Achieve Services, Inc.

POLICY AND PROCEDURE ON PARTICPANT DATA USE AND PRIVACY

Revised 8/14

I. POLICY

It is the policy of Achieve Services, Inc, ("Achieve") to recognize the privacy, interests, dignity, reasonable expectations and legal rights of all individuals with whom Achieve interacts. As this relates to information about Participants that is classified as "private" under State law, Achieve will maintain, use and disseminate such information in accordance with this Policy and established legal standards regarding the collection, maintenance, use and release of such information. Achieve encourages data privacy in all areas of practice and will implement measures to assure that data privacy is upheld.[1]

II. PURPOSE AND APPLICABILITY

The purpose of this Policy is to enhance the fulfillment of Achieve's mission of service, and to conform operations to the requirements of applicable laws which address the collection, content, maintenance, access to and release/disclosure of records containing information about Participants. Generally the purpose is to limit the access and use and thus protect privacy.

This policy and the related procedures apply to everyone: members of the Board of Directors, all managers, staff employees and contract vendors, i.e., all people that have access to Achieve records, and all records that personally identify any individual.

The legal standards that this Policy seeks to address are the requirements of Minn. Stat. §§13.01-13.90, 144.291-144.298, and 245D.04, subd. 3(a), and the HIPAA Privacy Rules, 45 C.F.R. Parts 160, 162 and 164, as well as other guidance and authority for these laws and regulations, and the substance and procedural requirements of related laws, i.e., reporting mandates.

III. PROCEDURES:

A. Definitions

1. Breach in the Security of Data. As used relative to the Government Data Practices Act. A breach in the Security of Data constitutes an unauthorized acquisition of data that compromises the data. A good faith acquisition of or access to the data or information by an employee, contractor, or agent of Achieve is not a breach of the security data if the data is not provided to or viewable by an unauthorized person, or accessed for a purpose not described in the Government Data Practices Act.
2. Covered Entity. As used relative to HIPAA Privacy and Security regulations, a Covered Entity is a health plan, a health care clearinghouse, or a health care provider (a person or entity who furnishes, bills, or is paid for health care in the normal course of business) who transmits any health information electronically as part of transactions described in federal regulations.
3. Employment and Training Data. As used relative to the Government Data Practices Act. Employment and Training Data are data on individuals that are enrolled in, or have been enrolled in employment and training programs funded with federal, state, or local

[1] For guidance relating to other data maintained by Achieve relating to its clients, see the applicable policies and procedures, e.g. policies relating to governance, human resources, vendors and safety.

resources. All Employment and Training Data are classified as private.

4. Health Record. As used relative to the Minnesota Health Records Act, a Health Record is any information, whether oral or recorded in any form or medium, that relates to the past, present or future physical or mental health or condition of a patient; the provision of healthcare to a patient or the past, present or future payment for the provision of health care to a patient.
5. Medical Data. As used relative to the Government Data Practices Act, Medical Data is data collected because an individual was or is a patient or client of a hospital, nursing home, medical center, clinic, health or nursing agency operated by a government entity including business and financial records, data provided by a private health care facilities, and data provided by or about relatives of the individual. All Medical Data are classifies as private.
6. Record Information about a Participant that is classified as "private: under the Government Data Practices Act. Including but not limited to a Participants Health Record. Medical Data and Employment and Training Data.
7. Participant. An individual who satisfies the eligibility requirements for services provided by Achieve and is receiving, or will receive, services provide by Achieve. *A Participant includes the Participant's legally authorized representative.*
8. Provider. A provider is a person who furnishes health care services as defined in Minn. Stat. § 144.291, and subd. 2(b).
9. Protected Health Information ("PHI"). Past, present, or future health information that is individually identifiable and is created or received by a Covered Entity in any form (oral, written, or electronic).
10. Responsible Authority. Within Achieve, the official designated as the individual responsible for the collection, use and dissemination of any set of data on individuals, government data or summary data.
11. Unauthorized Acquisition. As used relative to the Government Data Practices Act, an Unauthorized Acquisition means that a person has obtained, assessed, or viewed government data without the informed consent of the individuals who are the subjects of the data or statutory authority and with the intent to use the data for nongovernmental purposes.

B. Responsible Authority. Achieve' s Chief Executive Officer, or a person so designated by the Chief Executive Officer will act as the Responsible Authority and will be responsible for the collection, use, and dissemination of Records under this Policy. The Responsible Authority shall keep all Records in such an arrangement and condition as to make them easily accessible for convenient use, and shall also prepare as inventory of the Records in accordance with the Minnesota Government Data Practices Act.

   All board members, mangers and staff will receive training on this Policy at the inception of his or her involvement with Achieve and annually thereafter, regarding his or her responsibilities complying with this Policy and all data privacy practices at Achieve.

C. Orientation and Training. All new Achieve Participant's will complete an initial orientation at the beginning of the Participant's involvement with Achieve, and as needed thereafter. The orientation will include an explanation of this Policy and the Participant's rights regarding data privacy and the delivery to Participant of written copy of these policies and procedures which must include the reason the private data are being requested and a statement of the

consequences of not providing the requested information. The Designated Manager or Designated Coordinator at that time will keep a record of all orientations, including a record that the Participant received notification of his or her data privacy rights and that a copy of this Policy was provided to the Participant.

D. Maintenance of Participant's Records.
   1. A complete and accurate Record shall be maintained for every Achieve Participant. The Record may exist in multiple locations in both paper-based and electronic formats. The Record contents must be legible and can be maintained in either paper or electronic formats, including digital images, photographs, and films.
   2. Participants asked to supply private data for their own Record shall be informed of: (a) the purpose and intended use of the requested data; (b) whether the Participant may refuse or is legally required to supply the requested data; (c) any known consequence arising from supplying or refusing to supply private data; and (d) the identity of other persons or entities authorized by federal or State law to receive the data.
   3. The Record of the Participant, regardless of whether it was created, or received by, Achieve, including any billing information, is property of Achieve. As discussed below, the information contained within the Record must be accessible to the Participant.

E. Safekeeping of Information and Use of Flash/Thumb Drives.
   1. Safeguards to prevent loss, destruction, and tampering of Participant Records and other information will be maintained as appropriate.
   2. All Records will be kept in locked cabinets in the office area of Achieve. Records will not be removed from the program site without valid reasons, such as a court order subpoena, or as otherwise required by law. The security of the Records will be maintained at all times.
   3. The Designated Coordinator and/or Designated Manager will ensure that all information contained in the Records for Participants is safe, secure, and protected from loss or unauthorized disclosures. This includes information stored by computer for which a unique password and user identification is required.
   4. Special care will be exercised with Records and other medical data protected by federal and State laws covering mental health records and vulnerable adult maltreatment or abuse.
   5. Agency Issued Flash/Thumb Drives: Any agency issued Flash/Thumb drive must be stored in a secure location when not in use. It must be encrypted and password protected. It may NOT be used for any personal use purposes. And all files must be removed when no longer needed. Use can be revoked at the discretion of Achieve's IT staff or agency Management.
   6. Personal Flash/Thumb Drives: Personal Flash/Thumb drives may not be used on any Achieve computers or laptops and may not be used to store any Achieve information or documents.

F. Collection of Data. Achieve will give every Participant a written disclosure that details the Participant's right to request his or her own Record, as well as Achieve's duty not to disclose the Participant's Record to another party without consent, subject to certain limitations.

G. Disclosure of Records.
   1. Upon a Participant's request for his or her own Record, Achieve will provide the complete and accurate Record promptly, and at a reasonable cost, unless Achieve determines that the information will be detrimental to the Participant's physical or mental health.
   2. In order to release Record to the Participant, Achieve must obtain a signed and dated consent from the Participant authorizing the release unless an exception under applicable

federal and State law applies.

3. In order for Achieve to release a Record to another health care provider or other licensed caregiver, Achieve must obtain a written request for the release from the Participant who is the subject of the Record. The request must specify the name of the provider to whom the records are to be furnished. In limited circumstances, Achieve may release the necessary portion of the Record without the Participant's prior approval when authorized to do so under federal and State law.
4. Access to a Participant's Record is limited to authorized persons within the Achieve network. The following personnel may have immediate access to a Participant's Record and only for the relevant and necessary purposes to carry out their duties as directed by the *Coordinated Service and Support Plan* and/or the *Coordinated Service and Support Plan Addendum:*
   a) Executive staff.
   b) Administrative staff.
   c) Nursing staff including assigned or consulting nurses.
   d) Management staff including the Designated Coordinator and/or the Designated Manager.
   e) Direct Support Staff.
5. Achieve will obtain authorization to release Medical Data and other information of Participants when consultants, sub-contractors, or volunteers are working with Achieve and only to the extent needed to carry out the necessary duties.
6. The following entities also have access to a Participant's Health Record as authorized by applicable federal or State laws, regulations, or rules:
   a) Case Manager.
   b) Child or adult foster care licensor, when services are also licensed as child or adult foster care.
   c) Minnesota Department of Human Services and/or Minnesota Department of Health.
   d) County of Financial Responsibility or the County of Residence's Social Services.
   e) The Ombudsman for Mental Health or Developmental Disabilities.
   f) US Department of Health and Human Services.
   g) Social Security Administration.
   h) State departments including Department of Employment and Economic Development (DEED), Department of Education, and Department of Revenue.
   i) County, state, or federal auditors.
   j) Adult or Child Protection units and investigators.
   k) Law enforcement personnel or attorneys related to an investigation.
   l) Various county or state agencies related to funding, support, or protection of the person.
   m) Other entities or individuals authorized by law.
7. If a Record is released without a Participant's authorization as listed above, Achieve will document the release in the Participant's Record. If the release is to a law enforcement agency, the documentation will also include the date and circumstances under which the release was made, the person or agency to the release was made, and the records that were released.
8. Other entities or individuals not listed above who have obtained written authorization from the Participant may have access to written and oral information of the Participant, as detailed within that authorization. This includes other licensed caregivers or health care providers as directed by the release of information.
9. Information will be disclosed to appropriate parties in connection with an emergency if

knowledge of the information is necessary to protect the health and safety of the Participant. The Designated Coordinator and/or Designated Manager will ensure the documentation of the following on Achieve's "Incident and Emergency Report":

a) The nature of the emergency.
b) The type of information disclosed.
c) To whom the information was disclosed.
d) How the information was used to respond to the emergency.
e) When and how the person served and/or legal representative was informed of the disclosed information.

10. All authorizations or written releases of information and Records will be maintained in the Participant's individual file. In Addition, all requests made to review data, have copies, or make alterations, as stated below, will be recorded in the Participant's file including:
    a) Date and time of the activity.
    b) Who accessed or reviewed the records.
    c) If any copies were requested and provided.

H. Breach in the Security of Data

1. If there is an Unauthorized Acquisition of a Participants Record or other information that rises to a level of a Breach in the Security of Data, Achieve will provide written notification of the breach to the Participant in accordance with applicable federal and State law. Achieve will also take the following steps:
    a) Inform the participant that a report will be prepared regarding the incident and how he or she may obtain access to the report or delivery of the report by mail or email.
    b) Upon completion of an investigation into any Breach in the Security of Data, Achieve (through the Responsible Authority) will prepare a report on the facts and results of the investigation.
    c) If the breach involves unauthorized access to or acquisition of data by an employee, contractor, or agent of Achieve, the report must at a minimum include (1) a description of the type of data that were access or required; (2) the number of individuals whose data was improperly accessed; (3) the name of each employee determined to be responsible for the unauthorized access, unless the employee was performing his or her job duties; and (4) the final disposition of any disciplinary action taken against each employee in response.
    d) On an annual basis, Achieve will conduct a comprehensive security assessment of all Participants' private information.

I. Request for Alterations to Records.

1. The Participant has the right to request that his or her Record or other information and documentation be altered and to request copies of such information.
2. All objections to the accuracy of information by a Participant must be in writing and with an explanation as to why the information is incorrect or incomplete.
    a) The Designated Coordinator and/or Designated Manager will submit the written objections to the Chief Executive Officer who will make a decision in regards to any possible changes.
    b) A copy of the written objection will be retained in the Participant's file.
    c) If the objection is determined to be valid and approval for correction is obtained, the Designated Coordinator and/or Designated Manager will correct the information and notify the Participant and provide a copy of the correction. The Correction entry must be dated and signed by the person making the revision. The original entry, including an entry in electronic format, must not be obliterated, and the inaccurate

information should still be accessible.

d) If no changes are made and distribution of the disputed information is required, the Designated Coordinator and/or Designated Manager will ensure that the objection accompanies the information as distributed, either orally or in writing.

3. If there is a disagreement with the resolution of the issue, the Participant will be encouraged to follow the procedures outlined in the *Policy and Procedure on Grievances.*
4. If a member of Achieve's staff is presented with a subpoena, search warrant or other legal issues regarding the program, he or she will inform his or her immediate supervisor. The CEO or supervisor will consult with Achieve's legal advisors for assistance I responding to the request.
5. E-mail transmissions that contain private information will have an initial disclaimer message for the intended receiver, and how to respond if the message is sent in error. The actual message containing the private information will be sent as an attachment.

J. Miscellaneous.

1. Achieve will not disclose PHI about any Participant in the program when making a report to the participant and his or her case manager, unless the Participant consents to the disclosure. This nondisclosure also includes the use of other Participant information in another Participant's record.
2. Written and verbal exchanges of information regarding Participants are considered to be private and will be done in a manner that preserves confidentiality, protects their data, and respects their dignity.

Approved by the Board of Directors: September 11, 2014