federal Regulators

Notice is required to be provided to prominent media outlets serving a state or jurisdiction following the discovery of a Breach if unsecured PHI of more than 500 residents of such state or jurisdiction is, or is reasonably believed to have been, accessed, acquired, or disclosed during such Breach.

For Breaches involving 500 or more individuals, notice will be sent to the Department of Health and Human Services (HHS) on line concurrently with the notification sent to Participant. For Breaches involving fewer than 500 individuals, covered entities are required to submit information annually to HHS for Breaches occurring during the preceding year. Submission of this information is required no later than 60 days after the end of the calendar year in which the Breach is discovered (not in which the Breach occurred). The internal log or other documentation is maintained for 7 years.

All Breaches effecting under 500 persons are documented and submitted annually to HHS. Submission of this information is required no later than 60 days after the end of the calendar year in which the Breach is discovered (not in which the Breach occurred). The annual report can be submitted electronically, instructions are available at the following address:

http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html

13.0 SECURITY INCIDENT RESPONSE PLAN AND PROCEDURES

This Incident Response Procedure is in place to ensure incidents related to the areas and systems that maintain PHI are detected, responded to appropriately and action is taken to prevent future incidents.

Some examples of security incidents that an employee might recognize in their day to day activities include, but are not limited to:

- Theft, damage, or unauthorized access (e.g., unauthorized logins, papers missing from their desk, broken locks, missing log files, alert from a security guard, video evidence of a break-in or unscheduled/unauthorized physical entry)
- Fraud – Inaccurate information within databases, logs, files or paper records
- Abnormal system behavior (e.g., unscheduled system reboot, unexpected messages, abnormal errors in system log files or on terminals)
- Security event notifications (e.g., file integrity alerts, intrusion detection alarms, and physical security alarms)

All employees, regardless of job responsibilities, should be aware of the potential incident identifiers and who to notify in these situations. In all cases, every employee should report incidents per the instructions under Incident Reporting, unless they are assigned other activities within the incident response plan.

14.0 HARD COPY STORAGE REQUIREMENTS

Hard copy materials containing PHI (e.g., paper receipts, paper reports, faxes, etc.) are subject to the following storage guidelines:

- At no time are printed reports containing PHI to be removed from the secure office environment.
- All hardcopy material containing PHI should be clearly labeled as such.
- All hardcopy media which contains PHI must be stored in a secure and locked container (e.g. locker, cabinet, desk, storage bin). PHI is never to be stored in unlocked or unsecured containers or open workspaces.
- All PHI, when no longer needed for legal, regulatory or business requirements must be disposed of in hardcopy shred bins. All hardcopy shred bins must remain locked at all times (until shredding.

15.0 WORKSTATION PROTECTION

When an Employee who has access to PHI at their work station leaves the work station, for any duration of time, the Employee is responsible for removing all PHI from their desk and placing it in a locked secure area. Should a user forget to do one of the above aforementioned; the workstation is set up to automatically hibernate, turn off hard drives and require a password upon return.

Passwords are changed every 90 days. This password is comprised of 8 alpha-numeric characters, both upper and lower case letters, and numbers. If an employee believes their password has been compromised, they must immediately report to the Privacy Officer to have a new password generated.

Absolutely no PHI can be left at a work station or in an open area after closing. Each Employee will apply this policy as if the office was completely closed at the end of the shift. At the close of business each day, all employees are required to lock all PHI in assigned cabinets. Group printers must be checked before a Participant leaves for the day to ensure no PHI remains at the printing station. All mailboxes must also be

checked each evening before leaving. All storage, file cabinets and doors are to be locked at all times, unless in direct use. Workstations are restricted from any unauthorized use by visitors. Workstations that could be accessible by office visitors must have privacy filters on all monitors and be locked at all times when not in use.

16.0 LAPTOP USE AND SECURITY

Employees are not permitted to have PHI on their Laptops unless it is for a limited purpose and is coordinated by the Privacy Officer. After the limited purpose has been completed the PHI should be deleted from the Laptop, to the extent possible. Laptops that contain PHI are to be password protected, locked when out of the office or at a location where a third party may gain access including their home, or any offsite location. In the event a laptop containing PHI is lost or stolen, the employee must immediately notify the Privacy Officer who will perform a risk assessment.

Passwords are changed every 90 days. This password is comprised of 8 alpha-numeric characters, both upper and lower case letters, and numbers. If an employee believes their password has been compromised, they must immediately report to the Privacy Officer to have a new password generated.

17.0 ELECTRONIC DATA RETENTION AND STORAGE REQUIREMENTS – WRITABLE MEDIA

Minimal PHI can be stored in an electronic manner. This is limited to the Enrollment Data defined above as a Designated Record Set. No medical documentation received for GHP Administration should be stored electronically, example medical claims for an appeal sent to the Privacy Officer by a Business Associate who is not contracted to make final appeal determinations.

Electronic media containing PHI (e.g., CD, DVD, floppy disk, hard disk, tape, etc.) are subject to the Security Rule. At no time is electronic PHI to be removed from the secure office environment with the exception of computer system backups or as allowed under this Policy. PHI will be physically retained, stored or archived only within secure office environment, and only for the minimum time deemed necessary for their use. Any download of PHI that includes the employees Social Security Number has to be completed with the knowledge of the Privacy Officer for the purpose of GHP administration. Any violation of this Policy can be subject to discipline, including termination of employment depending on the purpose of the files.

18.0 PHI DESTRUCTION REQUIREMENTS

All PHI no longer needed for GHP Administration must be destroyed. TASC recommends retaining copies of the PHI obtained for 7 years in a secure environment.

Before any electronic device that received, transmitted or stored PHI can be sent to a vendor for trade-in, servicing or disposal, all ‘PHI will be destroyed or removed and rendered unrecoverable. Removable computer storage media such as floppy, optical disks or magnetic tapes may not be donated to charity or otherwise recycled.

Physical copies of PHI must be destroyed, shredding is the typical course. Outsourced destruction of PHI may be by a bonded Disposal Vendor that provides a “Certificate of Destruction”. Other documented approaches can be used if they show the physical destruction of the data.

19.0 ACCESS MANAGEMENT AND CONTROL POLICY

Access to PHI is limited to Employees who have completed HIPAA Privacy training. It is the purpose of this policy to identify access points and address appropriate usage of PHI. This Policy addresses physical access for Employees, vendors and visitors. This Policy also covers appropriate usage/access to external media. By restricting access the likelihood of a HIPAA Breach by malicious or non-malicious acts is reduced.

An Employee's access to PHI shall be determined by the Privacy Officer and authorized according to business needs. User access to computer resources shall be provided only when necessary to perform tasks related to business.

20.0 FIREWALL

The Employer has established appropriate administrative, technical, and physical safeguards to prevent PHI from intentionally or unintentionally being used or disclosed in violation of HIPAA's requirements. The Firewalls ensure only authorized Employees have access to PHI. The Firewall separates the PHI so that it is not used for any purpose other than GHP administration and access is only for the minimum necessary for the GHP function(s) performed. By following the secure process outlined in this Policy the PHI received will not be shared with any Employee who is not trained on HIPAA who has a GHP purpose for access.

The Employer prohibits the use of PHI for any employment related purpose such as, but not limited to unemployment hearings, promotions, or any evaluation for benefits under another employer sponsored plan such as disability coverage.

Only Employees who are trained on this Policy and have a business purpose related to a GHP function can have access to PHI, and only the data that is necessary to complete that function.

21.0 VISITORS

Physical access to any area where PHI, electronic or otherwise, is maintained will be under strict supervision. Visitors must be accompanied by an Employee while in the area where PHI is maintained. Employees who accompany Visitors must be sure that the areas that they visit are void of PHI. Prior announcements to areas that typically deal with PHI may be needed to ensure that PHI is not exposed to Visitors.

22.0 Automatic Amendments

Any term or item in this Privacy Policy will automatically be amended to comply with changes in the federal laws and regulations. This Privacy Policy will be updated once yearly with the goal of bringing it back into compliance.