POLICY: Senior Resources will defer to the Standards for Privacy of Individually Identifiable Health Information-Common Definitions; Final Rule, 45 CFR Part 164.501 for definition of terms necessary for definition to protect the confidentiality and integrity of confidential, protected information as required by law.

PROCEDURE: All personnel of Senior Resources will familiarize themselves with or refer to the Standards for Privacy of Individually Identifiable Health Information-Common Definitions; Final Rule, 45 CFR Part 164.501 – Definitions: Pages 82803 through 82805 of the Federal Register, Vol. 65, No. 250 published December 28, 2000, for the purpose of defining the meaning of common terms necessary to ensure compliance of Senior Resources Privacy Policies and Procedures.

Senior Resources will have readily available on its premises and accessible to all staff, an updated copy updated copies of the Standards for Privacy of Individually Identifiable Health Information; Final Rule and Final Modifications. The copy will be kept available by the HIPAA Privacy Compliance Officer/Compliance Advocate.

REFERENCES:
45 CFR 164.501 http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl
Attachment A
HIPAA §164.501 Definitions.

**Correctional institution:**

Means any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center operated by, or under contract to, the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody.

**Other persons held in lawful custody:**

Includes juvenile offenders adjudicated delinquent, aliens detained awaiting deportation, persons committed to mental institutions through the criminal justice system, witnesses, or others awaiting charges or trial.

**Data aggregation:**

Means, with respect to protected health information created or received by a business associate in its capacity as the business associate of a covered entity, the combining of such protected health information by the business associate with the protected health information received by the business associate in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities.

**Designated record set:**

Means:

(1) A group of records maintained by or for a covered entity that is:

   (i) The medical records and billing records about individuals maintained by or for a covered health care provider;

   (ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or

   (iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals.

(2) For purposes of this paragraph, the term record means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.

**Direct treatment relationship:**

Means a treatment relationship between an individual and a health care provider that is not an indirect treatment relationship.

**Health care operations:**

Means any of the following activities of the covered entity to the extent that the activities are related to covered functions:
(1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined in 42 CFR 3.20); population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;

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

(3) Except as prohibited under §164.502(a)(5)(i), underwriting, enrollment, premium rating, and other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of §164.514 are met, if applicable;

(4) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

(5) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and

(6) Business management and general administrative activities of the entity, including, but not limited to:

   (i) Management activities relating to implementation of and compliance with the requirements of this subchapter;

   (ii) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer.

   (iii) Resolution of internal grievances;

   (iv) The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and

   (v) Consistent with the applicable requirements of §164.514, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity.

**Health oversight agency:**

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

Means a relationship between an individual and a health care provider in which:

(1) The health care provider delivers health care to the individual based on the orders of another health care provider; and

(2) The health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services or products or reports to the individual.

**Inmate:**

Means a person incarcerated in or otherwise confined to a correctional institution.

**Marketing:**

(1) Except as provided in paragraph (2) of this definition, marketing means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.

(2) Marketing does not include a communication made:

   (i) To provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, only if any financial remuneration received by the covered entity in exchange for making the communication is reasonably related to the covered entity’s cost of making the communication.

   (ii) For the following treatment and health care operations purposes, except where the covered entity receives financial remuneration in exchange for making the communication:

      (A) For treatment of an individual by a health care provider, including case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual;

      (B) To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; or

      (C) For case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment.

(3) Financial remuneration means direct or indirect payment from or on behalf of a third party whose product or service is being described. Direct or indirect payment does not include any payment for treatment of an individual.

**Payment:**

Means:
(1) The activities undertaken by:

(i) Except as prohibited under §164.502(a)(5)(i), a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or

(ii) A health care provider or health plan to obtain or provide reimbursement for the provision of health care; and

(2) The activities in paragraph (1) of this definition relate to the individual to whom health care is provided and include, but are not limited to:

(i) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;

(ii) Risk adjusting amounts due based on enrollee health status and demographic characteristics;

(iii) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;

(iv) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;

(v) Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and

(vi) Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement:

(A) Name and address;

(B) Date of birth;

(C) Social security number;

(D) Payment history;

(E) Account number; and

(F) Name and address of the health care provider and/or health plan.

**Psychotherapy notes:**

Means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. Psychotherapy notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: Diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

**Public health authority:**
Means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

**Research:**

Means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

**Treatment:**

Means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.
POLICY: Senior Resources will fulfill its obligation and implement policies and procedures with respect to Protected Health Information (PHI) as stipulated in the Health Insurance Portability and Accountability Act (HIPAA), as specified in section 164.530(i)(1) that are designed to comply with the standards, implementation specifications, or other requirements of this subpart.

PROCEDURE: The required policies and procedures will be developed and implemented by Senior Resources to assure appropriate safeguarding of PHI in its operations and will make available to individuals a Notice of Privacy Practices.

Senior Resources will change its policies and procedures as necessary and appropriate to conform to changes in law or regulations. Senior Resources may make changes to policies and procedures at other times as deemed necessary to remain in compliance with applicable law or regulations. Where and when necessary, Senior Resources will make correlative changes in its Notice of Privacy Practices. Senior Resources will not implement a change in a policy or procedure prior to the effective date of the revised policy, procedure or Privacy Notice.

Senior Resources will maintain the required policies and procedures in written and/or electronic form to be accessible to its workforce, and will maintain copies of all communications, actions, activities or designations as are required to be documented hereunder, or otherwise under the HIPAA law or regulations, for a period of six (6) years from the most recent revision date.

ENFORCEMENT: It is the responsibility of the Chief Executive Officer, appointed HIPAA Privacy Compliancy Officer/Compliance Advocate and all managers of Senior Resources to enforce this policy. Any breach of this policy is to be reported immediately to the HIPAA Privacy Compliance Officer/Compliance Advocate and Chief Executive Officer.

REFERENCES:
45 CFR §164.530 (i)(1) http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl
HIPAA Privacy Compliance Officer / Compliance Advocate Policy

Policy: HP.1.3.4
Approved: [Signature], CEO
Effective Date: 3.18.2003
Revised: 3.15.16 Reviewed: 3.15.16

POLICY: Senior Resources will fulfill its obligation as stipulated in the Health Insurance Portability and Accountability Act (HIPAA), as specified in section 164.530(a) and 164.530(d) and appoint a HIPAA Privacy Compliance Officer / Compliance Advocate.

PROCEDURE: The HIPAA Privacy Compliance Officer/Compliance Advocate will oversee all ongoing activities related to the development, implementation, maintenance of, and adherence to Senior Resources policies and procedures covering the privacy of and access to individuals’ private health information (PHI) in compliance with federal and state laws and the healthcare organization’s information privacy practices and will review revised privacy laws as necessary to determine if new policies or modifications are needed.

The HIPAA Privacy Compliance Officer/Compliance Advocate will establish and administer a process for receiving, documenting, tracking, investigating, and taking action on all individual requests for additional information, complaints, accountings of disclosures, or restrictions concerning the individual’s PHI in coordination with Senior Resource’s privacy policies and procedures.

The HIPAA Privacy Compliance Officer/Compliance Advocate will ensure the delivery of initial privacy training and orientation to Senior Resources’ workforce: employees, volunteers, and enrollees. It is the responsibility of the Contracted Services Coordinator to ensure initial privacy and training for business associates. The HIPAA Privacy Compliance Officer/Compliance Advocate will ensure all individuals in Senior Resources’ workforce comply with its privacy practices and oversee the consistent application of sanctions for failures of compliance.

The HIPAA Privacy Compliance Officer/Compliance Advocate will also work closely with the Network Manager to coordinate the development and adherence of policies and procedures to comply with HIPAA Security Rules in compliance with federal and state laws.

ENFORCEMENT: It is the responsibility of the Chief Executive Officer of Senior Resources to enforce this policy. Any breach of this policy is to be reported immediately to the Chief Executive Officer.

REFERENCES:
45 CFR §164.530 (a) [Link]
45 CFR §164.530 (d) [Link]
Job Description
POLICY: An individual has the right to adequate notice of the uses and disclosures that may be made by Senior Resources of their Protected Health Information (PHI), to adequate notice of their rights, and of Senior Resources’ responsibilities with respect to their Protected Health Information (PHI).

Senior Resources is required to provide a Notice of Privacy Practices document to all individuals, as well as other workforce members who request a copy. Senior Resources workforce members, who enroll, assess or register individuals will be responsible for distributing a copy of the notice with explanation to individuals. This policy shall also apply to Senior Resources contractors that perform case management service on behalf of Senior Resources to its clients.

PROCEDURE: Senior Resources workforce members who enroll, assess or register individuals will:

- Distribute, with explanation, to every new individual enrolled a copy of the Senior Resources Notice of Privacy Practices at first face-to-face encounter
- Make a good faith effort to obtain an initial written acknowledgement of the receipt of notice from the individual, and document the receipt or lack of receipt of the acknowledgement in the individual’s record: each individual’s signed acknowledgment will be kept in the individual’s file for a minimum of six years; each unsigned acknowledgment, including signed and dated notations by the caseworker as to their attempt to obtain a signed acknowledgment, will be filed in the individual file and retained for a minimum of six years.
- Make available the notice to individuals at their request by e-mail, if receipt of the notice by the individual is documented. If Senior Resources knows that the e-mail transmission has failed, a paper copy of the notice must be provided to the individual.
- Have the notice available in printed form at the reception desk and posted on the agency web site at http://www.seniorresourceswmi.org
- Make a reasonable attempt, if an individual requests that a Notice of Privacy Practices be translated into a language other than English, to obtain the translation.
- Promptly revise and make notice available whenever there is a material change to the uses or disclosures, the individual’s rights, Senior Resources legal duties, or other privacy practices stated in the notice. Except when required by law, a material change to any term of the notice may not be implemented prior to the effective date of the notice in which such material change is reflected.
- Not automatically provide the notice to individuals whenever the notice is revised, but will make the notice available upon request on or after the effective date of the revision; Senior Resources will post the revised notice on the agency web site.

ENFORCEMENT: The HIPAA Privacy Compliance Officer/Compliance Advocate, program supervisors, and Business Associates providing case management service are responsible for enforcing this policy. All suspected violations are to be reported to the HIPAA Privacy Compliance Officer/Compliance Advocate. Individuals who violate this policy will be subject to the disciplinary process for staff, volunteers, and interns (workforce).

Business Associates subject to this policy who violate the policy will be considered to be in breach of their contract; Senior Resources will take reasonable, documented steps to resolve the breach and to end the practice of violation. In the event the Business Associate cannot or will not remedy the practice or pattern, Senior
Resources will terminate the contract and the Senior Resources Contracted Services Coordinator will report the breach to the U.S. Department of Health and Human Services - Office for Civil Rights, as required by law.

REFERENCES:
45 C.F.R. 164.520(c)  http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl
Mandatory Education And Training For Workforce Policy

<table>
<thead>
<tr>
<th>Policy: HP.1.6</th>
<th>Effective Date: 03/18/2003</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved:</td>
<td>Revised: 3.15.16</td>
</tr>
</tbody>
</table>

**POLICY:** All Senior Resources employees, volunteers, and interns are required to attend and complete all applicable in-service education, training and/or licensing courses upon hire and annually as required by Senior Resources and state and federal law (e.g. Privacy Practices for PHI training and other training based on job classification).

**PROCEDURES:** Human Resources and/or the HIPAA Privacy Compliance Officer/Compliance Advocate are responsible for providing the notification and opportunities to staff to achieve training and education required by this policy and to ensure that the required training is completed and attendance documented.

Documented attendance will be recorded for each individual as to training subject, date and time of participation.

**ENFORCEMENT:** If an individual is unable to sufficiently complete the training requirement, it is the Supervisor’s responsibility to ensure proper guidance is received to fulfill the requirement; guidance efforts should be documented and submitted to Human Resources for filing in the individual’s file.

Individuals who do not complete the training requirement will not be eligible for a salary increase until all applicable and assigned training has been completed.

Individuals who do not complete the training requirement after proper guidance by their Supervisor will be in violation of this policy and will be subject to the appropriate and applicable disciplinary process, up to and including termination.

**REFERENCES:**
45 C.F.R. 164.530(b)(1) [http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl](http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl)
POLICY: Workforce members of Senior Resources who fail to comply with its Health Insurance Portability and Accountability Act (HIPAA) Privacy, HIPAA Security or American Recovery and Reinvestment Act (ARRA) HITECH policies and procedures will be subject to sanctions. Disciplinary and/or corrective actions will be taken against workforce members who fail to comply with the privacy practices set forth in Senior Resources HIPAA policies and procedures.

PROCEDURE: Workforce Member’s Failure to Comply
Senior Resources will apply the appropriate sanction or disciplinary action against members of its workforce who fail to comply with Senior Resources’ privacy policies and procedures. The severity of the sanction will be determined by the HIPAA Privacy Compliance Officer/Compliance Advocate and/or the Chief Executive Officer in accordance with level of failure to comply (example: deliberate versus incidental or accidental disclosure of PHI).

Incidental or accidental disclosure of another individual’s PHI will be considered to be a minor, unintentional infraction at the discretion of the Compliance Officer and may result in a corrective action and/or written warning which will describe the infraction, steps to be taken to prevent re-occurrence, resources available to meet goal of no further occurrence and a follow-up review (within 45 days) by the member’s supervisor or the Chief Executive Officer.

Deliberate disclosure of another individual’s PHI will be considered to be a major, intentional infraction of the Personnel and Privacy policies and could result in immediate termination of the workforce member. All unauthorized disclosures of another individual’s PHI, whether incidental, accidental or deliberate will be considered to be a reportable incident; workforce member must immediately, upon discovery, report the disclosure to the HIPAA Privacy Compliance Officer/Compliance Advocate for investigation. Failure to report a known incident will result in immediate termination of employment, volunteer or contractual arrangement.

ENFORCEMENT: It is the responsibility of all members of Senior Resources’ workforce to report suspected violations of Senior Resources HIPAA Privacy policies and procedure to the HIPAA Privacy Compliance Officer/Compliance Advocate.

It is the responsibility of the HIPAA Privacy Compliance Officer/Compliance Advocate and Security Officers to confidentially investigate all reported violations, documenting the alleged violation, alleged members involved and persons interviewed during the investigation. Once an investigation is concluded, a written report will be given to the Chief Executive Officer and appropriate supervisor. Individuals who are found to have violated the policies and procedures will be subject to disciplinary action by the workforce member’s supervisor and/or the Chief Executive Officer.

REFERENCES:
45 C.F.R. §164.530(e)(g)(j)
http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl
45 C.F.R. §142.308 (a) (10) (iv)
http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl
HIPAA Policy HP.11 Confidentiality, Security and Storage of Protected Health Information Policy and Procedure
POLICY: Senior Resources has a duty to ensure the proper use and/or disclosure of PHI. To the extent practicable, Senior Resources will mitigate (i.e. lessen or alleviate) any harmful effect that becomes known to Senior Resources as a result of a use or disclosure of PHI in violation of Senior Resources’ policies and procedures or applicable law.

PROCEDURE: The actions Senior Resources may undertake to mitigate any harmful effects include, but are not limited to, the following:

- Taking operational and procedural corrective measures to remedy violations;
- Addressing and investigating workforce violations;
- Taking employment actions to re-train, reprimand or discipline workforce members as necessary, up to and including termination; and
- Addressing problems with Business Associates once Senior Resources is aware of a breach of privacy, up to and including contract termination.

The involved parties will document all corrective actions or steps taken.

ENFORCEMENT: It is the responsibility of all members of Senior Resources workforce to enforce this policy. Suspected violations should be reported immediately to the HIPAA Privacy Officer/Compliance Advocate. Individuals who violate this policy will be subject to disciplinary action by their supervisor or the Chief Executive Officer.

REFERENCES:

45 C.F.R. §164.530 (f)

http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl
POLICY: Senior Resources workforce members and clients shall be allowed to freely discuss and raise questions to Supervisors, the Chief Executive Officer or appropriate personnel about situations they feel may be in violation of federal or state law, Senior Resources policy and/or accreditation and regulatory requirements without fear of intimidation or retaliation.

PROCEDURE: Senior Resources shall not intimidate, threaten, coerce, discriminate against, or take any retaliatory action against the following individuals or in the following situations:

1) Any client, legally appointed personal representative, employee, enrollee, or volunteer that in good faith:
   a. Discloses or threatens to disclose information about a situation they feel is inappropriate, or potentially illegal;
   b. Provides information to or testifies against the alleged offending individual or Senior Resources;
   c. Objects to or refuses to participate in an activity they feel is in violation of federal or state law, Senior Resources policy or accreditation requirements;
   d. Is involved in any compliance review or peer review process.

2) Any individual who files a valid or legitimate report of violation, a complaint or an incident report.

The HIPAA Privacy Compliance Officer/ Compliance Advocate will review any allegation of retaliation, intimidation or coercion and if appropriate and necessary, enlist the assistance of the Chief Executive Officer and management staff. Complaints against the HIPAA Privacy Officer/ Compliance Advocate should be addressed to the Chief Executive Officer.

ENFORCEMENT: It is the responsibility of all members of Senior Resources workforce to enforce this policy. Suspected violations should be reported immediately to the HIPAA Privacy Compliance Officer/ Compliance Advocate. Individuals who violate this policy will be subject to disciplinary action by their Supervisor or the Chief Executive Officer.

REFERENCES:
45 C.F.R. §164.530 (g)
http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl
HR1.11 Employee Whistleblower Policy
POLICY: Senior Resources has a duty to protect the rights of individuals to file a complaint for which it collects and/or maintains Protected Health Information (PHI).

PROCEDURE: Senior Resources shall not require individuals to waive their rights under the Privacy Rule as a condition or provision:
- For eligibility or enrollment in a health care plan or service program;
- For delivery of services;
- For treatment;
- Of payment or reimbursement collection.

ENFORCEMENT: It is the responsibility of all members of Senior Resources workforce to enforce this policy. Suspected violations should be reported immediately to the HIPAA Privacy Officer/Compliance Advocate. Individuals who violate this policy will be subject to disciplinary action by their Supervisor or the Chief Executive Officer.

REFERENCES:
45 C.F.R. §164.530 (h)
http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl
PURPOSE: The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a multifaceted piece of legislation. The administrative simplification component covers privacy and security and requires healthcare organizations to protect individuals’ privacy and the confidentiality of protected health information. Privacy and confidentiality are no longer just an ethical obligation of health care, it is the law. Senior Resources is committed to protecting the privacy and integrity of confidential protected health information (PHI) of individuals as required by law, professional ethics, and the State of Michigan Department of Health & Human Services (MDHHS) requirements. Storage of PHI shall be done in a manner that ensures that the information is secure.

POLICY: Senior Resources will fulfill its obligations as stipulated in the Health Insurance Portability and Accountability Act (HIPAA), as specified in section 164.530(c). Senior Resources must have in place appropriate administrative, technical and physical safeguards to reasonably safeguard Private Health Information (PHI) from intentional or unintentional unauthorized use or disclosure.

DEFINITION: Individually identifiable information is any information, including demographic information that identifies an individual. HIPAA’s privacy regulation covers information conveyed on paper or via the spoken word as well as electronically.

PROCEDURE: All workforce members must strictly observe the following standards relating to the storage of PHI in order to assure that health information will be kept confidential:

- During business hours, PHI will be available only to staff/volunteers who are actively involved with that program or service, their supervisors, or staff that needs access for business purposes such as billing, data entry, or quality assurance. Information may be used and disclosed as outlined in the Notice of Privacy Practices. Any other use will require consumer authorization unless permitted or required by law.
- PHI will not be left unattended in an area of public access such as reception or break room.
- PHI records must always be protected from unauthorized access and must be appropriately secured, under lock and/or only accessible with a passcode or secure login.
- Visitors entering the building will be taken to a private area for any discussion that involves protected health information.
- Workforce members will not discuss protected health information with others who do not have a need-to-know, whether on or off the job.
- Workforce members will avoid discussions about PHI in public areas of the building or when others are present who do not have a need-to-know.
- Workforce members will not discuss one participant with another participant without authorization.
- PHI will be shredded when discarded. PHI will not be left in a wastebasket where it may be accessed by someone else.
- PHI, when removed from the building, will remain in the possession of the workforce member. If kept with the workforce member overnight, the information will be kept in a locked storage area when not in use.
- Staff will use passwords or other authentication technologies to protect information from unauthorized users. When leaving a computer, staff will exit any program that would identify participants. Staff will not share their passwords.
• If PHI records are to be stored on the hard disk drive, networked drive, or other internal components of a personal computer or other electronic device, its access must be protected by encryption and accessible only with a passcode. When not in use, this media must be secured from unauthorized access.
• If PHI is stored on removable data storage media, it must be appropriately secured under lock, encrypted and/or only accessible with a passcode or secure login.
• All faxes will be remitted with a cover sheet containing an approved confidentiality clause.
• PHI is not to be sent in an e-mail unless it is encrypted. Workforce members will double check e-mail addresses before sending a message.
• Printed e-mails will be filed or shredded.

OVERSIGHT: The Network Manager will administer, monitor and grant the appropriate passcodes, software to blank unattended computer monitor screens, and rights assignment according to access level granted each workforce member. The Network Manager will maintain appropriate secured logs and records of the same. All violations the Network Manager becomes aware of will be reported immediately to the HIPAA Privacy Compliance Officer/Compliance Advocate and the appropriate supervisor or manager.

ENFORCEMENT: All supervisors and managers are responsible for enforcing this policy. All suspected incidents or violations are to be reported to the HIPAA Privacy Compliance Officer/Compliance Advocate. Individuals who violate this policy will be subject to the appropriate and applicable disciplinary process, up to and including termination.

REFERENCES:
45 C.F.R. 164.530 (c)
http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl
HP.1.7 Workforce Sanctions Policy and Procedure
DEFINITION: A Business Associate is a person or entity that provides activities or services for a covered entity (in this case, Senior Resources) involving the use and/or disclosures of individuals’ Private Health Information (PHI). Business Associates include, but are not limited to, contractors, health care providers or persons with whom Senior Resources has contracted for, arranged for or purchased services for its participants. A Business Associate is not a Senior Resources employee.

POLICY: Senior Resources protects the confidentiality and integrity of confidential personal information of its participants as required by the Health Insurance Portability and Accountability (HIPAA) act, Health Information Technology for Economic and Clinical Health Act (HITECH), professional ethics, Michigan Department of Health and Human Services, and Aging and Adult Services Agency service delivery standards.

HITECH requires that notification of breaches of unsecured PHI discovered by Senior Resources as well as those discovered by its Business Associates be made to the affected individuals, be reported to the U.S. Department of Health and Human Services - Office for Civil Rights (OCR), and reported to the media (if more than 500 individuals are affected).

Senior Resources and its Business Associates are required to act if one or both become aware of an act, practice or pattern that could potentially constitute a breach of client PHI. Senior Resources and its Business Associates must also put into place procedures to report breaches if they occur, notify individuals if a breach involves their PHI, and must report the breach to the OCR.

STANDARDS: Senior Resources will enter into agreements with Business Associates that contain specific language that provides that the Business Associate will:
- Not use or further disclose PHI other than as permitted or required by the contract or as required by law;
- Use appropriate safeguards to prevent use or disclosure of the PHI other than as provided by its contract;
- Report immediately upon discovery to Senior Resources Privacy Compliance Officer any use or disclosure of the PHI of which it becomes aware that is not provided for by permission or through authorized release of which may constitute a breach or violation of PHI, whether intentional or not;
- If it discovers a breach of PHI may have or did occur, cooperate fully with Senior Resources Privacy Compliance Officer to take steps to notify individuals, determine remediation and correction action, and agree to report the breach to the OCR;
- Ensure that any staff or agents, including a subcontractor, to whom it provides PHI received from, created by or on behalf of Senior Resources, agree to the same restrictions and conditions that apply to the Business Associate with respect to such PHI;
- Make available PHI in accordance with the Standards for the Privacy Rule 45 CFR, Parts 160 and 164 and HITECH Title XIII regarding Patient Access to PHI;
- Make available PHI for amendment and incorporate any amendments to PHI in accordance with the Standards for the Privacy Rule 45 CFR, Parts 160 and 164 regarding Patient’s Right to Amend or Correct PHI;
- Make available the information required to provide an accounting of disclosures in accordance with the Standards for the Privacy Rule 45 CFR, Parts 160 and 164 regarding Accounting of PHI Disclosures;
• Make its internal practices, books, and records relating to the use and disclosure of PHI received from, created by or on behalf of Senior Resources available to the Office for Civil Rights for the purpose of determining Senior Resources compliance;
• At termination of the contract, if feasible, return or destroy all PHI received from, created by or on behalf of Senior Resources that the Business Associate still maintains in any form and retain no copies of such information. If such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

In the event Senior Resources becomes aware of a pattern or practice of the Business Associate that constitutes a PHI breach or violation of the Business Associate’s obligations under its contract, Senior Resources must take reasonable steps to remediate the breach or to end the violation, as applicable.

In the event the Business Associate cannot or will not remedy the practice or pattern, Senior Resources must terminate the contract if feasible.

**PROCEDURES:** It is the responsibility of all members of Senior Resources workforce and its Business Associates to report suspected violations of Senior Resources HIPAA Privacy policies and PHI breaches to Senior Resources Privacy Compliance Officer.

It is the responsibility of the Privacy Compliance Officer to confidentially investigate all reported violations, documenting the alleged violation, alleged members involved and persons interviewed during the investigation. Once an investigation is concluded, a written report will be given to the involved Business Associate, the HIPAA Privacy Compliance Officer/Compliance Advocate and the affected program’s Director. If deemed necessary, the Chief Executive Officer, Department of Health & Human Services, and Adult & Aging Services Agency will be notified. Senior Resources Privacy Officer will report the Business Associate to the OCR as required by law.

**ENFORCEMENT:** Business Associates who are found to have violated the policies and procedures will be subject to disciplinary action which may result in termination of contractual agreements.

**REFERENCES:**
45 C.F.R. §160.103
http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl
45 C.F.R. §164.502(e)(1)
http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl
45 C.F.R. §164.503
http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl
ARRA Title XIII Section 13402 – Notification in the Case of Breach
POLICY: Senior Resources workforce may use and disclose PHI for Treatment, Payment, or Healthcare Operations (TPO) providing the individual has been provided Senior Resources’ Notice of Privacy Practices. It shall be the policy of Senior Resources to obtain an individual’s signed authorization for all uses and disclosures of an individual’s PHI.

This policy shall also apply to Senior Resources and its Business Associates. The Business Associates are limited to those disclosures permitted in agreement with Senior Resources.

PROCEDURE: The Notice of Privacy Practices removes the requirement to obtain a consent form for the use and disclosure of confidential individual information for treatment, payment, and health care operations. However, Senior Resources shall attempt to obtain an individual’s signed authorization consent even if disclosure is exempt as specified in 45 CFR §164.502 which allows the disclosure of information without an authorization in the instances discussed below:

1) Senior Resources may use or disclose confidential information to the extent that law requires such use or disclosure and the use or disclosure complies with and is limited to the relevant requirements of such law, e.g., the reporting of communicable diseases to the local public health department. The rule specifically allows:
   - uses and disclosures for public health activities;
   - reporting about victims of abuse, neglect or domestic violence;
   - disclosures for health oversight activities;
   - disclosures for judicial and administrative proceedings;
   - disclosures for law enforcement purposes;
   - uses and disclosures about decedents;
   - uses and disclosures to coroners, medical examiners, or funeral directors after an individual expires;
   - uses and disclosures for cadaver organ, eye or tissue donation purposes;
   - disclosures to avert a serious threat to health or safety such as in Disaster Relief efforts;
   - uses and disclosures for specialized government function such as Armed Forces, Red Cross, lawful intelligence or national security activity;
   - uses and disclosures to U.S. Department of Health and Human Services - Office for Civil Rights (OCR) to determine Senior Resources compliance with HIPAA Privacy Standards.

2) Senior Resources is permitted to disclose to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, the confidential information directly relevant to such person’s involvement with the individual’s care or payment related to the individual’s health care, unless that individual has requested that such disclosure not occur.

3) Senior Resources is permitted to use and disclose PHI to notify or to assist in the notification of a family member, a personal representative or another person responsible for the care of the individual of the individual’s location, general condition or death. Senior Resources can also use and disclose PHI for these circumstances for identifying or locating the types of persons above. In order for Senior Resources to use or disclose PHI for these purposes, the individual’s presence and oral agreement to use and disclosure should be obtained.
4) If the individual is not present for, or the opportunity to agree or object to the use or disclosure is not practical due to the individual’s incapacity, or in an emergency circumstance, then Senior Resources may, in the exercise of professional judgment, determine whether the disclosure is in the best interest of the individual and, if so, disclose only the confidential information that is directly relevant to the person’s involvement with the individual’s health care.

**PROCEDURE:** All use and disclosure without authorization must be reported to the HIPAA Privacy Compliance Officer/Compliance Advocate or a member of Management in the absence of the HIPAA Privacy Compliance Officer/Compliance Advocate.

**ENFORCEMENT:** The HIPAA Privacy Compliance Officer/Compliance Advocate and program supervisors are responsible for enforcing this policy. Individuals who violate this policy will be subject to the disciplinary process for workforce members.

**REFERENCES:**
45 CFR §164.512 [http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl](http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl)
HIPAA Policy HP.3.2 Authorization for Use and Disclosure of PHI Policy and Procedure
Authorization for Use and Disclosure of Protected Health Information (PHI) Policy and Procedure

Policy: HP.3.2
Approved: [Signature] CEO
Effective Date: 04.01.03
Revised: 10.6.15

POLICY: Senior Resources will fulfill its obligation and implement policies and procedures with respect to Protected Health Information (PHI) as stipulated in the Health Insurance Portability and Accountability Act (HIPAA)-Privacy Rule, as specified in section 45 CFR 164.508. All use and disclosures require a signed authorization.

This policy shall also apply to Senior Resources and its Business Associates. Business Associates are limited to those disclosures permitted in agreement with Senior Resources.

STANDARDS: Senior Resources shall adopt a standard authorization form for the use and disclosure of an individual’s PHI, which shall be written in plain language, the standard to be in English translation and at a minimum, made available upon request in Spanish translation. Senior Resources must provide a copy of the signed authorization to the individual or personal representative upon request. Prior to any disclosure of PHI, an agent of Senior Resources disclosing PHI must verify the identity of any person requesting it, and authority of any such person to have that access, if the identity or authority of such person is not known to the agent.

PROCEDURE: Each authorization shall include at minimum, and shall be considered invalid if missing any of, the following information:
- Specific and meaningful description of information to be disclosed;
- Specific and meaningful description how the PHI will be used (purpose);
- Name or identification of the person or provider authorized to make the use or disclosure;
- Name or identification of the person or provider to whom the requested use or disclosure may be made;
- An expiration date;
- A statement of the individual’s right to revoke the authorization in writing, and exceptions to the right to revoke, together with a description of how the individual may revoke the authorization;
- A statement that the information may be subject to redisclosure by the recipient and no longer protected, except as required by law;
- A statement that treatment, payment and eligibility for benefits may be effected by the individual’s refusal to sign an authorization;
- A statement that the individual has the right to refuse to sign the authorization;
- The dated signature of the individual; and
- If the authorization is signed by a personal representative of the individual, a description of the representative’s authority to act on behalf of the individual.

Accounting of Disclosures: Pursuant to Senior Resources HIPAA Policy, No. HP.3.1, the office, program or workforce member must document and retain all information about uses and disclosures of PHI for a period of six (6) years as required to be available for an accounting for the same period, including:
- Date of disclosure;
- Name and, if known, address of recipient of PHI;
- Description of PHI disclosed; and
- Statement of purpose and basis for disclosure, or copy of authorization or request for disclosure.

ENFORCEMENT: The HIPAA Privacy Compliance Officer/Compliance Advocate, program supervisors, and Business Associates are responsible for enforcing this policy. All suspected breaches or violations are to be
reported to the HIPAA Privacy Compliance Officer/Compliance Advocate. Individuals who violate this policy will be subject to the disciplinary process for staff, enrollees, volunteers, and interns (workforce).

Business Associates subject to this policy who violate the policy will be considered to be in breach of their contract; Senior Resources will take reasonable, documented steps to cure the breach and to end the practice of violation. In the event the Business Associate cannot or will not remedy the practice or pattern, Senior Resources will terminate the contract and the Senior Resources Contracted Services Coordinator will report the breach to the U.S. Department of Health and Human Services - Office for Civil Rights (OCR), as required by law.

REFERENCES
45 CFR §164.508 [http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl](http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl)
Informed Consent
MI CHOICE WAIVER/TARGETED CARE MANAGEMENT
CONSENT FOR RELEASE OF INFORMATION

Name________________________________ D.O.B._____/____/____ SS#_______ ___ _____
Address__________________________________   __________________   _______
Number   Street               City                                 Zip

The undersigned hereby authorizes the release of the following information for the
person named above to an agent of Senior Resources. Please initial all applicable.

________ All health and medical records, including current and historical records, from
any and all hospitals, physicians and other healthcare agencies.

________ All financially-related information listed below:
• Social Security benefits and SSI. Beneficiary ID______________________________
• Financial institution records for all open accounts.
• Life insurance policy information including policy numbers, copies of policies and
cash surrender value.
• Health insurance policy information including policy numbers, premiums and
verification of benefits.
• Pension and retirement benefits.
• Verification of all end-of-life services including coverage, benefits and copies of
contractual agreements.
• Any assistance applied for or received through the Michigan Department of Health
and Human Services (MDHHS)
• Other:_______________________________________________________________

The undersigned hereby authorizes Senior Resources to release the following
information for the person named above to agencies, physicians and their
representatives, faith-based organizations, Michigan Department of Health and Human
Services (MDHHS) and other service providers. The purpose of this disclosure will be
to acquire, coordinate, request and authorize services. Only the information required to
secure or coordinate services will be released. Please initial all applicable.

________ Medical
________ Financial
________ Other: _________________________________________________________

By signing below, I hereby consent to the releases initialed above. This release of
information is valid for one year from the date of the Individual’s or Individual’s
Representative (where applicable) signature. This authorization may be revoked at any
time by providing written or verbal notice of revocation to any agent or employee of
Senior Resources.

______________________________________________    ______/______/_______
Signature or Representative’s Signature           Date

______________________________________________    ______/______/_______
Witness Signature (if necessary)             Date

______________________________________________    ______/______/_______
Representative of Senior Resources Signature         Date
<table>
<thead>
<tr>
<th>POLICY:</th>
<th>An individual has the right to and may revoke a prior authorization at any time, provided that the revocation request is made in writing or verbal and provided Senior Resources has not already provided PHI based on the individual’s prior authorization. Senior Resources will stop providing PHI based on the individual’s revocation of authorization as soon as possible.</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROCEDURE:</td>
<td>Individuals requesting revocation of a prior authorization should be referred to the Supports Coordinator or in his/her absence, to either the Social Work Supervisor or RN Supervisor or Access Supervisor. The Supports Coordinator or Supervisor will immediately notify all parties involved and the HIPAA Privacy and Compliance Officer/Compliance Advocate that the individual has revoked his/her authorization for the use and disclosure of his/her PHI.</td>
</tr>
<tr>
<td>ENFORCEMENT:</td>
<td>All managers, supervisors, and case workers are responsible for enforcing this policy. Questions regarding interpretation, definition or adherence should be referred to the HIPAA Privacy Compliance Officer/Compliance Advocate.</td>
</tr>
<tr>
<td>REFERENCES:</td>
<td>45 CFR §506 (b) <a href="http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl">http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl</a></td>
</tr>
</tbody>
</table>
Use and Disclosure of Protected Health Information (PHI) Policy and Procedure

Policy: HP.3.4
Approved:  
Effective Date: 04/01/2003
Revised: 10.06.2015

POLICY: Senior Resources workforce may use and disclose PHI for Treatment, Payment, or Healthcare Operations (TPO). However, this only allows Senior Resources and its workforce to use and disclose the “Minimum Necessary” amount of information required to complete the desired task.

DEFINITIONS: Use with respect to individually identifiable health information: The sharing, employment, application, utilization, examination or analysis of such information within an entity that maintains such information.

Disclosure: The release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

Treatment: The provision, coordination, management of health care related services by one or more health care providers, including the coordination or management of health care by a provider with a third party; consultation between health care providers relating to a client or the the referral of a client for health care from one health care provider to another.

Payment: Any activities undertaken either by a health plan or by a health care provider to obtain premiums determination or fulfill its responsibility for coverage and the provision of benefits or to obtain or provide reimbursement for the provision of health care. These activities include, but are not limited to:
1. Determining eligibility and adjudication or subrogation of health benefits claims,
2. Risk adjusting amounts due based on enrollee health status and demographics
3. Billing, claims management, collection activities, obtaining payment under contract for services, and related health care processing
4. Review of health care services with respect to necessity, coverage under a health care plan, appropriateness of care or justification of charges
5. Utilization review activities including pre-certification and preauthorization, concurrent and retrospective review of services
6. Disclosure to consumer reporting agencies of certain PHI relating to collection of reimbursement

Health Care Operations: Any one of the following activities to the extent the activities are related to providing health care:
1. Conducting quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting clients with information about treatment/service alternatives and related functions that do not involve treatment.
2. Reviewing the competence or qualifications of health care professionals, evaluating provider performance, health plan performance, conducting training programs in which providers of health care learn or improve their skills as health care providers, training of non-health professionals, accreditation, certification, licensing or credentialing activities.
3. Conducting or arranging for medical review, legal services, auditing functions, including fraud and abuse detection and compliance programs.
4. Conducting cost management and planning related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or covered policies, and

5. General administrative activities including HIPAA compliance; consumer service; resolution of grievances or complaints; the sale, transfer, merger or consolidation of covered entities with whom service arrangements are made for individuals; creating de-identified data sets; and fundraising for the benefit of Senior Resources.

MINIMUM NECESSARY: When using or disclosing PHI or when requesting PHI from another health care provider or health organization, Senior Resources must limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.

Indirect Treatment Relationship: A relationship between an individual and health care provider in which:
1. The health care provider delivers health care to the individual based on the orders of another health care provider; and
2. The health care provider typically provides services or products or reports the diagnosis or results associated with the health care, directly to another health care provider who provides the services, products or reports to the individual.

Personal Representative and Deceased Individuals
For information regarding proper uses and disclosures for Personal Representative and Deceased Individuals, see Senior Resources HIPAA Policy, Personal Representatives and Deceased Individuals, No. HP.3.5.

PROCEDURES: Acknowledgments
Except in an emergency treatment situation, Senior Resources must make a good faith effort to obtain a written acknowledgment of receipt of the Notice of Privacy Practices provided in accordance with Senior Resources Notice of Privacy Practices Policy, no. HP.1.5. If receipt is not obtained; Senior Resources will document good faith effort to obtain such receipt of acknowledgment and the reason why it was not obtained.

Permitted Uses and Disclosures - Senior Resource may use and disclose PHI for:
1. Its own treatment, payment or healthcare operations.
2. Treatment activities of a health care provider.
3. The payment activities of another covered entity or health care provider.
4. The healthcare operations of another covered entity or health care provider, if each entity has or had a relationship with the individual who is the subject of PHI being requested, and the disclosure is:
   a. for a purpose listed in the definition of health care operations; or,
   b. for the purpose of health care fraud and abuse detection or compliance.

In order for Senior Resources to use and disclose PHI for purposes other than those listed in this policy, see Senior Resources HIPAA Policy, Authorization for the Use and Disclosure of PHI, No. HP.3.2.

ENFORCEMENT: The HIPAA Privacy Compliance Officer/Compliance Advocate, staff supervisors and managers are responsible for enforcing this policy. All suspected breaches or violations are to be reported to the HIPAA Privacy Compliance Officer/Compliance Advocate. Individuals who violate this policy will be subject to the disciplinary process for staff, enrollees, volunteers, and interns (workforce).

REFERENCES:
45 CFR §164.506 http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl
HIPAA Policy HP.1.5 Notice of Privacy Practices for PHI Policy and Procedure
HIPAA Policy HP.3.2 Authorization for Use and Disclosure of PHI Policy and Procedure
HIPAA Policy HP.3.5 Disclosure of PHI to Personal Representatives Policy and Procedure
POLICY: Senior Resources will recognize a Personal Representative as the person to act in the place of the individual receiving treatment or services for acknowledgment of the receipt of the Notice of Privacy Practices and/or authorizations for any other use and disclosures of the represented individual’s PHI.

PROCEDURE: General Rule
As a general rule, incapacitated and deceased individuals must have a personal representative identified in order to provide acknowledgment of Senior Resources’ Notice of Privacy Practices or to sign Authorizations to Use and Disclose PHI.

A Personal Representative shall be recognized as the adult who has been given authority, by law or by willing agreement from the individual represented, who is acting on behalf of that individual. This includes legal guardians or properly appointed agents identified in legal documents such as a Medical Power of Attorney or individuals designated by State law.

Abuse, Neglect or Endangerment Situations
Senior Resources does not have to recognize a personal representative, notwithstanding a state law or enforced requirement to the contrary, if they are suspect in cases of abuse, neglect or endangering the individual they represent. If Senior Resources chooses not to recognize a person as a personal representative, Senior Resources must believe that it is not in the best interest to treat the person as the individual’s personal representative and believes that one of the following conditions exist:
1. The individual has been or may be subjected to domestic violence, abuse, or neglect by a guardian or personal representative; or
2. Treating such a person as the personal representative could endanger the individual.

Deceased Individuals
If under applicable law, an executor, administrator or other person with authority to act on behalf of a deceased individual or the individual’s estate, Senior Resources must recognize such a person as a personal representative under this policy.

Absent an executor, administrator or other court-appointed representative for the deceased individual’s estate, the following individuals listed may authorize the release of PHI in order of priority (an entire category should be exhausted before moving to the next category):
1. Surviving spouse
2. Surviving adult children
3. Surviving parents
4. Surviving adult grandchildren
5. Surviving adult brothers and sisters
6. Surviving grandparents
7. Surviving adult children of brothers and sisters

ENFORCEMENT: All managers and supervisors are responsible for enforcing this policy. Individuals who violate this policy may be subject to disciplinary actions.
REFERENCES:
45 C.F.R. §164.502(f)(g) http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl
POLICY: The use and disclosure of Protected Health Information (PHI) must be limited to the minimum necessary to satisfy the request or to complete the task, unless otherwise specified by the individual.

STANDARDS: Use and Disclosure Limitations
In general, PHI may be used internally by Senior Resources’ workforce for treatment, payment or health care operations. All individuals who handle PHI on behalf of Senior Resources in any manner are expected to know and abide by the following protocols:

1. Determining Workforce Access to PHI - Access to PHI will be granted based on the individual’s role and determined by their supervisor. Senior Resources will document in each individual’s Job Description:
   a) Those individuals in the workforce who need access to PHI to carry out their duties; and
   b) For each individual, the level of PHI to which access is needed and any conditions appropriate to such access.

2. Requests for Uses or Disclosures of PHI - Only the minimum information required to accomplish the purpose of the requestor or to initiate treatment, payment, or health care operations (TPO) from a provider or business associate is to be disclosed. Entire medical record information should never be released to providers or business associates without client authorization.

3. Good Faith Reliance - Individuals may rely on the belief that the PHI requested from Senior Resources is the minimum amount necessary to accomplish the purpose of the request when:
   a) The information is requested by another person previously approved for access
   b) The information is requested by a profession (such as a purchase of service provider or auditor) providing services either as a business associate or other covered entity
   c) Making disclosure to entities or agencies that do not require by law consent, authorization, or opportunity to agree or object

Disclosures for Payment
Only the minimum necessary PHI shall be disclosed for payment functions, as provided through contractual agreements. Persons handling PHI in a payment context shall refrain from publicizing an individual’s diagnosis information. This policy shall apply to checks collected, paper receipts, envelopes and invoices sent to clients.

Disclosures Required by Law
1. Disclosures Ordered by a Court or Administrative Tribunal - The minimum necessary standard does not apply to disclosures ordered from an administrative tribunal or by order of court. Only information directly requested by such an order is to be provided.

2. PHI About a Victim of a Crime or Abuse – The minimum necessary standard shall apply to information released to law enforcement regarding victims of crime or abuse. However, if the law requires information to be released, then the disclosure will be in compliance with the subpoena, statute, or law.

Disclosures for Worker’s Compensation
PHI may be disclosed to comply with Worker’s Compensation laws and regulations without consent, authorization, or opportunity to object by the individual, but such disclosure shall still only be the minimum necessary. Requests for entire records should be scrutinized and approved by the Human Resources director, as appropriate.
Disclosures to Family and Friends
Persons with access to and authority to disclose PHI may only make disclosures to family and friends (of the individual owning the PHI) in accordance with Senior Resources HIPAA Policy, No. HP.3.6.

Minimum Necessary Use and Disclosure to Volunteers, Interns and Trainees
Volunteers, interns and trainees are not exempt from following the rules outlined in this policy. Only those volunteers, interns and trainees who are actively involved in the TPO of the individual, and therefore, not limited in their access of the individual’s PHI, may so access the PHI.

ENFORCEMENT: The HIPAA Privacy Compliance Officer/Compliance Advocate, managers and program supervisors are responsible for enforcing this policy. All suspected breaches or violations are to be reported to the HIPAA Privacy Compliance Officer/Compliance Advocate. Individuals who violate this policy will be subject to the disciplinary process for staff, enrollees, volunteers, and interns (workforce).

REFERENCES:
45 C.F.R. §164.514 [http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl]  
45 C.F.R. §164.512 [http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl]  
45 C.F.R. §164.506 [http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl]
POLICY: Senior Resources has a duty to protect the confidentiality and integrity of PHI as required by law, professional ethics, and accreditation requirements. Whenever possible, de-identified PHI should be used, and when not possible, limited data sets should be created. This policy defines the guidelines and procedures that must be followed for the de-identification of PHI or the creation of limited data sets.

DEFINITION:
De-Identified PHI: De-identified PHI is PHI rendered anonymous when identifying characteristics are completely removed.

PROCEDURE:
PHI must be de-identified prior to disclosure to non-authorized users. De-identification requires the elimination not only of primary or obvious identifiers, such as the individual’s name, address, date of birth (DOB), and case worker, but also of secondary identifiers through which a user would deduce the individual’s identity.

For information to be de-identified, the following identifiers of the individual must be removed:
- Names
- Street Address, other than city, state or zip code
- Telephone or fax numbers
- Names of relatives, contacts, caregivers, case worker and/or employer
- DOB
- Screen date
- Assessment dates
- Client ID number
- Social Security number
- Diagnosis codes
- Medications
- Health beneficiary plan number
- Medicare number
- Medicaid number
- Other account numbers
- License numbers
- Photographs (showing full face)
- Biometric identifiers (finger or voice prints)
- E-mail addresses
- Personal website or URLs or IP addresses
- Any other unique identifying number characteristic or code

Whenever possible, de-identified PHI should be used for quality assurance monitoring and routine utilization reporting. If de-identified PHI cannot be used, a limited data set should be used whenever possible. PHI used for research should be de-identified unless the individual provides authorization.
**Limited Data Sets**
A subset of PHI that excludes the direct identifiers listed above. All direct identifiers must be removed for the individual. Senior Resources may use PHI to create a limited data set or may disclose PHI to a business associate in order to create a limited data set. Business associates may not disclose information in a limited data set without Senior Resources’ approval.

Any questions regarding identifiable data should be referred to the HIPAA Privacy Compliance Officer/Compliance Advocate.

**ENFORCEMENT**: All supervisors and managers are responsible for enforcing this policy. Individuals who violate this policy will be subject to the appropriate and applicable disciplinary process, up to and including termination or dismissal.

**REFERENCES:**
45 C.F.R. §164.502(d) [http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl](http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl)
45 C.F.R. §164.512 (b) [http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl](http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl)
POLICY: Senior Resources will protect the confidentiality and integrity of the protected health information (PHI) of individuals as required by law, professional ethics, and accreditation requirements. It is the policy of Senior Resources that the use and disclosure of PHI for research must have appropriate individual authorizations for the use of identifiable PHI.

PROCEDURE: Individual authorizations should be obtained for all research endeavors.

If obtaining individual authorizations are not possible, de-identified PHI should be used; if PHI cannot be de-identified, then a limited data set must be used.

REFERENCES:
45 C.F.R. §164.512(i). http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl
HIPAA Policy HP.3.7 De-Identified PHI & Limited Data Set Policy
HIPAA Policy HP.3.2 Authorization for Use and Disclosure of PHI
Use and Disclosure for Fundraising and Marketing Policy and Procedure

Policy: HP.3.9
Effective Date: 04.01.03
Approved: , CEO
Revised: 10.6.15

**POLICY:** Senior Resources will protect the confidentiality and integrity of the protected health information (PHI) of individuals as required by law, professional ethics, and accreditation requirements. In general, it is the policy of Senior Resources that the use and disclosure of PHI for fundraising & marketing must have appropriate individual authorizations for the use of identifiable PHI.

**PROCEDURE:** Individual authorizations should be obtained for all fundraising & marketing endeavors which will require PHI if obtaining individual authorizations are not possible, de-identified PHI should be used; if PHI cannot be de-identified, a limited data set must be used.

Examples of information that CANNOT be used without prior authorization include:

- Individual’s name
- Individual’s address
- Individual’s age
- Individual’s gender
- Individual’s program/service status
- Individual’s dates of service
- Birth date
- Telephone numbers
- Fax number
- E-mail address
- Social Security number
- Medical record number
- Health plan information
- Diagnosis
- Nature of treatment
- Hospitalization or other facilities placement dates
- Medications use
- Names of relatives and employers
- Account number
- Certificate/license number
- Any vehicle or other device serial number
- Web URL
- Finger or voice prints
- Photographic images

**REFERENCES:**
45 C.F.R. §164.514(f) [http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl](http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl)
45 C.F.R. §164.508(3)(i) [http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl](http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl)
45 C.F.R. §164.508
[http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl](http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl)
HIPAA Policy HP.3.7 De-Identified PHI & Limited Data Set Policy
PURPOSE: Senior Resources is committed to protecting the privacy and confidentiality of protected health information in regards to its staff and participants.

POLICY: Senior Resources will fulfill its obligation as stipulated in the Health Insurance Portability and Accountability Act (HIPAA), as specified in section 164.530 (d) and investigate any and all complaints made in regards to privacy rights having been violated. Individuals have the right to file a formal complaint if it is believed that privacy rights have been violated. A complaint may be filed with Senior Resources or with the Secretary of the Office for Civil Rights (OCR) at the U.S. Dept. of Health and Human Services. Complaints may be filed without fear of coercion, discrimination, reprisal, or unreasonable interruption of services. Individuals will not be penalized for filing a complaint. Individuals may comment about privacy rights.

PROCEDURES:

- Individuals are encouraged to first discuss the complaint with the HIPAA Privacy Compliance Officer/Compliance Advocate at Senior Resources at (231) 739-5858.
- Complaints must be filed in writing whether on paper or electronically within 180 days of the date the complainant knew about the violation.
- Complaints made to this agency must be written on the Form to File a Privacy Complaint which is available by calling this agency’s HIPAA Privacy Compliance Officer/Compliance Advocate at (231) 739-5858 and requesting the Privacy Complaint form or by accessing the agency’s web site at www.seniorresourceswmi.org.
- A written acknowledgement of receipt of the complaint will be sent to the complainant within 48 hours of receipt of the written complaint.
- The HIPAA Privacy Compliance Officer/Compliance Advocate will investigate the complaint and attempt to resolve the problem, either within the agency or by contacting a provider. All attempts will be made to satisfy the individual’s expectations.
- Case Management Participant complaints regarding privacy violations are to be noted in the participant chart.
- For agency workforce (personnel, enrollees, interns, and volunteers), a copy of the complaint will be maintained in the personnel file.
- All complaints are logged in a centrally located Complaint Log and are referenced as a tool for quality assurance.
- The HIPAA Privacy Compliance Officer/Compliance Advocate shall investigate the complaint as to the violation of protected health information, and within ten (10) working days after the receipt of the written complaint, give his/her decision in writing.
- If it is found that there was no violation of privacy or confidentiality of protected health information, the matter will conclude and the findings will be logged in the central log, the participant chart as appropriate and the complainant will be notified in writing.
- If it is found that there was a violation of privacy and/or confidentiality, appropriate steps will be taken by Senior Resources to correct the situation. The party responsible for the violation or breach of confidentiality will be disciplined, instructed as to the appropriate use of private/confidential health information, and/or may be terminated.
• If the party responsible for a violation of privacy and/or confidentiality of private health information is a business associate, Senior Resources will take reasonable steps to cure the breach or to end the violation, as applicable. In the event the business associate cannot or will not remedy the practice or pattern, Senior Resources will terminate the contract if feasible. Where termination is not feasible, the Senior Resources HIPAA Privacy Compliance Officer/Compliance Advocate will report to the OCR, as required by law.

• The outcomes of all complaints filed will be logged in the centrally located Complaint Log to be referenced as a tool for quality assurance. Outcomes of complaints filed will be charted in an individual’s chart/file as applicable.

• If the complainant is not satisfied with the outcomes following a complaint, a complaint may be made with the OCR.

• The OCR has the authority to audit this agency’s privacy practices for HIPAA compliance and will do so by reviewing the organization’s policies and procedures and interviewing staff.

ENFORCEMENT: The HIPAA Privacy Compliance Officer/Compliance Advocate, staff supervisors and managers are responsible for enforcing this policy. All suspected breaches or violations are to be reported to the HIPAA Privacy Compliance Officer/Compliance Advocate. Individuals who violate this policy will be subject to the disciplinary process for staff, enrollees, volunteers, and interns (workforce).

REFERENCES:
45 CFR 164.530 (d) http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl
Form to File a Privacy Complaint
POLICY: Individuals have a right to request a restriction of the uses and disclosures of their personal Protected Health Information (PHI) maintained by Senior Resources. Participant shall be informed of possible service disruption due to restriction of PHI but does not affect enrollment status.

PROCEDURE: Acceptance of Request for Restriction of PHI
1. Senior Resources must accept all requests from individuals to restrict personal PHI.
2. Senior Resources does not have to agree to the request of the individual for restriction unless the PHI pertains solely to a service for which the individual has paid SR for in its entirety.
3. Senior Resources may not use or disclose PHI in violation of such agreed to restriction unless the individual who requested the restriction is in need of emergency treatment and the restricted PHI is needed to provide emergency treatment. Senior Resources may use the restricted PHI itself or Senior Resources may disclose such restricted PHI to a health care provider to provide such treatment to the individual. If restricted PHI is disclosed to another health care provider for emergency treatment, Senior Resources must request that the health care provider not further use or disclose the PHI.
3. The individual can make the request in writing or verbally to their supports coordinator, or if supports coordinator is unavailable, to the supports coordinator’s direct supervisor to prevent:
   • Uses or disclosures from being made to the individual for inspection or copying of their own PHI;
   • The individual from obtaining an accounting of disclosures of their own PHI;
   • The inclusion in an inter-agency client directory; or
   • Uses or disclosures for which consent, authorization or opportunity to agree or object is not required.

Confidential Communications Requests
Senior Resources must permit individuals to request and accommodate reasonable requests by individuals to receive communications of PHI from Senior Resources by alternative location or means if they so request. For example, if an individual requests Senior Resources to not mail their information to their home, but rather to a post office box, Senior Resources must accommodate that request. Senior Resources cannot require explanations by the client for confidential communications requests.

Termination of Request for Restriction of PHI
Senior Resources may terminate a previously agreed to restriction if:
1. The individual agrees to or requests the termination in writing; or
2. The individual agrees orally to the termination and the oral agreement is documented in writing; or
3. Senior Resources informs the individual that it is terminating the previously agreed to restriction.

ENFORCEMENT: All supervisors, managers, and the HIPAA Privacy Compliance Officer/ Compliance Advocate are responsible for enforcing this policy. Any suspected violation should be reported to the HIPAA Privacy Compliance Officer/ Compliance Advocate or Chief Executive Officer.

REFERENCES:
45 C.F.R. §164.522 http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl
Attachment A: Restriction for Use and Disclosure of PHI Form
In completing this form, you are requesting the following restrictions be considered as limitations to Senior Resources use and disclosure of your PHI. If we grant your request, we are bound by the terms of the agreement. You will be notified in writing of Senior Resources’ decision to accept or deny your restriction request. Until a decision is reached, your request for restriction will not be honored.

Individual’s Name: _________________________________ Date of Request: __________________

(Please print name)

Description of Requested Restrictions (Please be very specific providing details and dates):

______________________________________________________________________________
______________________________________________________________________________
______________________________________________________________________________
______________________________________________________________________________
______________________________________________________________________________
______________________________________________________________________________

Phone number where Individual can be reached:_________________________

Signature:_____________________________________

☐ Signed by Personal Representative

Describe relationship _______________________

For office use only – Route to Compliance Officer:

Date Received:_________________________________________ Individual’s ID #:_____________________

☐ Accepted  ☐ Denied,

Reason:_______________________________________________________________________________________

☐ Case Worker informed of decision and restrictions as applicable  ☐ Individual notified of decision in writing

Compliance Advocate Signature:_________________________________________ Completed:__________________
POLICY: In general, clients and workforce members of Senior Resources shall have the right to request an accounting of their personal Protected Health Information (PHI) disclosures made by Senior Resources.

PROCEDURE: Right to an Accounting of Disclosures

Senior Resources must provide the individual with a written accounting that meets the following requirements:

1. Except as otherwise provided, the accounting must include disclosures of PHI. This includes disclosure to and by business associates for purposes other than Treatment, Payment and/or Healthcare Operations (TPO).

2. The accounting for each disclosure must include:
   a. The date of the disclosure;
   b. The name of the entity or person who received the PHI, and if known, the address of such;
   c. A brief description of the PHI disclosed; and
   d. A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure.

3. Senior Resources must act on the individual’s request for an accounting, no later than 60 days after the receipt of such request, as follows:
   a. Provide the individual with the accounting requested; or
   b. If Senior Resources is unable to provide the accounting within the 60 days, Senior Resources may extend the time to provide the accounting by no more than 30 additional days, provided that:
      1) Senior Resources, within the time limit of 60 days, provides the individual with a written statement of the reasons for the delay; and
      2) Senior Resources may have only one such extension of time for action on a request for an accounting.

4. Senior Resources will provide the first accounting to an individual in any 12-month period at no charge. Senior Resources may impose a reasonable, cost-based fee for each subsequent request for an accounting within the same 12-month period by the same individual. Senior Resources will inform the individual in advance of the estimated cost of the fee and will provide the individual an opportunity to withdraw or modify the request to avoid or reduce the fee. The fee will be set by the number of pages to be copied at a per copy rate to be set by the Chief Financial Officer.

5. If Senior Resources has made multiple disclosures of PHI to the same person or entity for a single purpose, the accounting may with respect to such disclosures provide:
   a. The information required above;
   b. The frequency, periodicity or number of disclosures made during the requested accounting period;
   c. The date of the last such disclosure during the requested accounting period.

6. The HIPAA Privacy Compliance Officer/Compliance Advocate will be responsible for receiving and overseeing the processing of requests for an accounting of disclosures. HIPAA Privacy Compliance Officer/Compliance Advocate will document and maintain a log to record each accounting of disclosures to include:
   a. Date of request;
   b. Individual making request;
   c. The name of the entity or person who received the PHI, and if known, the address of such;
   d. A brief description of the PHI disclosed;
   e. The date of the disclosure;
f. Notation if accounting of disclosures was made prepared within 60 days, brief summary of reason why, and whether or not a notice for 30 days extension to disclose was sent to the requesting individual;
g. The fee charged (if any);
h. Name of personnel who prepared accounting of disclosure.

**Exceptions to Right of Accounting of Disclosures**

The right of an individual to request an accounting of disclosures of PHI must be temporarily suspended if Senior Resources receives a written statement from an oversight or law enforcement agency that states that to do so would be likely to impede with the oversight or law enforcement agency’s activities. The written statement from the oversight or law enforcement agency must specify the time period for which such a suspension is required. Senior Resources must document the identity of the oversight or law enforcement agency and its official and temporarily suspend the individual’s right to an accounting of disclosures as identified in the oversight or law enforcement agency’s written statement.

**ENFORCEMENT:** All supervisors, managers and HIPAA Privacy Compliance Officer/Compliance Advocate are responsible for enforcing this policy. Any suspected violation should be reported to the HIPAA Privacy Compliance Officer/Compliance Advocate or Chief Executive Officer.

**REFERENCES:**

45 CFR: §164.528 [http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl](http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl)

Attachment A: Senior Resources Request for an Accounting of Disclosures
SENIOR RESOURCES
Request for an Accounting of Disclosures

TO BE COMPLETED BY INDIVIDUAL MAKING REQUEST:

Individual’s Name: ______________________________ Date of Request: ____________

Period Dates of Accounting Request: from: ____________,20__ to: ____________,20__

(From date cannot be prior to April 14, 2003 and period covered cannot be greater than six years)

Brief description of PHI disclosure(s) individual is requesting an accounting of:

_____________________________________________________________________________________
_____________________________________________________________________________________

Address where Accounting is to be sent:

_____________________________________________________________________________________
_____________________________________________________________________________________

Phone number where Individual can be reached: ____________________________

Signature: ______________________________ □ Signed by Personal Representative

For Compliance Advocate use only

Date received: ______________ Individual’s ID No.: ____________________________

□ Extension (30 day) Notice sent to Individual; Date sent: ____________________________

Summary of reason for extension: ________________________________________________

□ Accounting not Applicable

(PRIMARY not created by Senior Resources, PRIMARY was part of TPO, or accounting prohibited by law enforcement or oversight agency)

□ Accounting Released to Individual; Date sent: _______________________________

□ Fee Charged Individual; Amount of Fee: _________________________________

□ Accounting Prepared by ____________________________________________________

□ Accounting recorded in Disclosure Log

Notes: ____________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________
Policy: HP.4.4

Effective Date: 04.14.03

Approved: CEO

Revised: 10.06.15

**POLICY:** Individuals have a right to request access to their personal Protected Health Information (PHI) maintained by Senior Resources for up to six years prior to the date of the request. All Senior Resources Workforce must strictly observe this policy.

**PROCEDURE: Acceptance of Request for Access to PHI**

1. Any individual has the right to inspect, or receive copies at their expense, of PHI in their records maintained by Senior Resources.
2. Senior Resources must accept all requests from individuals to access personal PHI.
   a. If Senior Resources does not maintain the PHI that is the subject of the individual’s request for access, and Senior Resources knows where the requested information is maintained, Senior Resources must inform the individual where to direct their request for access.
3. The individual must complete a Consent for Release of Information indicating on the request:
   1) Individual making request;
   2) A brief description of the PHI to be accessed; and
   3) Notation if the individual is requesting to inspect and/or have copies made.
4. If the access is granted, in whole or in part:
   - Senior Resources must make the appropriate arrangements and provide the individual access to the PHI that is the subject of the request in the format requested; or if not, in a readable hard copy as agreed to by both parties.
   - Senior Resources may provide the individual with a summary of the PHI requested, in lieu of providing access to the PHI or may provide an explanation of the PHI to which access has been provided, if the individual agrees in advance to such a summary or explanation.
   - Senior Resources must provide the access requested in a timely manner or within 30 days of request, including arranging with the individual for a convenient time and place to inspect or receive a copy or a mailing of the PHI as requested.
   - If the individual requests copies of, or mailing of the PHI, Senior Resources may impose a reasonable, cost-based fee, provided the fee includes only the cost of copying, postage if agreed to by the individual. Senior Resources must inform the individual of the estimated fee(s) prior to carrying out the request and give the individual opportunity to withdraw or modify their request.

**Denial of Request for Access to PHI**

1. Senior Resources may deny an individual’s request for access, if it is determined that the PHI that is the subject of the request:
   a) Is not maintained by Senior Resources;
   b) Is not part of the record;
   c) Senior Resources is under the direction of a correctional institution or law enforcement request or court order to temporarily deny the individual access;
   d) The Supports Coordinator designated or appointed by Senior Resources for the purpose of managing the client’s health care and privacy rights has determined that the access request is likely to endanger the life or physical safety of the individual or another person; or
   e) The PHI was obtained from someone other than Senior Resources under a promise of confidentiality and access would likely reveal the source of the information.
2. If the requested access is denied, in whole or in part, Senior Resources must provide the individual with a timely, written denial and must include:
   a) The reasoning for denial;
   b) State the individual’s right to submit a written statement to disagree with the denial and where to send a statement to disagree; and
   c) State the individual’s right to file a complaint with Senior Resources or with the U.S. Dept. of Health & Human Services - Office for Civil Rights (OCR).
3. Senior Resources may prepare a written rebuttal to the individual’s statement of disagreement, but it is not required. If a written rebuttal is prepared, a copy must be sent to the individual who submitted a statement to disagree.
4. If an individual submits a written statement of disagreement, Senior Resources must include the individual’s request for amendment and its denial, the client’s statement of disagreement, and the rebuttal, if any, or an accurate summary of such information, with any subsequent disclosure of the PHI to which the disagreement relates.

**ENFORCEMENT:** All supervisors, managers and the HIPAA Privacy Compliance Officer/Compliance Advocate are responsible for enforcing this policy. Any suspected violation should be reported to the HIPAA Privacy Compliance Officer/Compliance Advocate or Chief Executive Officer.

**REFERENCES:**
45 C.F.R §164.524 [http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl](http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl)
Consent for Release of Information
POLICY: Individuals have a right to request amendment to their personal Protected Health Information (PHI) maintained by Senior Resources prior to the date of the request. All Senior Resources Workforce must strictly observe this policy.

PROCEDURE: Acceptance of Request for Access to PHI
1. The individual must make the request to amend PHI in writing to the HIPAA Privacy Compliance Officer/Compliance Advocate at Senior Resources with reasoning to support a requested amendment. The request should be made on the form Request for an Amendment/Correction of PHI (attachment A).
2. Senior Resources must accept all requests from individuals to amend personal PHI.
3. Senior Resources must act on the individual’s request for an amendment no later than 60 days after receipt. If Senior Resources is unable to act on the amendment request within 60 days, Senior Resources may extend the time for such action by no more than 30 days, provided that:
   a) Senior Resources provides the individual with a written statement of the reasons for the delay and the date by which action on the request will be completed; and Senior Resources may have only one such extension of time for action on each request for an amendment.
   b) The HIPAA Privacy Compliance Officer/Compliance Advocate will be responsible for receiving and overseeing the processing of requests for amendment to PHI. The HIPAA Privacy Compliance Officer/Compliance Advocate will document and maintain a log to record each amendment of PHI to include:
      • Date of request;
      • Individual making request;
      • The name of the providers or persons who received the PHI, and if the individual consents, if they are to be notified of the amendment;
      • A brief description of the PHI amended;
      • The date of the amendment;
      • Notation if amendment was not made within 60 days, brief summary of reason why not, and whether or not a notice for 30 days extension to disclose was sent to the requesting individual;
      • The fee charged (if any) to include amount of personnel time and number of pages copied;
      • Name of personnel who made the amendment to the record.
4. If the amendment is granted, in whole or in part:
   1) Senior Resources must make the appropriate amendment to the PHI or record that is the subject of the request for amendment by, at a minimum, identifying the records that are affected by the amendment and appending or otherwise providing a link to the location of the amendment.
   2) Senior Resources must inform the individual in a timely manner that the amendment is accepted and obtain the individual’s identification of an agreement to have Senior Resources notify the relevant person or provider with which the amendment needs to be shared.
   3) Senior Resources must make reasonable efforts to inform and provide the amendment within the required time, to:
      i. Persons or providers identified by the individual as having received PHI about the individual and needing amendment; and
      ii. Persons or providers that Senior Resources knows have the PHI that is the subject of the amendment and that may have relied, or could rely, on such information to the detriment of the individual.
Denial of Request for Amendment to PHI

1. Senior Resources may deny an individual’s request for amendment, if it is determined that the PHI that is the subject of the request:
   a) Was not created by Senior Resources, unless the individual provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment;
   b) Is not part of the designated record or data set;
      i. Would not be available for inspection under the Denial of Access section of Senior Resources HIPAA Policy, No. HP.4.4, Request for Access to PHI.
      ii. Is determined to be accurate and complete as written.

2. If the requested amendment is denied, in whole or in part, Senior Resources must provide the individual with a timely, written denial and must include:
   a) The reasoning for denial;
   b) State the individual’s right to submit a written statement to disagree with the denial and where to send a statement to disagree; and
   c) State the individual’s right to file a complaint with Senior Resources or with the Dept. of Health & Human Services - Office of Civil Rights.

3. Senior Resources may prepare a written rebuttal to the individual’s statement of disagreement, but it is not required. If a written rebuttal is prepared, a copy must be sent to the individual who submitted a statement to disagree.

4. If an individual submits a written statement of disagreement, Senior Resources must include the individual’s request for amendment and its denial, the client’s statement of disagreement, and the rebuttal, if any, or an accurate summary of such information, with any subsequent disclosure of the PHI to which the disagreement relates.

ENFORCEMENT: All supervisors, managers and the HIPAA Privacy Compliance Officer /Compliance Advocate are responsible for enforcing this policy. Any suspected violation should be reported to the HIPAA Privacy Compliance Officer/ Compliance Advocate or Chief Executive Officer.

REFERENCES:
45 C.F.R. §164.526 http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl
HIPAA Policy, No. HP.4.4, Request for Access to PHI
Attachment A: Senior Resources Request for an Amendment/Correction of PHI
TO BE COMPLETED BY INDIVIDUAL MAKING REQUEST:
(Complete separate form for each amendment/correction requested)

Individual’s Name: ___________________________ Date of Request: _________________

Dates of Entry/Record to be Amended/Corrected: _____________, 20____

Brief description of PHI individual is requesting an amendment/correction of:
_____________________________________________________________________________________
_____________________________________________________________________________________
_____________________________________________________________________________________  

Would you like the accepted amendment sent to anyone to whom we may have disclosed the information to? If so, please specify the name and address of the individual or provider:
Name: ____________________________________ Address: ______________________________
_________________________________________ ____________________________________________
_________________________________________ ____________________________________________
_________________________________________ ____________________________________________

Phone number where Individual can be reached: ______________________________

Signature: _______________________________ □ Signed by Personal Representative

For HIPAA Privacy Compliance Officer /Compliance Advocate use only

Date received: ___________________ Individual’s ID No.: ____________________________

□ Request Accepted; Date amendment/correction made: ____________________________

□ Request Denied
Reason denied:
(PHI not created by Senior Resources, PHI not part of record, PHI is deemed accurate and complete or prohibited by law)

□ Case Worker informed of decision and amendment/correction as applicable

□ Individual notified of decision in writing

HIPAA Privacy Compliance Officer /Compliance Advocate Signature: ___________________________ Completed on: ___________________
POLICY: Senior Resources shall implement appropriate policies and procedures to comply with the standards, implementation specifications and other requirements of the Security Rule.

PROCEDURES: Senior Resources may change the policies at any time, to ensure compliance with federal and state security regulations and standards.

Senior Resources shall maintain and retain documentation of policies, procedures and actions implemented under these regulations.

Senior Resources shall make documentation available to those persons responsible for implementing procedures to which the documentation pertains.

The HIPAA Security Officer in conjunction with the HIPAA Privacy Compliance Office/Compliance Advocate shall:

- Investigate security incidents (i.e. known or suspected violations of the security policies and procedures and breaches in security measure or the security of the agency’s PHI.
- Review information system activity to ensure compliance with agency’s security policies and procedures.
- Develop and implement a security training and awareness program for the employees, staff and volunteers.
- HIPAA Security Compliance Officer/Compliance Advocate shall review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of electronic protected health information.

ENFORCEMENT: The Security Administrative Requirements are reviewed with and approved by the Security Officer and the Chief Executive Officer.

REFERENCES:
45 CFR §164.316 http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl
45 CFR §164.308(a)(1)(i)
POLICY: Senior Resources has established a comprehensive security management process to ensure the availability, integrity, and confidentiality of participant information and other sensitive information. The goals of this program include preventing, detecting, containing, and correcting threats to the security of sensitive information.

Storage and access to centralized electronic Personal Health Information (ePHI) on a server, processing of additions, changes and deletions to ePHI, transmission of ePHI between Senior Resources and Center for Information Management (CIM) centralized server, and the submission of ePHI to the State of Michigan is under the control of CIM and is beyond the scope of Senior Resources. Security Management for these functions is the responsibility of CIM and is covered in the contract with CIM.

Storage and access to centralized electronic Personal Health Information (ePHI) on a server, processing of additions, changes and deletions to ePHI, transmission of ePHI between Senior Resources and Mediware/Harmony centralized server, and the submission of ePHI to the State of Michigan is under the control of Mediware/Harmony and is covered in the contract with Mediware/Harmony.

PROCEDURE: Technical and non-technical evaluation procedure – annual evaluation of all incidents and investigations are summarized in a report with recommendations for changes to policy and procedure presented to the full management team. Technical and non-technical evaluation will be performed internally and with assistance of a third party associate.

ENFORCEMENT: It is the responsibility of the Security Officer, HIPAA Privacy Compliance Officer/Compliance Advocate, and the Chief Executive Officer to enforce this policy. Any breaches of this policy are to be reported immediately to the HIPAA Privacy Compliance Officer/Compliance Advocate.

REFERENCES:
45 CFR §164.308(a)(1)(i) http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl164.308(a)(8)
Technology Plan
CIM Contract
Mediware/Harmony Contract
Assignment of Security Officer Responsibilities

**Policy:** HP.5.3
**Effective Date:** 04.01.06
**Approved:** Yam Curtis, CEO
**Revised:** 10.8.15; 2.9.16
**Reviewed:** 2.9.16

**POLICY:** The Security Officer develops and implements policies and safeguards allowing only those staff members who have the appropriate qualification and job responsibilities to use Senior Resources electronic personal health information (ePHI) and information systems.

**PROCEDURE:** The Security Officer shall ensure that all members of the workforce have appropriate access to electronic protected health information.

The Security Officer shall implement reasonable and appropriate security measures to prevent staff members of the workforce who do not need access to electronic protected health information from obtaining such access.

The Security Officer shall ensure that workforce members, who work with electronic protected health information, (ePHI) or in locations where it might be accessed, are authorized for such access.

The Security Officer shall ensure that workforce members utilizing ePHI will be forced to use user name and case sensitive passwords and that workstations must be protected by password-protected screen saver or password-protected power schemes.

The Security Officer shall review every six month all employees’ access to ePHI and shall terminate that access to ePHI when it is determined that such access is not appropriate.

The Security Officer shall implement procedures for terminating access to electronic protected health information when the staff member is no longer employed by the agency. Human Resources will notify security officer upon employee separation and access will be immediately terminated by disabling access to administrative offices or altering passwords to prevent computer entry.

**ENFORCEMENT:** This Assignment Policy is reviewed with and approved by the Security Officer, and Chief Executive Officer.

**REFERENCES:**
45 C.F.R.164.308(a)(2) [http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl](http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl)
SCOPE: All personnel of Senior Resources who have or are responsible for an account on any system that resides at Senior Resources facility, has access to the Senior Resources network, or stores any non-public Senior Resources information.

POLICY: Senior Resources assures the development and maintenance of appropriate mechanisms to protect the confidentiality, integrity and availability of its computerized data and information resources security requirement for all workforce use of Senior Resources’ computer systems and data. This policy covers Senior Resources central computer network, all software programs and systems, all data maintained in active or archived files.

PROCEDURE: The Security Officer or other authorized staff will establish all levels of security.

- Access to Senior Resources network or data systems will be regulated at all times.
- Obsolete computer equipment will be disposed of according to the Senior Resources Electronic Equipment Disposal Policy.
- All network and equipment will be installed and maintained by Senior Resources.
- Users may not install hubs, wireless access points, terminal services, or other equipment that extends the network nor may they alter, remove, or tamper with any equipment managed by Senior Resources.
- Programs that interfere with proper network operations or that create interference or risk will not be allowed.
- Traffic that poses a possible threat to Senior Resources will be prevented from entering and exiting the network.
- Wireless access will be permitted for registered computers, and approved guests of Senior Resources through the Security Officer.
- Antivirus Software will be active on workstations connected to the network.
- Workstations will be protected from the Internet by a firewall and by encryption software on those that contain Personal Health Information (PHI).
- Security Officer will enforce group policies on workstations accessing PHI or employees records and will install, monitor and manage workstations requiring encryption software.
- Workstations accessing sensitive information, including PHI, must be protected by password-protected screen saver or password-protected power schemes. In addition, workstations containing sensitive information, including PHI, must be protected by encryption software. Backups will be performed according to schedules determined by type, sensitivity, importance, and value.
- Sensitive data transmitted into or out of the Senior Resources network or data systems via the public Internet must be encrypted.
- Access to systems and data will be granted and managed by the Security Officer or other authorized staff as needed, using appropriate passwords.
- Access will be immediately terminated when a user separates from Senior Resources by the Security Officer and/or other authorized staff.

ENFORCEMENT: The Workforce Security Policy is reviewed with and approved by the Senior Resources Security Officer, HIPAA Privacy Compliance Officer/Compliance Advocate, other authorized staff and the Chief Executive Officer.
It is the responsibility of the Security Officer, the HIPAA Privacy Compliance Officer/Compliance Advocate and the Chief Executive Officer to enforce this policy. Any breaches of this policy are to be reported immediately to the Security Officer, HIPAA Privacy Compliance Officer/Compliance Advocate or the Chief Executive Officer.

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

REFERENCES:
45 CFR §164.308(a)(3)(i) http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl
HP.7.5 Removal of Electronic Protected Health Information
HP.7.6 Record of Movement of Hardware and Electronic Media
45 CFR §164.308(a)(3)(ii)(C)
POLICY: The Security Officer is responsible for developing and implementing procedures to authorize staff members use of personal health information (PHI) resources. This includes establishing access to PHI, based upon a staff member’s job responsibilities and qualifications. Authorization is limited to information the employee needs to fulfill their job responsibilities as documented in their job descriptions.

PROCEDURE: Access to PHI and other confidential information is under the jurisdiction of the Security Officer or Managed Care Operations Manager and will be assigned to users, programs, processes or other automated mechanisms using role-based access. Access will be assigned to programs, transactions and data based on the workforce documented job descriptions or contractual agreements.

Systems or applications containing electronic PHI, the password to the administrator account or account with highest privileges will be documented and maintained in a secure location accessible only by authorized personnel to be used in cases where emergency access is required.

All terminals/consoles that allow logon access to systems containing electronic PHI or other confidential information will implement electronic procedures that terminate or lock an electronic session after a predetermined time of inactivity. Higher inactivity time limits can be set on terminals that are located in more physically secured locations; however, no limits greater than 8 minutes should be used. In addition, portable computing devices that allow logon access to systems containing PHI will be further protected by encrypting data in accordance with the State of Michigan Encryption Policy. Only authorized staff members are allowed to use workstations (computer terminals, personal computers, and other devices) that can access PHI.

ENFORCEMENT: The Information Access Management Policy is reviewed with and approved by the Senior Resources Security Officer, HIPAA Privacy Compliance Officer/ Compliance Advocate, Managed Care Operations Manager, the Executive Director and Senior Resources Management. It is the responsibility of the Security Officer, HIPAA Privacy Compliance Officer/ Compliance Advocate, Managed Care Operations Manager, and the Chief Executive Officer of Senior Resources to enforce this policy. Any breaches of this policy are to be reported immediately to the Security Officer.

REFERENCES:
45 CFR §164.308(a)(4)(7) [http://www.ecfr.gov/cgi-bin/text-idx;tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl]
45 CFR §164.312(a)(2)(iv)
45 CFR §164.312(a)(2)(iii)
45 CFR §164.312(d)
POLICY: The Security Officer periodically reviews records of information system activity, such as audit logs, access reports, and security tracking reports. The Security Officer shall design and implement a security awareness and training program for all members of the workforce, including volunteers and management.

PROCEDURE: The Security Officer reviews all security incident reports and ensures that any breaches in security have been corrected.

The Security Officer regularly reviews records of system activity to identify any patterns of activity that suggest Senior Resources security policies and procedures have been breached, either by a staff member or by individuals or organizations that are not business associates. The Security Officer determines whether security has been violated and takes appropriate corrective action, including changes in security policies and procedures.

The Security Officer maintains records of all reviews of security incidents and system activity, and reports any finding to the other members of Senior Resources.

The Security Officer shall design and implement a security awareness and training program for all members of the workforce, including volunteers and management.

Senior Resources will keep anti-virus software up-to-date and the Security Officer shall regularly remind users to be attentive to security, such as guarding passwords.

ENFORCEMENT: The Security Awareness and Training Policy is reviewed with and approved by the Security Officer, HIPAA Privacy Compliance Officer/Compliance Advocate, and Chief Executive Officer.

It is the responsibility of the Security Officer, HIPAA Privacy Compliance Officer/Compliance Advocate, the Chief Executive Officer of Senior Resources to execute and enforce this policy.

REFERENCES:
45 C.F.R.164.308(a)(5)(i) http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl
POLICY: Security incidents are to be reported promptly to the Senior Resources security officer. Incidents should be reported by the staff members responsible for the incident or staff members who identify the incident. No sanction or penalty is imposed for simply reporting a security incident.

SCOPE: This policy applies to all Senior Resources (SR) employees and volunteers including those who are part time, temporary and contractual, hereby referred to as “staff.”

PROCEDURE: Any staff member of Senior Resources who suspects the occurrence of a security incident must report the incident through the following channels:

All suspected events involving possible breaches electronic personal identity information (ePHI), must be reported to the Security Officer as quickly as possible by phone (preferred), e-mail, or in person. If the Security Officer cannot be reached, contact the HIPAA Privacy Compliance Officer / Compliance Advocate or Chief Executive Officer.

The security officer investigates security incident and determines:
1. Whether a breach of security has occurred
2. The appropriate actions to take to repair any damage or potential damage to security that the incident might have caused.

The security officer ensures that actions needed to repair any damage caused or potentially caused by a security incident are taken.

The security officer documents the incident date and time, computer system(s) name and/or numbers affected, operating system(s) on the system affected, type of system affected (workstation, mail server, file server, etc.), type of intrusion (data compromise, virus incident, etc.), how the intrusion was discovered, effect of the intrusion, how the intrusion was removed, steps taken to prevent the same type of intrusion again, who was notified about the intrusion.

ENFORCEMENT: The Security Administrative Requirement are reviewed with and approved by the HIPAA Privacy Compliance Officer/ Compliance Advocate, and Chief Executive Officer.

It is the responsibility of the Security Officer, HIPAA Privacy Compliance Officer/ Compliance Advocate, and Chief Executive Officer to execute and enforce this policy.

REFERENCES:
45 CFR §164.308(a)(6) http://www.ecfr.gov/cgi-bin/text-index.tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl
Security Incident Log
Electronic Contingency Planning Policy and Procedure

Policy: HP.5.8.9

Approved: , CEO

Effective Date: 04/01/2006


**POLICY:** The agency shall establish and implement as needed, reasonable and appropriate procedures for responding to an emergency or other occurrence (fire, vandalism, system failure and natural disaster) that damages systems that contain electronic protected health information (ePHI). Security includes the availability, integrity, and confidentiality of the information.

**PROCEDURE:** The security officer shall establish and implement a data backup plan for creating and maintaining retrievable exact copies of electronic protected health information.

The security officer shall establish and implement as needed, an Internal Business Continuity Policy and Procedure and a Risk Management Plan for restoring any loss of data.

The security officer shall establish and implement as needed, an emergency mode operation plan to enable continuation of critical business processes that are used to protect the security of electronic protected health information during emergencies.

The security officer shall annually test and revise contingency plans.

The agency shall assess the relative criticality of specific applications and data needed for other contingency plan components.

Senior Resources has arranged for daily back-up of all ePHI to be performed by CIM server. Secondary back-ups are performed at least daily of all ePHI to Senior Resources Network Area Storage drive. Weekly / Monthly portable drives are taken off site. Portable drives are secured monthly in a bank deposit box and weekly in a home safe.

**ENFORCEMENT:** The Contingency Planning is reviewed with and approved by the HIPAA Privacy Compliance Officer/ Compliance Advocate and Chief Executive Officer.

It is the responsibility of the Security Officer, and Chief Executive Officer to enforce this policy. Any breaches of this policy are to be reported immediately to the Security Officer.

**REFERENCES:**

45 CFR §164.308(7)(i)

http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl

A.D.1.2 Internal Business Continuity Policy and Procedure

F.C.1.21 Risk Management Plan
Security Risk Analysis Policy and Procedure

<table>
<thead>
<tr>
<th>Policy: HP.5.10</th>
<th>Effective Date: 04.01.06</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved:</td>
<td>Revised: 10.14.15; 4.13.16</td>
</tr>
<tr>
<td></td>
<td>Reviewed: 4.13.16</td>
</tr>
</tbody>
</table>

**POLICY:** The Security Officer and Managed Care Operation Manager is responsible to ensure that an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI) held by Senior Resources is conducted for the purpose of reducing risks and vulnerabilities to a reasonable and appropriate level.

Storage and access to centralized ePHI on a server, processing of additions, changes and deletions to ePHI, transmission of ePHI between Senior Resources and Center for Information Management (CIM) centralized server, and the submission of ePHI to the State of Michigan is under the control of CIM and beyond the scope of Senior Resources. Risk analysis for these functions is the responsibility of CIM and is covered in the Contract with CIM.

**PROCEDURES:** A comprehensive analysis of MICIS and COMPASS and Mediware/Harmony security threats is conducted at least every three years by CIM and Mediware. The risk analysis by CIM and Mediware will identify threats to the security of Senior Resources’ MICIS and COMPASS and Mediware / Harmony system ePHI including natural, human, and environmental threats.

In addition, a third party IT vendor will conduct, no less than once every three years, a security risk analysis for Senior Resources. Network Manager will run an internal risk assessment on internet activity/event logs monthly.

The IT vendor risk-management plan will summarize the results of the risk analysis, including the major security threats and the measures that will be implemented to mitigate or reduce risks to an acceptable level, and will identify the specific actions that will be taken to implement the security measures identified in the risk analysis.

**ENFORCEMENT:** Each risk analysis will be reviewed and approved by the Security Officer, Managed Care Operation Manager and HIPAA Privacy Compliance Officer/ Compliance Advocate. The results of the risk analysis will be shared with the Chief Executive Officer and other management staff.

**REFERENCES:**
45 CFR §164.308(a)(1)(ii)(B)
http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl
CIM Contract
Mediware/Harmony Contract
POLICY: Breach notification must be carried out in compliance with the American Recovery and Reinvestment Act (ARRA)/Health Information Technology for Economic and Clinical Health Act (HITECH) as well as any other federal or state notification law.

DEFINITION:
Breach: Means the non-permissive or unauthorized acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the PHI and poses a significant risk of financial, reputational, or other harm to the individual. *Refer to Attachment A: Breach Examples Grid.*

Breach excludes:
1. Any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of Senior Resources (SR) or its Business Associate (BA) if such acquisition, access, or use was made in good faith and within the scope of assigned authority (by SR) and does not result in further use or disclosure in a manner not permitted under the Privacy Rule.
2. Any inadvertent disclosure by a person who is authorized to access PHI retained by SR or its BA to another person authorized to access PHI at SR or its BA or an organized health care arrangement in which the SR participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule.
3. A disclosure of PHI where SR or its BA has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to access or retain such information.

PROCEDURE: The date a breach of PHI is "discovered" is the first day that any person who is a workforce member of SR or a BA of SR becomes aware that potential breach occurred. Following the discovery of a potential breach, the workforce member or BA is required to submit a Breach Incident Report form (*Attachment B*) immediately to the Security Officer of SR. The Security Officer will begin an investigation. With an investigative team comprised of Security & HIPAA Privacy Compliance Officer/ Compliance Advocate, Managed Care Operations Manager, and supervisors by conducting an assessment of potential breach and its risk. *Refer to Attachment C: PHI Breach Notification Process Flowchart.*

Based on the results of the investigation, if the investigative team of SR determines that a breach did indeed occur, the Security Officer will begin the process to determine remediation and corrective actions, and the Privacy Officer will take action to notify each individual whose PHI has been or is reasonably believed to have been breached. The HIPAA Privacy Compliance Officer/ Compliance Advocate will also begin the process of determining what external notifications are required or should be made such as to the Department of Health & Human Services (DHHS), media outlets, law enforcement officials, etc.). All investigation, remedial and notification steps will be logged by the Security and HIPAA Privacy Compliance Officer/ Compliance Advocate.

Upon determination that breach notification to clients is required, the notice shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach by the organization involved or the business associate involved. The HIPAA Privacy Compliance Officer/ Compliance Advocate will document that all notifications were made as required. If a law enforcement agency provides a statement in
writing to SR that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, SR will delay such notification, notice, or posting temporarily and no longer than 30 days from the date of the request.

Client notices will be written in plain language and will contain the following information:
1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
2. Description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved).
3. Any steps the client should take to protect themselves from potential harm resulting from the breach.
4. A brief description of what SR is doing to investigate the breach, to mitigate harm to clients, and to protect against further breaches.
5. Contact information for clients to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, web site, or mailing address.

The following methods of notification will be utilized accordingly:
1. Written notification by first-class mail to the client at the last known address of the client. The notification shall be provided in one or more mailings as information is available. If SR knows that the client is deceased and has the address of the next of kin or personal representative of the client, written notification by first-class shall be carried out.
2. Substitute Notice: In the case where there is insufficient or out-of-date contact information (including a phone number, email address, etc.) that precludes direct written notification, a substitute form of notice reasonably calculated to reach the client shall be provided. A substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative. In a case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, then the substitute notice may be provided by an alternative form of written notice such as by telephone, or other means. In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then the substitute notice shall be in the form of either a conspicuous posting for a period of 90 days on the home page of SR’s website, or a conspicuous notice by broadcast media or newssprint in SR’s geographic areas where the individuals affected by the breach reside. The notice shall include a toll-free number that remains active or at least 90 days where a client can learn whether their PHI may be included in the breach.
3. If the organization determines that notification requires urgency because of possible imminent fraud or abuse of clients due to release of unsecured PHI, notification may be provided by telephone or other means, as appropriate in addition to the methods noted above.
4. When more than 500 clients are involved in a breach of PHI, notice will be provided to DHHS via their internet website at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/br_instruction.html at the same time notice is made to the individuals. In addition, notice will be provided to prominent media outlets serving the state and regional area when the breach of unsecured PHI affects more than 500 patients. The Notice will be provided in the form of a press release.
5. For breaches involving less than 500 individuals, SR will maintain a log of the breaches and annually submit the log to the Secretary of Office of Civil Rights 60 days before the completion of the calendar year. Instructions for submitting the log are provided at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/br_instruction.html
6. SR will maintain a process to record or log all breaches of unsecured PHI regardless of the number of clients affected that includes all investigative and remediation steps taken, all the information provided in
the client notice, document any law enforcement notifications/requests, and steps taken to mitigate the breach and prevent future occurrences. All documentation related to the breach investigation, including the investigation, law enforcement requests to delay, client notices and remediation/corrective actions will be retained for a minimum of six years.

**PENALTIES:** Penalties for violations or breach of PHI have been established under the HITECH act and has given authority to the US Dept. of Health & Human Services to determine penalty level. Penalties do not apply if the involved entity did not have knowledge of, or by exercising reasonable diligence would not have known of, the violation or if the failure to comply was due to a reasonable cause and was corrected within thirty (30) days. The Secretary of the Dept. of Health & Human Services will base its penalty determination of the nature and extent of the breach and what harm it may have caused involved individuals, and has the discretion to impose corrective action without penalty. Minimum penalties are tiered based upon culpability.

**ENFORCEMENT:** It is the responsibility of all members of Senior Resources workforce and its Business Associates to report suspected violations of Senior Resources HIPAA Privacy policies and PHI breaches to Senior Resources’ Security and HIPAA Privacy Compliance Officer/ Compliance Advocate, and/or contracts coordinator

It is the responsibility of the Privacy, HIPAA Privacy Compliance Officer/ Compliance Advocate and Contracts Coordinator to confidentially investigate all reported violations, documenting the alleged violation, alleged members involved and persons interviewed during the investigation. Once an investigation is concluded, a written report will be given to the Chief Executive Officer of Senior Resources and the involved Business Associate and appropriate supervisor(s). Individuals who are found to have violated the policies and procedures will be subject to disciplinary action which may result in termination of employment or contractual.

**REFERENCES:**
45 C.F.R. §160.103 [http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl](http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl)
45 C.F.R. §164.503 [http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl](http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl)
### Attachment A

**Breach Example Grid**

<table>
<thead>
<tr>
<th>Situation:</th>
<th>Notify Security Officer?</th>
</tr>
</thead>
<tbody>
<tr>
<td>PHI mistakenly faxed to a non-associate business</td>
<td>Yes</td>
</tr>
<tr>
<td>PHI mistakenly faxed to wrong business associate</td>
<td>Not Required</td>
</tr>
<tr>
<td>PHI faxed to client’s former provider who is still a business associate of Senior Resources</td>
<td>Not Required</td>
</tr>
<tr>
<td>PHI provided to wrong client (other client name on form)</td>
<td>Yes</td>
</tr>
<tr>
<td>PHI provided to wrong client, but was retrieved before the client was able to view the other client's name/information (can take word of ‘wrong’ client that they have not seen or opened)</td>
<td>Not Required</td>
</tr>
<tr>
<td>Claim or PHI sent to incorrect third party payer or other Medicaid Agent</td>
<td>Not Required</td>
</tr>
<tr>
<td>Client PHI sent to an incorrect mailing address, lost in mailing process, and was never received or returned</td>
<td>Yes</td>
</tr>
<tr>
<td>Info given to a family member for a client who requested restricted access</td>
<td>Yes</td>
</tr>
<tr>
<td>PHI documents viewable in area of office building used by the public or other agency’s staff</td>
<td>Yes</td>
</tr>
<tr>
<td>Can hear client names called in a waiting area</td>
<td>Not Required</td>
</tr>
<tr>
<td>Briefcase or file folder containing client paper record documents stolen</td>
<td>Yes</td>
</tr>
<tr>
<td>Papers containing protected health information missing or found offsite such as in trash (not shredded), or after a vehicle is involved in a break-in, or there is an accident involving the vehicle, or papers fall out of an unsecured briefcase/tote bag in a public area.</td>
<td>Yes</td>
</tr>
<tr>
<td>Agency documents containing client PHI improperly disposed of at an employee's residence</td>
<td>Yes</td>
</tr>
<tr>
<td>Workforce members who have no HIPAA authorization listed in their job description who intentionally access the record information of a client for their own non-work related curiosity</td>
<td>Yes</td>
</tr>
<tr>
<td>Unencrypted flash drive lost that contains client PHI</td>
<td>Yes</td>
</tr>
<tr>
<td>Misdirected e-mail of client PHI to outside (non-business) associate</td>
<td>Yes, unless encrypted</td>
</tr>
<tr>
<td>Stolen/lost laptop containing unsecured PHI</td>
<td>Yes</td>
</tr>
<tr>
<td>PDA, Smartphone or cell phone lost or stolen containing client-identifying information such as name &amp; phone number or address; few are encrypted</td>
<td>Yes</td>
</tr>
</tbody>
</table>
## Private Health Information (PHI) Security Breach Incident Report Form

If you suspect a breach, or receive information suggesting a breach may have occurred, involving the PHI of a Senior Resources client, complete this Security Breach Incident Report form to collect initial details about the incident to assist the Senior Resources investigation team in determining whether a breach has occurred and if so, the extent of the breach. It is essential also that you verbally report the suspected breach to your supervisor as well. Route the completed Incident Report form to Senior Resources Security or Privacy Officer immediately by faxing to (231) 733-3561 or (231) 733-3508.

### A. Incident Details:

1. **Date of incident (indicate if known date or estimated)**

2. **Date of discovery of incident**

3. **Date incident was first reported and by whom. Include contact information (phone, email, mailing address)**

4. **Indicate to whom the incident was verbally reported (Executive Director, Contract/Data manager, Privacy Officer, Security Officer, or any other Senior Resource staff person)**

5. **Identify any staff or providers (business associates) with knowledge of the incident (include phone numbers when possible)**

### B. Incident Description:

1. **Description of the incident: Describe what (reasonably believed) unauthorized use or disclosure client PHI occurred?**

2. **If a Business Associate/Provider was identified in No. A-5 above, describe their involvement/knowledge of the incident:**

3. **List or describe what client PHI, documents or data elements were involved?**

4. **Description of where the PHI is believed to have been improperly transmitted sent or utilized.**

5. **How many clients do you believe had their PHI breached?**

*If there is not adequate space to complete answers, please continue explanations on a blank sheet, numbered according to Section/Question and attach to this form.*
**Attachment B**

**BREACH NOTIFICATION PROCESS Flowchart**

**You Suspect Breach of Client PHI: Complete a Senior Resources Breach Incident Report**
- cc: report to your Supervisor

**You call Security Officer & fax or email* Breach Incident report**
- cc: report to Data Manager & Privacy Officer

**Security Officer, Privacy Officer, Supervisor(s) & Data Manager meet to determine if suspected breach is a violation**
- NO
  - Log breach details to report annually to www.HHS.OCR.gov
  - Data Manager determines if adequate contact info available for written notification method to individuals and queries data necessary to mail notices.
  - Security Officer determines remediation plan to secure PHI & implements correction actions to prevent future occurrence.
- YES
  - Security officer determines remediation & correction action
  - Privacy Officer drafts notice to individuals and logs necessary breach data for annual reporting to HHS. If necessary, confers with Director and Community Relations regarding media notices.

**Did breach involve more than 500 individuals?**
- NO
  - Log breach details to report annually to www.HHS.OCR.gov
  - Security Officer determines remediation & correction action
- YES
  - Immediately report breach to www.HHS.OCR.gov to report breach

*Only email incident report if using encryption software and/or emailing within “srwmi.org” domain, otherwise fax report to (231) 733-3508 or 733-3561.
POLICY: The Security Officer develops and implements policies and procedures that allow only authorized staff members and contractors to physically and remotely access Personal Health Information (PHI). The Security Officer has the right to grant or deny access to PHI by staff members. Human Resources has the right to grant or deny access to the building and office entrances. Any maintenance on areas housing PHI will be approved by the facility manager and a record of maintenance will be retained.

PROCEDURE: Security Officer with assistance from third party vendor monitors servers and firewalls daily for security/access breaches or potential failures. All entry doors to Senior Resources administration offices are secured with keycard entry or keyed entry. Senior Resources Management staff, fire department and the cleaning company are the only persons that have administrative office access 24 hours a day. Management staff with 24-hr administrative office access includes the Chief Executive Officer, MI Choice Medicaid Waiver Director, Human Resources, Community Services Director, Network Manager, and Call Center Director.

Documentation of physical alterations to facilities that change access and security of PHI, both written and electronic, will be documented and logged by facility manager. Responsibility for maintaining records is tasked to the owners of the building (LifeCircles).

Senior Resources maintains a complete inventory of all assets belonging to the agency. They are listed on the SR Computer Inventory log. All laptop, desktop, printers are listed.

ENFORCEMENT: The Security Administrative Requirement are reviewed with and approved by the Security Officer, the Chief Executive Officer, the HIPAA Privacy Compliance Officer/Compliance Advocate and Senior Resources Management.

REFERENCES:
45 CFR§164.310(a)(1) http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl
45 CFR§ 164.310(a)(2)(iv) http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl
SR Computer Inventory log
45 CFR§ 164.310(a)(2)(ii)
POLICY: The Security Officer and third party vendor oversee and safeguard the company's assets, computer systems and network security. Employees are responsible for maintaining the physical security of their computer resources under their control and for protecting the integrity and privacy of the data, including the privacy and difficulty of network passwords. Senior Resources reserves the right to inspect all data and to monitor the use of its computers systems. Senior Resources provides all staff access to electronic email for business purposes and reserves the right to block any incoming email that is flagged as SPAM.

Any device containing or accessing protected health information must be protected by password and encrypted.

Senior Resources respects the privacy of staff and desires to provide a reasonable level of privacy. However, users will be made aware that the data they create on the agency systems remain the property of Senior Resources.

Passwords are not to be inserted into email messages or other forms of electronic communication. Passwords and user names for computer systems and networks must not be stored on portable computing devices or in a public place.

All network and equipment will be installed and maintained by Senior Resources. Users may not install any other equipment that extends the network nor may they alter, remove, or tamper with any equipment managed by Senior Resources. Users may not independently install hardware or software to the computing resources of Senior Resources.

PROCEDURE: All employees/volunteers are granted access to devices/programs based upon need-to-know or need-to-use basis.

Each new staff member also receives access to an email account. No email account of Senior Resources network shall be used for commercial purposes or for personal financial gain.

All devices must be equipped with updated software for detection of the presence of malicious software.

Every user must log off the applications on their workstations and shut down their computer at the end of the workday.

All employees accessing the network from a remote location, such as a connection from home, should employ appropriate approved security safeguards.

A password-protected screensaver or locking software must be activated after an approved set period of time. Senior Resources Security Officer sets that time in accordance with HIPAA’s standards.

Passwords are an important aspect of computer security. All users should be aware of how to select a strong password. All user passwords must conform to the guidelines described; all passwords are to be treated as sensitive, confidential, information. Passwords must contain both upper and lower case characters and contain
one digit 0-9; they may contain special characters (#&$%^); passwords should not be based on personal information or names of family members. Group Policy requires users’ passwords to be changed at least every 90 days.

If an account or password is suspected to have been compromised, it is to be reported to the Senior Resources Network Manager/Security Officer.

Senior Resources shall take reasonable and appropriate steps to ensure that laptops and workstations that containing electronic protected health information ePHI are protected with security controls, such as full disk encryption.

Employees are required to sign an Acceptable Use Agreement as found in HR.1.12a Acceptable Use Policy (Agency Systems/Device/Infrastructure).

Upon termination or change of job position, users will have network access removed or modified.

ENFORCEMENT:
It is the responsibility of the Security Officer, HIPAA Privacy Compliance Officer/Compliance Advocate, and the Chief Executive Officer to enforce this policy. Any breaches of this policy are to be reported immediately to the HIPAA Privacy Compliance Officer/Compliance Advocate and the Security Officer.

An employee or volunteer who believes that he or she has been wrongly charged with a security violation may appeal the decision using the Employee Complaint Policy. Violation of ePHI may be subject to disciplinary action, up to and including termination of employment.

REFERENCES:
45 CFR §164.312(a-d) http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl
45 CFR §164.308(b) http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl
45 CFR §164.308(c) http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl
HR.1.10 Employee Complaint Policy
HR.1.12a Acceptable Use Policy (Agency Systems/Device/Infrastructure)
HR.1.12b Acceptable Use Policy – Non Agency Owned Devices
POLICY: The Security Officer is responsible to ensure that required access and control safeguards are in place to ensure the safe transmission of electronic protected health information (ePHI) entered by Senior Resources workforce to protected information databases. Storage and access to centralized ePHI on a server, processing of additions, changes and deletions to ePHI, transmission of ePHI between Senior Resources and Center for Information Management (CIM) centralized server, and the submission of ePHI to the State of Michigan is under the control of CIM and beyond the scope of Senior Resources. Risk analysis for these functions is the responsibility of the individual agencies managing the database and covered in the Statement of MICIS/COMPASS Service Bureau Compliance.

PROCEDURES: The Managed Care Operations Manager is responsible to request from CIM a password and login with access rights assigned by CIM for each workforce member using the MICIS system.

The Security Officer is responsible to ensure that each MICIS/COMPASS user is accessing the ePHI via a Virtual Private Network (VPN) connection as provided by CIM.

The transmission functions controlled by CIM (comprehensively described as the MICIS/COMPASS system) include the following:
- The computer hardware and software that make up the MICIS/COMPASS system
- The access and audit controls for those who use the system
- The functions and activities that are supported by the MICIS system
- The physical environment that houses MICIS/COMPASS components
- On-site and off-site storage of MICIS/COMPASS information and backups
- The organizations to which information is transmitted including the State of Michigan Medicaid Administration
- The data and information that are transmitted to other organizations
- The internal and external connections between Senior Resources and the MICIS/COMPASS system including monitoring and identifying the nature of threats or vulnerability that may damage Senior Resources’ ePHI transmissions.

ENFORCEMENT: It is the responsibility of the Security Office, HIPAA Privacy Compliance Officer/Compliance Advocate, and the Chief Executive Officer of Senior Resources to enforce this policy.

REFERENCES:
45 CFR §164.312(e)(1) http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl
POLICY: Senior Resources will perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, which establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.

Such a review process should include, but is not limited to, the following:

• A review of security incidents
• The results of any contingency plan tests or actual emergency responses.
• A review of any changes in the entity’s operating processes (e.g., staff organization or reporting) which may justify a revision in security procedures. This includes Administrative Safeguards, Organizational Requirements and Policies and Procedures affecting the security of electronic Protected Health Information (ePHI).
• A review of significant changes to the computing infrastructure (e.g., new software or a major upgrade in existing software) that might require an update to security procedures and outside review of network environment. This includes Technical Safeguards affecting the security of electronic Protected Health Information (ePHI).
• A review of changes to the physical environment (e.g., new construction or a change of location) that could impact security procedures. This includes Physical safeguards affecting the security of electronic Protected Health Information (ePHI).

ENFORCEMENT - The frequency of the evaluation process is to take place at least on an annual basis. This can be conducted by the Security Officer, the HIPAA Privacy Compliance Officer/Compliance Advocate and the Managed Care Operations Manager, and reviewed by the manager of each department, as necessary or annual. These evaluations should be made available to the Senior Resources HIPAA Officers as described in the Senior Resources HIPAA Compliance Policy.

REFERENCES
45 C.F.R. §164.308 (a)(6)(i)
http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl
45 C.F.R. §164.308 (a)(7)(i)
http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl
45 C.F.R. §164.308(a)(8)
http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl
HP.5.1 Security Administrative Requirements Policy and Procedure
Security Evaluation
SCOPE: Applies to all Senior Resources Electronic Equipment.

POLICY: It is the policy of Senior Resources to either recycle or properly dispose of electronic equipment. Senior Resources Security Officer or contracted IT specialists will implement procedures for information security in disposal and recycling of unwanted electronic equipment and implementing procedures for removal of electronic protected health information (ePHI) from electronic media before the media are made available for re-use or when equipment is donated.

PROCEDURE: To protect sensitive or ePHI data that may be stored on electronic equipment, hard drives and data storage devices must be sanitized of sensitive data prior to disposal or donated. Example of devices with hard drives include: Desktop, Laptops, Tablet Computers, Servers, Multi-Function Copiers etc.

The Security Officer or contracted IT specialists will implement procedures that require all ePHI that must be retained to be copied or moved to other secure media, before the media are made available for re-use or disposal.

1. Before any ePHI is removed, the Information Technology Department will verify that information required to be retained has been copied or moved to a secure media.
2. The Information Technology Department will document that a copy of the information and/or the move has been made.

The following steps may be used to ready media for re-use with the agency:
1. The “delete” command may be used to remove files.
2. Reformatting of the disk may be done to make files inaccessible to other users.
3. Hard Disk Drives may be “wiped” in order to remove all data from the Master Boot Record, File Allocation Tables, and Data Area.
4. For Secure Solid Drive (SSD), the Information Technology Department will use Secure Erase function that tells the SSD to flush itself, before reusing the SSD.

The following steps may be used to ready media for disposal.
1. The hard drive can be removed from the unit and stored or destroyed.
2. The hard drive may be over written to the point of preventing the recovery of the data on the device or media that is being sanitized.
3. Degauss using a magnetic field to erase the data bits stored on magnetic media.

The Security Officer or contracted IT Specialist will document all activities related to preparing electronic media for re-use or disposal.

The documentation will be maintained by the Information Technology Department and Security Officer, and retained for at least six years from the date of creation.

REFERENCES
45 C.F.R. § 164.310(d)(2)(ii) http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl,\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\",\”,}
Record of Movement of Hardware and Electronic Media

Policy: HP.7.6  
Effective Date: 10.20.15

Approved: [Signature], CEO  
Revised: 10.20.15

PURPOSE: Electronic media and equipment must often be moved due to office relocation, equipment upgrades, and other issues. The purpose of this document is to establish a standard for achieving accountability in protecting or tracking the movement of ePHI in and out of a department, as well as the movement of these items within the department.

POLICY: A paper and/or electronic log specifying the location of the device is to be maintained at all times. All Senior Resources hardware that stores or transmits electronic protected health information (ePHI) is inventoried and tracked electronically or on SR Computer Equipment FY Hardware Log, by the Senior Resources Security Officer.

PROCEDURE: The physical movement of such items is to be coordinated through the Security Officer or contracted IT Specialists. They will be responsible for maintaining a log, either electronic or paper, tracking the movement of electronic media and equipment, including software. The Senior Resources Computer Equipment Hardware Log will also identify the individuals who have access to such media and equipment once the item(s) have moved.

To facilitate the maintenance of the tracking log, all movement of media and equipment must be coordinated through the Security Officer or contracted IT Specialist.

The data and equipment are Senior Resources property and no employee is entitled to it for personal use.

If an individual moves to another position within the agency, the equipment will not move with him/her, unless explicitly approved by the supervisor, IT and HIPAA Security or Privacy Officer.

The Security Officer will create a tracking template for use across all departments. Copies of the logs must be filed with the finance office on an annual basis for audits.

REFERENCES:
45 C.F.R. 164.310(d)(2)(iii)  
http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl  
HP 6.1 Facility Access Controls Policy and Procedure  
SR Computer Hardware Log  
HP 7.5 Removal of Electronic Protected Health Information