HIPAA
Policies

Audrain Developmental Disability Services

HIPAA POLICIES
Notice of Privacy Practices

1. **Purpose:** This Notice of Privacy Practices (NPP) describes how health information about staff and persons served may be used and disclosed and how staff and persons served can get access to this information. Questions about this NPP should be directed to the ADDS Executive Director or a Program Coordinator in one of the ADDS Programs.

   (1) This NPP will explain:

   (1) How ADD may use and disclose Protected Health Information;

   (2) ADDS obligations related to the use and disclosure of Protected Health Information;

   (3) Individual rights related to any Protected Health Information that ADDS receives and retains.

   (2) This NPP describes how ADDS may use and disclose Protected Health Information to carry out treatment, payment and/or health care operations and for other purposes that are permitted or required by law. It also describes one's rights to access and control Protected Health Information. Protected Health Information is information about individuals, including demographics; past, present or future physical or mental health or conditions; and related health care services.

   (3) ADDS is required to abide by the terms of this NPP. A copy is available at all Programs, and at the ADDS website (www.audraindds.org). ADDS may change the terms of this NPP at any time. The new NPP will be effective for all Protected Health Information that ADDS maintains at that time.

2. **Use and Disclosure of Protected Health Information:**

   (1) Staff and individuals served may be asked to complete and sign an information form to acknowledge they have received and read this NPP.

   (2) ADDS may obtain, but is not required to, consent for the use or disclosure of Protected Health Information for treatment, payment and/or health care operations. ADDS is required to obtain authorization for the use or disclosure of information for other specific purposes or reasons. ADDS has listed some of the types of uses or disclosures in this NPP. Not every possible use or disclosure is covered, but all of the ways that ADDS is allowed to use and disclose information will fall into one of the categories.

   (3) Protected Health Information may be used and disclosed by ADDS, ADDS staff and others outside of our Agency that are involved in care and treatment for the purpose of providing health care services to staff or person served. Protected Health Information may also be used and disclosed to pay health

care bills and to support the operations of ADDS.

(4) Following are examples of the types of uses and disclosures of Protected Health Information that ADDS is permitted to make.

(1) **Treatment:** ADDS will use and disclose Protected Health Information to provide, coordinate, or manage health care and any related services. This includes the coordination or management of Protected Health Information with a third party that has already obtained permission to have access to Protected Health Information. For example, ADDS would disclose Protected Health Information, as necessary, to a home health agency that provides care to an individual. ADDS will also disclose Protected Health Information to other providers or health facilities that may treat individuals when it has the necessary permission from said individuals to disclose their Protected Health Information. For example, Protected Health Information may be provided to a health provider to whom an individual has been referred to ensure that the provider has the necessary Protected Health Information for diagnosis and treatment. In addition, ADDS may disclose Protected Health Information from time-to-time to another health care provider (e.g., a specialist or laboratory) who, at the request of an individual's provider, becomes involved in their care by providing assistance with their health care diagnosis or treatment.

(2) **Payment:** Protected Health Information will be used, as needed, to obtain payment for an individual's health care services. This may include certain activities that a health insurance plan may undertake before it approves or pays for the health care services recommended, such as: making a determination of eligibility or coverage for insurance benefits; reviewing services provided for medical necessity; and undertaking utilization review activities. For example, ADDS may need to provide an insurance plan information about treatment received so that the insurance will pay for the services.

(3) **Operations:** ADDS may use or disclose, as needed, Protected Health Information in order to support the business activities of ADDS. These activities include, but are not limited to: quality assessment activities; licensing; and employee review activities. In addition, ADDS may use a sign-in sheet at the registration desk where visitors will be asked to sign their name. ADDS may also call individuals by name in a lobby when a provider is ready to see them. ADDS may use or disclose Protected Health Information, as necessary, to contact individuals to remind them of their appointment. ADDS will share Protected Health Information with third party "business associates" that perform various activities (e.g., billing, reading of x-rays, performing lab tests, transcription services). Whenever an arrangement between our office and a business associate involves the use or disclosure of Protected Health Information, ADDS will have a written contract that contains terms that will protect the privacy of Protected Health Information.

3. **Written Authorization:**

(1) Other uses and disclosures of Protected Health Information will be made only with an individual's written authorization, unless otherwise permitted or required by law as described below. Individuals may revoke this authorization, at any time, in writing, except to the extent that their provider has taken an action in reliance on the use or disclosure indicated in the authorization.

(2) **Research:** To comply with laws and regulations other than HIPAA, ADDS will not allow Protected Health Information collected by their staff, to be used in research projects without individuals' written consent. Under certain circumstances, ADDS may use and disclose Protected Health Information for research purposes when the Institutional Review Board has approved a waiver of authorization for the Protection of Human Subjects. For example, a research project may involve comparing the health and recovery of all persons served who received one medication to those who received another for the same condition. All research projects, however, are subject to a special approval process under Missouri law. This process evaluates a proposed research project and its use of health information, trying to balance the research needs with the individual's need for privacy of their health information. Before we use or disclose Protected Health Information for research, the project will have been approved through this research approval process. ADDS may, however, disclose Protected Health Information to people preparing to conduct a research project, for example, to help them look for persons served with specific medical needs, so long as the health information they review does not leave the facility.

4. **No Consent Required:**

(1) ADDS can use or disclose Protected Health Information about individuals without consent or authorization when:

(1) There is an emergency or when ADDS is required by law to treat an individual;

(2) When ADDS is required by law to use or disclose certain information; or

(3) When there are substantial communication barriers to obtaining consent.

(2) ADDS can also use or disclose Protected Health Information without consent or authorization for:

(1) **Appointment Reminders:** ADDS may use and disclose Protected Health Information to contact individuals to reminder them about appointments for treatment or services at the Agency.

(2) **Treatment Alternatives and Health-Related Benefits and Services:** ADDS may use and disclose Protected Health Information to tell individuals about or recommend possible treatment options or alternatives or health-related benefits or services that may be of interest.

(3) **Individuals Involved in Disaster Relief:** Should a disaster occur, ADDS may disclose Protected Health Information about individuals to any agency assisting in a disaster relief effort so that family can be notified about an individual's condition, status or location.

(4) **As Required By Law:** ADDS will disclose Protected Health Information when required by law.

(5) **To Avert a Serious Threat to Health or Safety:** ADDS may use and disclose Protected Health Information when necessary to prevent a serious threat to the health and safety of staff, persons served, the public, or any other person. However, any such disclosure would only be to

someone who is able to help prevent the threat.

(6) **Organ and Tissue Donation:** If an individual is an organ donor, ADDS may release Protected Health Information to organizations that handle organ procurement or organ, eye or tissue transplantation or to an organ donation bank, as necessary to facilitate organ or tissue donation and transplantation.

(7) **Military and Veterans:** If an individual is a member of the armed forces, ADDS may release Protected Health Information about them as required by military command authorities. ADDS may also release Protected Health Information about foreign military personnel to the appropriate foreign military authority.

(8) **Workers' Compensation:** ADDS may release Protected Health Information to comply with workers' compensation or similar programs. These programs provide benefits for work-related injuries or illnesses.

(9) **Public Health Risks:** ADDS may disclose Protected Health Information for public health activities. These activities generally include the following: to prevent or control disease, injury or disability; to report births and deaths; to report child abuse or neglect; to report reactions to medications or problems with products; to notify people of recalls of products they may be using; to notify a person who may have been exposed to a disease or may be at risk for contracting or spreading a disease or condition; or to notify the appropriate government authority if we believe a person served has been the victim of abuse, neglect or domestic violence. However, ADDS will only make this disclosure by agreement of the individual or when required or authorized by law.

(10) **Health Oversight Activities:** ADDS may disclose Protected Health Information to a health oversight agency for activities authorized by law. These oversight activities include, for example, audits, investigations, inspections, and licensure. These activities are necessary for the government to monitor the health care system, government programs, and compliance with civil rights laws.

(11) **Lawsuits and Disputes:** If an individual is involved in a lawsuit or a dispute, ADDS may disclose Protected Health Information in response to a court or administrative order as required by law.

(12) **Law Enforcement:** ADDS may release Protected Health Information if asked to do so by a law enforcement official; however, if the material is protected by 42 CFR Part 2 (a federal law protecting the confidentiality of drug and alcohol abuse treatment records), a court order is required. ADDS may also release limited Protected Health Information to law enforcement in the following situations: 1) about a person served who may be a victim of a crime if, under certain limited circumstances, ADDS is unable to obtain the agreement of the person served; 2) about a death ADDS believes may be the result of criminal conduct; 3) about criminal conduct at the ADDS; 4) about a person served where a person served commits or threatens to commit a crime on the premises or against program staff (in which case ADDS may release the person served's name,

address, and last known whereabouts); 5) in emergency circumstances, to report a crime, the location of the crime or victims, and the identity, description and/or location of the person who committed the crime; and 6) when a person served is a forensic client and ADDS is required to share with law enforcement by Missouri statute.

(13) **Coroners, Medical Examiners and Funeral Directors:** ADDS may release Protected Health Information to a coroner or medical examiner. This may be necessary, for example, to identify a deceased person or determine the cause of death. ADDS may also release Protected Health Information about persons served of the ADDS facilities to funeral directors as necessary to carry out their duties.

(14) **National Security and Intelligence Activities:** ADDS may release Protected Health Information to authorized federal officials for intelligence, counterintelligence, and other national security activities authorized by law.

(15) **Protective Services for the President and Others:** ADDS may disclose Protected Health Information to authorized federal officials so they may conduct special investigations or provide protection to the President of the United States and other authorized persons or foreign heads of state.

(16) **Inmates:** If an individual is an inmate of a correctional institution or under the custody of a law enforcement official, Protected Health Information may be released to the correctional institution or law enforcement official if the release is necessary for 1) the institution to provide health care; 2) to protect an individual's health and safety or the health and safety of others; or 3) the safety and security of the correctional institution.

5. **Other Uses or Disclosures:** Other uses or disclosures not covered in this NPP will not be made without written authorization, unless otherwise permitted or required by law. Individuals who provide ADDS with written authorization to use or disclose information may change their mind and revoke authorization at any time, as long as it is in writing. If authorization is revoked, ADDS will no longer use or disclose the information. However, ADDS will not be able to take back any disclosures that have been made pursuant to the previous authorization.

6. **Individual Rights:** Individuals have the following rights regarding Protected Health Information maintained by ADDS:

1.1. **Right to Inspect and Copy:** Individuals have the right to inspect and receive a copy of their Protected Health Information with the exception of psychotherapy notes and information compiled in anticipation of litigation. To inspect and receive a copy of one's Protected Health Information, a request in writing must be made to the ADDS Executive Director or designee. ADDS may charge a fee for the costs of copying, mailing or other supplies associated with the request. ADDS may deny a request to inspect and copy Protected Health Information in certain limited circumstances. If denied access to Protected Health Information because of a threat or harm issue, an individual may request that the denial be reviewed. Another licensed health care professional chosen by ADDS will review the request and the denial. The person conducting the review will not be the person who denied the

original request. ADDS will comply with the outcome of the review.

1.2. **Right to Request an Amendment:** Anyone who feels that their Protected Health Information is incorrect or incomplete may ask to have their information amended. They have the right to request an amendment for as long as the information is kept by or for ADDS. Requests for an amendment must be made in writing and submitted to the Executive Director or designee. A reason to support the request for an amendment must be provided. ADDS may deny the request if it is not in writing or if it does not include a reason supporting the request. In addition, ADDS may deny the request if it seeks to amend information that:

(1) Was not created by ADDS, unless the person or entity that created the information is no longer available to make the amendment;

(2) Is not part of the Protected Health Information kept by or for ADDS;

(3) Is not part of the information which one would be permitted to inspect and copy or;

(4) Is accurate and complete.

1.3. **Right to an Accounting of Disclosures:** Anyone has the right to request an "accounting of disclosures," a list of the disclosures made by ADDS of one's Protected Health Information. To request an accounting of disclosures, individuals must submit their request in writing to the ADDS Executive Director or designee. The request must state a time period which may not go back more than six years and cannot include dates before April 14, 2003. The request should indicate in what form the list is wanted (for example, on paper or electronically). The first list requested within a twelve-month period will be free. For additional lists in a twelve-month period, ADDS may charge for the cost of providing the list. ADDS will notify the requestor of the cost and the opportunity to withdraw or modify the request before being charged. There are some disclosures that ADDS does not have to track. For example, when ADDS is given an authorization to disclose some information, ADDS is not required to track that disclosure.

1.4. **Right to Request Restrictions:** You have the right to request a restriction or limitation on the Protected Health Information ADDS uses or discloses about you for treatment, payment and/or health care operations. For example, you could ask that ADDS not use or disclose information about your family history to a particular community provider. ADDS is not required to agree to your request. If ADDS does agree, it will comply with your request unless the information is needed to provide you emergency treatment. To request restrictions on the use or disclosure of your Protected Health Information for treatment, payment or health care operations, you must make your request in writing to ADDS' Privacy Officer or designee. In your request, you must tell ADDS (1) what information you want to limit; (2) whether you want to limit our use, disclosure or both; and (3) to whom you want the limits to apply (for example, disclosures to your spouse).

1.5. **Right to Request Confidential Communications:** You have the right to request that ADDS communicate with you about medical matters in a certain way or at a certain location. For example, you can ask that that ADDS only contact you at work or by mail. To request confidential communications, you must make your request in writing to the ADDS Privacy Officer or designee.

Your request must specify how or where you wish to be contacted. ADDS will not ask you the reason for your request and will accommodate all reasonable requests.

1.6. **Right to a Paper Copy of This Notice:** You have the right to a paper copy of this notice even if you have agreed to receive the notice electronically. You may ask ADDS to give you a copy of this notice at any time by contacting the ADDS Privacy Officer or designee.

2. **Changes to This Notice:** ADDS reserves the right to change this NPP. ADDS may make the revised notice effective for Protected Health Information ADDS already has about you as well as any information ADDS receives in the future. ADDS will post a copy of the current NPP in all Facilities. The NPP will contain on the first page, in the top right-hand corner, the effective date. In addition, each time you register at or are admitted or apply for services to ADDSfor treatment and/or services, you will be offered a copy of the current NPP in effect. If you want to request any revised NPP, you may contact the Executive Director or Privacy Officer.

3. **Complaints:** If you believe your privacy rights have been violated you may:

3.1. File a complaint with ADDS by contacting its Executive Director or Privacy Officer by dialing the ADDS' main number 573-581-8210 or mailing to Audrain Developmental Disability Services, Inc., 222 E. Liberty St., Mexico, Missouri 65265.

3.2. File a grievance with the Office of Civil Rights by calling 866-OCR-PRIV (866-627-7748), or 886-788-4989 TTY.

3.3. All complaints must be submitted in writing. You will not be penalized for filing a complaint.

ACKNOWLEDGEMENT NOTICE OF PRIVACY PRACTICES

I,_____(Person served) hereby acknowledge that I have received the Notice of Privacy Practices.

_____ _____

Person served or Legal Guardian or Parent of Minor Child Signature

Date Signed

HIPAA POLICY

1. The purpose of this policy is to describe mandatory training as required by the Health Insurance Portability and Accountability Act (HIPAA).

2. All employees of ADDS shall attend training on the privacy and security provisions of HIPAA.

3. HIPAA training curriculum must remain consistent agency-wide to assure appropriate implementation of the HIPAA Privacy and Security regulations. To maintain that important consistency, no local customization at a facility level shall be permitted. Any variation in content may be subject to the sanctions provision.

    3.1. Mandatory privacy training shall be scheduled whenever there is a material change in ADDS' privacy policies or procedures as determined by ADDS management and Security Officer.

    3.2. Periodic mandatory security training shall be scheduled as determined by the Security Officer.

4. Unless otherwise noted, ADDS employees shall receive HIPAA training as part of their initial employee orientation with annual reviews.

5. Documentation of mandatory HIPAA training shall be recorded and placed in employee's file.

HIPAA POLICY

1. Individual Access to Health Information:

1.1. **Purpose:** It is the policy of the Audrain Developmental Disability Services, Inc., (ADDS) to protect the privacy of individually identifiable Protected Health Information in compliance with federal and state laws governing the use and disclosure of Protected Health Information (PHI). ADDS recognizes the rights of individuals to access PHI pertaining to them in a designated record set as set forth in 45 CFR Section 164.524. ADDS further recognizes that access to PHI may be limited or restricted as defined in this policy, in the Notice of Privacy Practices ("NPP") and as allowed by law. In cases where the individual has been civilly adjudicated incapacitated or is a minor, the parent (if a minor), or the legal guardian or personal representative may request access. There may be additional exceptions as allowed by law.

1.2. **Application:** ADDS

(1) Definitions
(2) Request for Access to Protected Health Information
(3) Denial of Access
(4) Appeal and Review of Denial
(5) Release of Protected Health Information of a Deceased Individual
(6) Provision of Access and Fees
(7) Review Process
(8) Sanctions

1.3. **Definitions:**

(1) **Abstract (Summary):** A brief summary on ADDS letterhead of the essential information as requested on a proper authorization

(2) **Person Served/Individual:** Any individual who has received or is receiving services from an ADDS program. Person Served can also indicate Personal Representative if Person Served has a Personal Representative.

(3) **Designated record set:** A group of any records under the control of a covered entity from which Protected Health Information (PHI) is retrieved by the name of the individual or by identifying number.

(4) **Direct Access:** An in-person review of the medical record, and/or obtaining a copy of the record.

(5) **Licensed Health Care Professional:** As defined in Section 630.005, RSMO; 9 CSR 30-4.010; and 9 CSR 45-2.010(2)(U). Such professionals may be a licensed physician, nurse, therapist,

counselor, speech pathologist, nurse practitioner, audiologist, athletic trainer, physical therapist, physician assistant, social worker, pharmacist, and other licensed health care specialist.

(6) **Personal Representative:** Person with a court order appointing them as guardian or with a valid Power of Attorney signed by the person served specifying the authority to review and make decisions regarding medical, psychiatric, therapy treatment or habilitation counseling concerns.

(7) **Protected Health Information(PHI):** Defined as any information, including demographic information, collected from an individual that is created or received by a healthcare provider, health prescription plan, employer, or healthcare and pharmacy clearinghouse; and is related to the past, present, or future physical or mental health or condition of an individual, the provision of healthcare to an individual, or the past, present, or future payment for the provision of healthcare to an individual; and which identifies the individual; or with respect to which, there is reasonable basis to believe that the information can be used to identify the individual.

(8) **Psychotherapy Notes:** 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. Such notes exclude medication prescriptions 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.

(9) **Official Signature:** Legal Name, credential, and job title or position description.

(10) **Disclosure of Protected Health Information Summary:** An accounting of disclosures of Protected Health Information (in paper or electronic format) containing: date of disclosure; name and address of the organization or person who received the Protected Health Information; a brief description of the information disclosed; purpose for which the Protected Health Information was disclosed.

(11) **Program Coordinator:** The individual who is responsible for the Program where records of the person served are kept or maintained in any form or format. The Business Manager shall be the Agency Privacy Officer for the purposes of this Policy.

1.4. Request for Access to Protected Health Information (PHI):

(1) A person served who has or is receiving services from ADDS, parent of a minor, and personal representative or legal guardian as relevant to their representation, must request in writing for access to inspect, or receive copies of, Protected Health Information except in those instances covered by federal regulations and outlined in the NPP acknowledged at admission, and must further specify the exact information requested for access. This does not mean that ADDS cannot give a person served, a copy of their test results, preventive measures, care instructions,

or information to assist the understanding of the person served regarding their diagnosis, during the delivery of health care without a written release.

(2) The "Access Request Form for Protected Health Information" shall be provided to facilitate the request. ADDS personnel may assist in initiating the process requesting access to Protected Health Information.

(3) All requests by persons served and their legal representatives for Protected Health Information must be forwarded to the Program Coordinator or Agency Privacy Officer for action.

(4) If it is acceptable after discussion with the person served, ADDS may provide a summary of the Protected Health Information to the person served. If the summary is acceptable, ADDS shall determine the appropriate staff to provide that explanation to the person served. The agreement of the person served to a summary shall be documented in writing in the record as a check in the appropriate box in the "Access Request Form for Protected Health Information" form. The agreement of the person served to any costs associated with the summary shall be documented in the record. The form shall be filed in the record of the person served.

(5) This request shall be processed in a timely consistent manner according to established time frames but not more than thirty (30) days after receipt of the request. If the record cannot be accessed within the thirty (30) days, the time frame may be extended once for no more than an additional thirty (30) days with notification in writing to the individual outlining reasons for the delay and the date the request will be concluded.

(6) Requests for Access to Protected Health Information may be denied without a right to review as follows:

- If the information conforms to one of the following categories: psychotherapy notes; HIV testing information; information compiled for use in a civil, criminal or administrative action or proceeding; or information that would be prohibited from use or disclosure under the Certified Laboratory Information Act (CLIA) laws and regulations;
- If the person served is participating in research related treatment and has agreed to the denial of access to records for the duration of the study;
- If access is otherwise precluded by law;
- If the information was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.
- If the facility has been provided a copy of a court order from a court of competent jurisdiction, which limits the release, or use of Protected Health Information.

(7) Requests for Access to Protected Health Information may be denied provided the individual is given a right to have the denial reviewed as follows:

- A licensed health care professional based on an assessment of the particular circumstances, determines that the access requested is reasonably likely to endanger the life or physical

safety of the person served or another person.

- ADDS may deny the person served access to Protected Health Information if the information requested makes reference to someone other than the person served and a health care professional has determined that the access requested is reasonably likely to cause serious harm to that other person.
- ADDS may deny a request to receive a copy or inspect Protected Health Information by a personal representative of the person served if ADDS has a reasonable belief that the person served has been or may be subjected to domestic violence, abuse, or neglect by such person; or treating such person as the personal representative could endanger the individual; and the facility, exercising professional judgment, decides that it is not in the best interest of the person served to treat that person as the patient's personal representative.

1.5. **Denial of Access:**

(1) Upon denial of any request for access to Protected Health Information, in whole or in part, a written letter shall be sent to the person served, or other valid representative making the request for access, stating in plain language the basis for the denial.

(2) If the person served has a right to a review of the denial as outlined in subsection 3.g. above, the letter shall contain a statement of how to make an appeal of the denial including the name, title, address, and telephone number of the person to whom an appeal should be addressed.

(3) This letter shall also address the steps to file a complaint with the Secretary of HHS.

(4) If ADDS does not maintain the information requested, but it is known where the person served may obtain access, ADDS must inform the person served where to direct the request for access. The person served is to have access to records from another facility that are maintained in the current facility's record.

1.6. **Appeal and Review of Denial of Requests** as Defined in Subsection 3.g:

(1) A person served, parent of a minor, or guardian of a person served has the right to appeal the decision to withhold portions or all of the record for safety or confidentiality reasons.

(2) The appeal shall be submitted in writing to the Executive Director of ADDS who will designate a licensed health care professional, or if the appeal is to the ADDS's Privacy Officer concerning any information maintained by a ADDS, then to a designated licensed health care professional.

(3) The designated licensed health care professional who did not participate in the original decision to deny access shall review the record and the request for access to the record of the person served. (Form attached to this policy)

(4) The reviewer must determine if access meets an exception as described in Section 3 above.

(5) If the reviewer determines that the initial denial was appropriate, the person served must be

notified in writing, using plain language, that the review resulted in another denial of access. The notice must include the reasons for denial and must describe the process to make a complaint to the Secretary of HHS.

(6) If the denial was not appropriate, the licensed health care professional who acts as the reviewer shall refer the request to ADDS or ADDS' Privacy Officer or designee for action.

(7) If access is denied to any portion of the Protected Health Information, access must still be granted to those portions of the Protected Health Information that are not restricted.

(8) ADDS is bound by the decision of the reviewer.

1.7. **Release of Protected Health Information of a Deceased Person served:**

(1) The Protected Health Information of a deceased person served may only be released via a Probate Court order from the County Circuit Court where the deceased resided or from another Probate Court in the State of Missouri, or as otherwise determined legally appropriate by ADDS' legal counsel.

(2) Upon request to obtain information, the Privacy Officer or designee shall ask for a copy of the Probate Court Order or other necessary documentation.

1.8. **Provision of Access and Fees:**

(1) If ADDS provides a person served or legal representative with access, in whole or in part, to Protected Health Information, the ADDS must comply with the specifications as outlined in federal regulations to the extent of ADDS' capabilities and as identified in ADDS' Notice of Privacy Practices.

(2) Requested information must be provided in designated record sets.

(3) If the requested information is maintained in more than one designated record set or in more than one location, ADDS only needs to produce the information one time in response to the request.

(4) ADDS may provide a summary or explanation of the requested Protected Health Information if:

(5) The person served agrees in advance to the summary or explanation in place of the record.

(6) The person served agrees in advance to any fees imposed for the summary or explanation.

(7) These agreements shall be documented as set forth in subsection 3.d. above.

(8) If the requested information is maintained electronically and the person served requests a copy or faxed copy, ADDS should accommodate the request if possible and explain the risk to security

of the information when transmitted as requested.

(9) If the information is downloaded to computer disk, the person served should be advised in advance of any charges for the disk and mailing the disk.

(10) If the information is not available in the format requested, ADDS must produce a hard copy document or other format agreed upon by the person served and facility.

(11) ADDS shall provide the access requested in a timely manner and arrange for a mutually convenient time and place for the person served to inspect the Protected Health Information or obtain copies, unless access by another method has been requested by the person served and agreed to by ADDS as set forth in subsection 6.a.(4) above. Any requests for accommodations shall be sent or given in writing to the Privacy Officer or designee.

(12) The fee charged will be in compliance with the current Missouri State Statute (See Section 191.227, RSMO), the ADDS's Open Meetings and Records Policy, and federal law.

1.9. **Review Process:** The ADDS Privacy Officer will collect information from the Program Coordinators during the month of April each year beginning in 2014 for the purpose of providing feedback to the HIPAA Management Team as to compliance with the procedure and any proposed modification or recommendation that additional training be implemented.

1.10. **Sanctions:** Any person found to have violated the requirements of this policy shall be subject to disciplinary action up to and including dismissal.

2. ADDS Access to Health Information:

2.1. **Purpose:** It is the policy of ADDS to protect the privacy of individually identifiable health information in compliance with federal law. To assist in assuring that protection, it is the practice of ADDS to assure that its workforce recognize the importance of such confidentiality provisions, and affirmatively acknowledge those guidelines. See 45 CFR Sections 160 and 164, et seq.

2.2. **Application:** Contents

(1) Definitions
(2) Staff Access
(3) Training on Access
(4) Required Confidentiality Agreement
(5) Visitors

2.3. **Definitions:**

(1) **Protected Health Information (PHI):** Defined as any information, including demographic information collected from an individual that is created or received by a healthcare provider, health plan, employer, pharmacy, prescription, or healthcare clearinghouse; and is

related to the past, present, or future physical or mental health or condition of an individual, the provision of healthcare to an individual, or the past, present, or future payment for the provision of healthcare to an individual; and identifies the individual; or with respect to which, there is reasonable basis to believe that the information can be used to identify the individual.

(2) **Workforce:** Includes employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity (facility or Department). This shall include any client workers employed by the ADDS 45 CFR Section 160.103.

2.4. **Staff Access** (Any Person with Access to Protected Health Information):

(1) ADDS workforce members shall be granted access to protected health information (Protected Health Information), whether written, electronic or verbal in nature, in accordance with state and federal law (HIPAA, P.L. 104-191); (42 CFR Part 2 et seq.; Privacy 45 CFR Parts 160 and 164); and other relevant regulations. Such access shall be limited to the minimum necessary amount of Protected Health Information to accomplish the purpose of any requested use or disclosure of Protected Health Information, e.g., to the amount of Protected Health Information the employee or workforce member needs to know in order to accomplish their job or task. In addition, communications between workforce members, which involve Protected Health Information, shall also be considered confidential and should not take place in public areas. If it is absolutely necessary to conduct such conversations in public areas, reasonable steps shall be taken to assure the confidentiality of the Protected Health Information.

(2) Protected Health Information should never be removed from ADDS without specific authorization from the Program Coordinator, pursuant to a signed Business Associate Agreement, or the appropriate medical records personnel. ADDS shall establish a procedure for how workforce members are to physically access Protected Health Information in medical records (i.e., how to sign records in and out and under what conditions, etc.)

(3) If Protected Health Information in any form is lost or stolen, the Program Coordinator and the Privacy Officer should be notified as soon as practical, but no later than two (2) business days after the loss is discovered, in order for the Privacy Officer or designee to initiate the mitigation process.

2.5. **Training:** ADDS workforce members shall be informed of their obligations with respect to Protected Health Information by mandatory participation in HIPAA Privacy Training.

2.6. **Required Confidentiality Agreement:** ADDS workforce members that receive or maintain Protected Health Information shall be required to agree to the protection of such Protected Health Information in accordance with the state and federal laws as set forth above. These workforce members shall sign a confidentiality statement. The model statement is attached as HIPAA Regulation 8.040, Form 1. A copy of the signed confidentiality statement shall be maintained in the personnel file of ADDS.

2.7. **Visitors:** Visitors to all facilities are required to sign the confidentiality agreement if they are going to have access to Protected Health Information. A copy of the confidentiality agreement shall be located in each facility.

3. Obtaining Disclosure:

3.1. **Purpose:** It is the policy of ADDS to protect the privacy of individually identifiable health information in compliance with federal and state laws governing the use and disclosure of Protected Health Information (PHI) and confidentiality. It is also the policy of ADDS to provide for the person served's voluntary authorization for use or disclosure of his or her protected health information (Protected Health Information) as set out in 45 CFR Sections 164.508; 164.510; and 164.512. Whether Protected Health Information may be used or disclosed is subject to the review of the Executive Director, Program Coordinator, or designee.

3.2. **Application:** Contents

(1) Definitions
(2) Procedure

3.3. **Definitions:**

(1) **Person Served:** any individual who has received or is receiving services from ADDS. Person Served can also indicate Personal Representative if Person Served has a Personal Representative

(2) **Disclosure:** the release, transfer, provision of access to, or divulging in any other manner of information outside ADDS.

(3) **Psychotherapy notes:** 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 patient's medical record. Such notes exclude 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 notes to date.

(4) **Protected Health Information:** As defined in HIPAA Procedure 1.005,1.b.and c., and includes:

- Names
- All geographies smaller than a state, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census; the geographic unit formed by combining all zip codes with the same three initial digits contains more that 20,000 people; and the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000
- Dates (other than year) directly related to an individual
- Phone numbers

- Fax numbers
- Email addresses
- Social Security numbers
- Medical record numbers
- Health insurance beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web Uniform Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers including finer, retinal and voice prints
- Full face photographic images and any comparable images
- Any other unique identifying number, characteristic, or code except the unique code assigned by the investigator to code the data

3.4. **Procedure:**

(1) ADDS may not use or disclose Protected Health Information without a valid authorization completed by the person served, or applicable personal representative, with limited exceptions. The standard authorization form is attached. The Program Coordinator should obtain written information regarding the identity of the requestor, the date of the request, the nature and purpose of the request and any authority that the requestor has to request such information, consistent with Verification Procedures. If other staff receives a completed authorization form for the release of Protected Health Information, they shall direct it to the Program Coordinator, Executive Director, or representative for review.

(2) Any disclosures that occur shall be limited to the minimum amount of information necessary to meet the purpose of the use or disclosure.

(3) Exceptions to the minimum necessary requirement are as follows:

- When the person served or applicable personal representative authorizes the disclosure;
- Disclosures required by law.

(4) ADDS must obtain an authorization for any use or disclosure or psychotherapy notes except:

- To carry out treatment, payment or health care operations;
- For ADDS to use in defending itself in litigation or other proceedings brought by the patient.

(5) Protected Health Information may only be disclosed without authorization in the following situations unless authorized by the NPP and HIPAA Procedure 1.005:

- To a public health authority (e.g., required reporting to the Missouri Department of Health and Senior Services, FDA, communicable diseases), per § 164.512(b);

- To report child abuse/neglect situations, and other situations involving abuse, neglect or domestic violence (if disclosure is allowed by law), per § 164.512(c);
- To a health oversight agency, per § 164.512(d);
- In response to order of judicial or administrative tribunal (or a subpoena or discovery request if satisfactory assurances of notice to the individual pursuant to § 164.512(e));
- To law enforcement (but only in certain circumstances; including when they present a grand jury subpoena; information concerning forensic clients; to locate a missing person, suspect, or fugitive; or at the discretion of the Director of the Home when the information is requested to assist law enforcement in their investigation, per § 164.512(f));
- To medical examiners, coroners and funeral directors, per § 164.512(g);
- For organ donation, per § 164.512(h);
- For research purposes, per § 164.512(I) and policy 8.055;
- To avert a serious threat to health or safety, per § 164.512(j);
- Governmental functions (such as national security, veterans information, eligibility for public assistance programs), per § 164.512(k);
- To comply with worker's compensation laws, per § 164.512(l);
- As required by law, per § 164.512(a).

(6) Any questions as to whether a use or disclosure is permitted or required by law should be directed to the ADDS Privacy Officer and/or ADDS legal counsel.

(7) If it is ADDS that requests that the person served to complete the Authorization, ADDS must provide the person served with a copy of the signed authorization.

4. Accounting of Disclosures:

4.1. **Purpose:** It is the policy of the ADDS to abide by the Health Insurance Portability and Accountability Act (HIPAA), Public Law 104-191, standards for privacy of individually identifiable health information. A person served has the right to receive a written Accounting of Disclosures of their protected health information (Protected Health Information) made by the UHF in the six years prior to the date of which the accounting is requested. (45 CFR § 164.528). A person served may request an accounting of a period of time less than six years. Beginning on April 14, 2003, a person served is only entitled to request an Accounting of Disclosures from April 14, 2003 to the current date. After April 14, 2009, a person served is entitled to request a full six years' worth of disclosures.

4.2. **Application**: The ADDS and workforce

(1) Definitions
(2) Procedure

4.3. **Definitions:**

(1) **Person served:** any individual who has received or is receiving services from ADDS. Person Served can also indicate Personal Representative if Person Served has a Personal Representative.
(2) **Disclosure:** Disclosure is defined as, "the release, transfer, provision of access to, or divulging

in any other manner of information outside the entity which holds the information." This includes disclosures to or by business associates of the covered entity.

(3) **Individually Identifiable Health Information:** any information, including demographic information, collected from an individual that is created or received by a healthcare provider, health plan, employer, healthcare clearinghouse or pharmacy clearinghouse; and is related to the past, present, or future physical or mental health or condition of an individual, the provision of healthcare to an individual, or the past, present, or future payment for the provision of healthcare to an individual; and identifies the individual; or with respect to which, there is reasonable basis to believe that the information can be used to identify the individual.

(4) **Protected Health Information:** Defined as, "individually identifiable health information that is (I) transmitted by electronic media; (ii) maintained in any medium described in the definition of electronic media; or (iii) transmitted or maintained in any other form or medium"

4.4. **Procedure:**

(1) All disclosures of Protected Health Information need to be accounted for upon the request of the individual. This is not limited to hard copy information but any manner of communication that discloses information, including verbal release. However, the following list of exceptions to this requirement do not require tracking or need to be accounted for upon the request of the individual:

- Disclosures made for treatment, payment, and healthcare operation purposes as set out in 45 CFR§164.502.
- Disclosures made to the patient. (45 CFR §164.502)
- Disclosures made for facility directory purposes, if utilized (45 CF§164.510). (Please note that ADDS will not utilize a facility directory as defined under HIPAA without ADDS Privacy Officer approval).
- Disclosures made for national security or intelligence purposes. (45 CFR §164.512 (K) (5)).
- Disclosures made to correctional institutions or law enforcement officials related to health or safety of an inmate or other person. (45 CFR § 164.512(k)(5)).
- Disclosures made prior to the date of compliance with the privacy standards, meaning prior to April 14, 2003.

(2) There are further exceptions for disclosures to health oversight agencies (see section 164.528 (a)(2)(I) et seq.). Please contact the Executive Director or Privacy Officer should this situation arise. ADDS Privacy Officer and Executive Director shall assure that a mechanism is in place which tracks disclosure of Protected Health Information. One format shall be utilized for all ADDS programs. See HIPAA Procedure 1.060, Form 2.

(3) ADDS will include the following required content in the Accounting of Disclosures:

- The name and identification number of the person served whose Protected Health Information was disclosed.

- Date of disclosure
- Name and address, if known, of the entity or person who received the Protected Health Information
- Brief description of the Protected Health Information disclosed
- Brief statement of purpose that reasonably informs the person served of the purpose for the disclosure, or provide the persons served with a copy of the authorization, or provide the patient with a copy of the written request for disclosure.

(4) If multiple disclosures are made to the same entity or person for the same reason, it is not necessary to document items 4.a.-d. for each disclosure. ADDS may document instead the first disclosure, the frequency or number of disclosures made during the accounting period, and the date of the last disclosure in the accounting period.

(5) The person served (or legal guardian) must make a written request for an Accounting of Disclosures to the ADDS or Home Privacy Officer, or designee, (whichever is applicable). The request shall be on the HIPAA Procedure 1.060, Form 1, as attached to this policy. Staff may assist the person served in completing the form if requested to do so.

(6) ADDS has sixty (60) days after receipt of the request for such an accounting to respond to the request for an accounting of disclosure. If ADDS has disclosed information to a business associate regarding the person served requesting the accounting, then ADD through its Privacy Officer or designee must request an accounting of disclosures of that person served's information from that business associate, who has twenty (20) calendar days to provide the accounting. ADDS may request one 30-day extension, which is allowed, but the person served must be informed in writing of the delay:

- The reason for the delay,
- The date the accounting will be provided, and
- Such notification to the person served or person requesting the accounting of disclosures of any delay must take place within the 60-day time frame.

(7) ADDS must provide the first accounting of disclosures free of charge in any 12-month period. Any subsequent request can be charged based on Missouri Statute (RSMO Section 191.227, § 610.010 et seq.). Before charging a fee, ADDS must inform the person served and allow the opportunity to withdraw or modify the request to avoid or reduce the fee. No additional handling fee is allowed.

(8) ADDS must retain a copy of the written accounting that is provided to the patient in the patient's medical record.

5. Ensuring Confidentiality:

5.1. **Purpose:** In compliance with the Health Insurance Portability and Accountability Act of 1996 (45 CFR Sections 164 et seq.), it is the policy of ADDS to provide procedures for best practices for employees, and clients to utilize in the field when traveling outside the ADDS. These procedures are

to protect the privacy of Protected Health Information (Protected Health Information) of consumers in compliance with federal and state laws governing the use and disclosure of such Protected Health Information.

5.2. **Application:** ADDS and workforce.

(1) Definitions
(2) Protected Health Information: Unattended
(3) Protected Health Information: Within View
(4) Protected Health Information: Faxing

5.3. **Definitions:**

(1) **Authorized Persons:** those individuals involved in the treatment, payment or health care operations pertaining to the subject of the Protected Health Information.

(2) **Designated Record Set:** A group of any records under the control of a covered entity from which personal health information is retrieved by the name of the individual or by identifying number.

(3) **Individually Identifiable Health Information:** Any information, including demographic information, collected from an individual that (a) is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse; and (b) related to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual, and (I) identifies the individual or (ii) with respect to which, there is reasonable basis to believe that the information can be used to identify the individual.

(4) **Protected Health Information:** Individually identifiable health information.

(5) **Vehicle:** Any mode of transportation utilized in ADDS' business.

5.4. **Unattended Health Information:** Protected Health Information that is unattended shall be secured in a manner to protect such information from persons without authorized access to this Protected Health Information.

(1) Vehicles containing any Protected Health Information shall be kept locked while unoccupied. Protected Health Information shall be kept locked in the trunk of the vehicle, when possible. In the event of extreme temperature situations, an electronic device (laptop, personal digital assistant (PDA), etc.) containing Protected Health Information shall be maintained in the temperature controlled cab in a case while the vehicle is occupied. In the event of a vehicle accident, any ADDS employee or student who suspects there is Protected Health Information in the vehicle shall make every reasonable attempt to make sure that the Protected Health Information is not accessible to anyone who does not need to have access to it, after assuring the health and safety of any individual(s).

(2) Upon an employee or student leaving an area where they have materials containing Protected Health Information, e.g., to use the restroom, the employee or student shall take the materials with them or ensure that the area is protected from viewing by those without authorization by locking the area, or informing ADDS personnel if they are ADDS' records, or using some other reasonable intervention.

(3) Electronic devices containing Protected Health Information and other forms of Protected Health Information shall not be left in a hotel room for the day when cleaning service is expected. Upon leaving the hotel, employees or clients shall take these items with them or ensure they are locked in the valuables area at the front desk or locked in a safe in the room if one is available. Should this not be possible, each document that is contained on the laptop shall be password protected on an individual basis.

(4) Employees and clients shall travel in the field taking only Protected Health Information necessary to carry out their duties.

(5) Any documentation or equipment such as laptops, pagers, briefcases, palm pilots, etc. that may contain Protected Health Information shall be secured from access by those without authorization to the Protected Health Information. This includes all locations including an employee's or student's home. Again, each document that is contained on the laptop shall be password protected on an individual basis.

(6) If a designated record set is checked out from ADDS, the medical records policy of ADDS shall be followed. If not ADDS, careful consideration should be used to determine whether checking out any original records containing Protected Health Information is appropriate, and what measures may be used to secure these when unattended.

(7) Data contained on all laptops, etc., should be backed-up to a disk or to the network when at all possible to avoid loss of valuable consumer protected health information.

(8) If Protected Health Information in any form is lost or stolen, the ADDS Executive Director (as applicable), or designee, should be notified as soon as practical, not to exceed two (2) business days, in order to initiate the mitigation process.

5.5. **Within View:** Protected Health Information that is potentially within view of others, even if ADDS' employee or student is present, shall be protected in a manner that such information is not communicated to persons without authorized access to this Protected Health Information.

(1) All Protected Health Information within a vehicle shall be maintained so as to protect from plain view through the windows of the vehicle.

(2) Any electronic device containing Protected Health Information shall not have the screen placed in view of others and if left unattended briefly, a screen saver with password shall be employed consistent with the ADDS's security and Office of Information Systems requirements.

(3) All documentation containing Protected Health Information shall be maintained out of the view of unauthorized persons.

(4) While working with Protected Health Information, the employee or student shall keep the documentation within line of sight or within arm's reach.

(5) This documentation shall be viewed in the most private settings available.

(6) Only Protected Health Information documentation necessary for the task at hand shall be in view.

(7) Briefcases containing Protected Health Information shall remain closed when not in use.

(8) When having Protected Health Information material copied, the employee or student shall ensure that this material is only viewed by authorized persons.

(9) When the employee or student is finished with reviewing Home records containing Protected Health Information, the records shall be returned to Home personnel and secured prior to the field employee or student departing, or in the case of an ongoing audit or investigation, etc., at the time of completion.

5.6. **Faxing:** Employees and clients shall send and receive faxed materials containing Protected Health Information to and from ADDS' locations only, unless such locations are not readily available and timely transmission of records is necessary for safety needs. If in non-ADDS locations:

(1) When sending or receiving a fax containing Protected Health Information, the employee or student shall ensure only those authorized to view have access to the material during the process of transmission.

(2) The fax cover sheet shall not contain Protected Health Information.

(3) Upon sending or receiving material containing Protected Health Information, the employee or student or designee shall call the location to verify with the sender or the receiver that the transaction was successful.

(4) The employee or student shall be waiting to receive the fax at the fax machine when the transmission is expected if the material could be accessed by those without authorization to view the Protected Health Information.

5.7. Field-based employees/clients will utilize appropriate discretion in the use of ID badges when providing treatment in public areas, in accord with the policies of the site.

5.8. When using sign language interpreters where Protected Health Information may be transmitted, the most private setting available out of view of others shall be used.

5.9. Protected Health Information that is verbally transmitted to others shall be protected in a manner that such information is not communicated to persons without authorized access to this Protected Health Information.

(1) Conversations where Protected Health Information is discussed shall occur in the most private settings. There shall be as much distance as possible between any individuals without authorized access to the Protected Health Information.

(2) Conversations where Protected Health Information is discussed shall occur with the employee or student using a volume level which cannot be overheard by those without authorized access to the Protected Health Information. This includes telephone conversations. If there is no way to prevent being overheard, a specific code shall be used to identify an individual such as chart number, or patient initials.

- The employee or student shall make every effort to keep the volume level of all participants low enough so as to not be overheard.
- Conversations shall involve using only the first name of an individual whenever possible.

5.10. Protected Health Information that may be shared with others in the course of an employee carrying out duties shall be protected in a manner that such information is not communicated to persons without authorized access to this Protected Health Information.

5.11. Deaf and linguistic interpreters shall be used by field staff in accordance with guidelines established by the ADDS' Office of Disability Support Services. When the use of an interpreter is required, field staff and clients shall contact the Office of Disability Support Services for guidance; however, in the absence of verified interpreter certification or licensure, the following minimal requirements shall be ensured:

- The interpreter shall not be an immediate family member or close family friend of the subject of the Protected Health Information, unless the subject of the Protected Health Information consents.
- The interpreter shall not use or disclose any Protected Health Information obtained as a result of providing interpretation services. If at all possible, the interpreter shall sign a confidentiality agreement as set forth in these procedures.

6. **Designated Records:**

6.1. **Purpose:** It is the policy of ADDS to identify those records maintained by or for the department and its facilities that meet the definition of designated record set covered by the HIPAA Privacy rule, specifically 45 CFR Section 164.501.

6.2. **Application:** ADDS

(1) Definitions
(2) Procedure

(3) Not Part of the Record Set
(4) Data Trustee
(5) Record Destruction

6.3. **Definitions:**

(1) **Designated Record Set:** A group of records maintained by or for a covered entity that is: (a) the medical records and billing records about individuals maintained by or for a covered health care provider; (b) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (c) used, in whole or in part, by or for the covered entity to make decisions about individuals.

(2) **Record:** any item, collection, or grouping of information that includes protected health information and is maintained, collected, used or disseminated by or for a Home.

(3) **Sentinel Event:** a term used by the Joint Commission on Accreditation of Healthcare Organizations (accreditation held by CPS facilities). A sentinel event is an unexpected occurrence involving death or serious physical or psychological injury, or the risk thereof.

(4) **Protected Health Information:** See HIPAA Procedure 1.005, 1.b. and c.

6.4. **Procedure:**

(1) ADDS shall identify all information systems (defined as an organized collection of information) that contain Protected Health Information, including the location, unique system identifier, the form of the data (electronic or paper), the data maintainer, and a description of the type of Protected Health Information contained.

(2) That inventory shall be maintained by the Program Coordinator or designee, or the ADDS Privacy Officer, if applicable. Assistance may be requested from the Information Services staff. Any new or modified systems shall be added to the inventory by the appropriate Privacy Officer.

(3) In order to maintain an accurate inventory of record systems, when new systems are created, the staff responsible for developing and maintaining the information shall notify the Program Coordinator that the system is in production and it contains Protected Health Information. When a current system that contains Protected Health Information is no longer used or needed, the staff responsible for maintaining the information shall notify the Home Privacy Officer so that the inventory system can be amended and the information retained or destroyed according to retention policies.

(4) For the purpose of the implementation of this policy, the term designated record set includes any item, collection, or grouping of information that includes Protected Health Information and is maintained, collected, used, or disseminated by or for ADDS for covered care or payment decision making including but not limited to:

- Medical record and billing records about covered persons served maintained by ADDS;
- Enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for ADDS; and
- Any records or information used, in whole or in part, by or for ADDS to make decisions about persons served.

6.5. **Not Part of the Designated Record Set:**

(1) Information that is not part of the Designated Record Set is defined as follows: any documents that are used for census information, quality assurance or quality improvement, peer review, sentinel event, Centers for Medicare and Medicaid purposes, utilization review, abuse/neglect investigations, incident/injury reports, state auditors, or various electronic databases, etc., which are not used to make decisions regarding an individual consumer, shall not be considered as part of the Designated Record Set. FERPA education and treatment records may or may not be included, based on unit determinations. See HIPAA Procedure 1.005, 2.

(2) However, please note that these types of information may be accessible by parents or guardians upon presentation of appropriate documentation. In addition, for forensic cases (defined as Chapter 552 or 557, RSMO, evaluations), the pretrial commitment order, the pretrial evaluation, or any correspondence relating to the pretrial is not part of the designated records set.

- Working files, either paper or electronic, are also not considered part of the designated records set, and are defined in Appendix Ai.
- Psychotherapy notes are not included in the designated records set (psychotherapy notes are defined in 45 CFR Section 164.501, and are to be kept separate from the medical record).

6.6. **Data Trustee:** When an individual or department has been given sanctioned, exclusive possession and control of Protected Health Information as part of their assigned duties, they shall be responsible for all administrative duties of a data trustee in terms of security, data access, privacy, data backup, disaster recovery and accountability. When ADDS does not have the technical expertise or equipment to adequately protect the Protected Health Information, they must arrange for technical assistance through the Information Systems to assure the confidentiality of the Protected Health Information.

6.7. **Record Destruction:** The designated record set shall be created, stored, released, transported, copied and destroyed based on policy 8.110, Record Retention and Destruction.

7. **Retention & Protection:**

7.1. **Purpose:** To ensure the availability of relevant data and information, it is the policy of the ADDS to maintain specific retention schedules for various types of individually identifiable health information in compliance with federal and state laws and professional practice standards. ADDS has a records disposition schedule approved by the State Records Commission. (RSMo 109.250) Microfilm/microfiche and electronic imaging are accepted forms of records maintenance. This policy shall be consistently applied with the more stringent law followed and records destroyed after the retention period has expired.

7.2. **Application:** ADDS

(1) Definitions
(2) Storage Procedure
(3) Retention Procedure
(4) Destruction Procedure

7.3. **Definitions:**

(1) **Protected Health Information:** See HIPAA Procedure 1.005, 1.b. and c.

7.4. **Storage Procedure:**

(1) **Paper:** Protected Health Information records storage must be adequate to protect the physical integrity of the record and prevent loss, destruction, and unauthorized use.

a) If the records' office is shared with other programs not responsible for maintaining the records, the shelves or file cabinets must be lockable and kept locked whenever records staff are not in attendance.

b) If Protected Health Information records are retained in a lockable office that is not shared with other staff or in a separate locked file room, open-shelf filing without lockable doors is acceptable. The office or file room should always be locked when staff is not in attendance.

c) Storage area environment should not cause damage to the records and documents and meet accreditation and safety standards.

d) Off-site storage should meet the above standards, be approved by the Unit or ADDS Privacy Officer, as applicable, and have a signed business associates agreement.

e) A record tracking system must be in place to identify when a record has been removed, who took the record, and where it is located.

f) When a microfilm/microfiche imaging copy of the original paper record has been produced, it may be used as a permanent record of the original.

(2) **Electronic:** Electronic storage of Protected Health Information records, if applicable, should have a permanent retrievable capability, and such capability should occur even when there is a technology change.

7.5. **Retention Procedure:** Retention of Protected Health Information records and databases shall comply with federal and state regulations; accreditation, licensure and accepted standards of practice. The more stringent between federal and state law must be followed. This policy should be consistently applied and records destroyed after the retention period has expired.

(1) **Medical Record:** permanent retention or as advised in the current ADDS departmental Records Disposition Schedule. Medical Record documents not on the schedule for permanent retention shall be kept six (6) years, and for minors, three (3) years after the patient reaches legal age as define by Missouri law.

(2) **Financial Records of Person Served:** permanent retention or as advised per current ADDS departmental Records Disposition Schedule. Financial documents not on the schedule for permanent retention shall be kept six (6) years.

(3) Accounting of Disclosure of Information, a minimum of six (6) years, according to the HIPAA Privacy Rule.

7.6. **Destruction Procedure:** Destruction of Protected Health Information in paper or electronic format shall be carried out in accordance with federal and state law and pursuant to the ADDS' Records Disposition Schedule. Records approved for destruction must be destroyed so that there is no possibility of reconstruction of information.

(1) **Paper:** Microfilm/microfiche is an accepted form of records maintenance. When paper records have been microfilmed the original paper may be destroyed. If they are not destroyed, then their retention must be in accord the procedures outlined in this policy.

a) Because all media and reproductions typically have the same legal effect as originals, when a record meets the guideline for destruction, all copies in any media should be destroyed.

b) Appropriate methods for destroying paper records include burning, shredding, pulping, and pulverizing.

c) Documentation of the destruction of records should include: date of destruction; method of destruction; description of records; inclusive date of records; statement that the records were destroyed in the normal course of business; the signatures of the individual supervising and witnessing the destruction. Destruction documents should be permanently retained. Documentation records must be maintained by the Unit Director, or the ADDS Privacy Officer, as applicable.

d) If destruction services are contracted, the contract should be a business associates agreement that specifies: the method of destruction; the time that will elapse between acquiring and destroying the records; identify safeguards against breaches in confidentiality; indemnify the facility from loss due to unauthorized disclosure; and provide proof of destruction to the Unit Director or ADDS Privacy Officer.

(2) **Electronic:** When electronic records or computerized data is destroyed, it should be permanently and irreversibly non-retrievable.

a) **Computer Disks:** Methods may include overwriting data with a series of characters, reformatting the disk, or physical destruction. Deleting a file does not destroy the data but

merely deletes the filename from the directory preventing easy access until it is overwritten.

b) **For laser disks, back-up tapes, hard drives, and servers**, the method of destruction shall be in a format or process as approved or prescribed by the Executive Director. The data must be irreversibly non-retrievable either through electronic or physical destruction.

7.7. Any questions as to whether information retention or destruction is permitted or required by law should be directed to the Unit Director or his/her designee.

8. HIPAA Complaint Process:

8.1. **Purpose:** It is the policy of ADDS to provide persons served with the means to file a complaint if they believe that their protected health information has been improperly used or disclosed. See 45 CFR Section 164.530(d)(1).

8.2. **Application:** ADDS

(1) Definitions
(2) Procedure
(3) Retention
(4) Retaliation

8.3. **Definitions:** As used in this operating regulation, the following terms shall mean:

(1) **Complaint:** Allegation that a person served's protected health information has been improperly used or disclosed. A person served may file a complaint, or a legal guardian or personal representative or a parent, if a minor, may file the complaint. An original Privacy Complaint Form is to be placed in the person served's medical record. If the person served has a guardian, a copy of the complaint shall be sent to the guardian, and the person served should be notified that such action has occurred.

(2) **Person served:** Any person who has received health care services or who is receiving such services from ADDS. Person Served can also indicate Personal Representative if Person Served has a Personal Representative.

(3) **Protected Health Information:** Defined as any information, including demographic information collected from an individual that is created or received by a healthcare provider, health plan, employer, pharmacy, prescription, or healthcare clearinghouse; and is related to the past, present, or future physical or mental health or condition of an individual, the provision of healthcare to an individual, or the past, present, or future payment for the provision of healthcare to an individual; and identifies the individual; or with respect to which, there is reasonable basis to believe that the information can be used to identify the individual.

8.4. **Procedure:** ADDS strongly encourages, and wishes to promote that persons served and service

providers discuss and attempt to resolve issues in the most direct and informal manner and at the local level. The following steps constitute the HIPAA complaint process.

(1) Utilize standardized Audrain Developmental Disability Services, Inc., HIPAA Privacy Complaint form.

(2) Forward a copy of the complaint form to the ADDS Executive Director or ADDS Privacy Officer.

(3) The ADDS Privacy Officer must describe the acts or omissions the person served believes to have occurred.

(4) The HIPAA Privacy Complaint must include the following information:

- The date on which the act or omission occurred;
- A description of the Protected Health Information affected and how it was affected; and
- The name(s) of anyone who may have improperly been provided with the Protected Health Information.

(5) All Privacy Complaints received by the Executive Director or designee will be date-stamped upon arrival.

(6) The Executive Director, Privacy Officer or designee will review and act on the complaint in a timely manner and not more than thirty (30) days from receipt of the complaint. If greater time is necessary to review and investigate the complaint, the Executive Director Privacy Officer or designee shall, within thirty (30) days, notify the grievant, in writing of the delay, and inform the grievant of the expected time frame for completion of the review.

(7) The Executive Director, Privacy Officer or designee shall determine what Protected Health Information is affected by the complaint and if the Protected Health Information was provided to other covered entities and business associates.

(8) If the affected Protected Health Information was created and maintained by a business associate, the complaint will be forwarded to the business associate as outlined in the Business Associate Agreement. Complaints forwarded to business associates will be logged and a notice of the action sent to the patient making the complaint.

(9) The Executive Director, Privacy Officer or designee shall determine if there is cause to believe that a violation of ADDS privacy operating regulations occurred, and the recommended course of action to be taken.

(10) If no violation has occurred the complaint and finding will be date-stamped, the complaint will be considered closed and a written notice of this shall be provided to the person served.

(11) If cause exists to believe that a violation has occurred, the Executive Director, Privacy Officer or designee shall be responsible for determining if:

- Performance or training need to be improved;
- A recommendation for a change to the ADDS operating regulation or creation of a new HIPAA Policy; or
- Conclusion of policy violation is to be reported to implement disciplinary action (Sanction).

(12) The Executive Director, Privacy Officer or designee shall notify the appropriate Program Coordinators, staff or clients of the action needed.

(13) If Program Coordinator or staff discipline must be taken, it must follow the ADDS policies, and is to be initiated by the appropriate administrator on referral of the report of the Executive Director.

(14) If the complaint resolution finds that no cause exists to believe a violation occurred, then the consumer may seek resolution to the ADDS Privacy Officer (if it is an ADDS complaint).

- The person served, through completion of the Complaint Form, will request that the Program Coordinator or designee forward the complaint to the ADDS Privacy Officer.
- The ADDS Privacy Officer will review and act on the complaint in a timely manner and not more than thirty (30) days from receipt of the complaint form.

(15) The ADDS Privacy Officer shall determine one of the following:

- That the original determination of the Executive Director is accurate.
- That remediation should occur at the Program level through increased training, or that a recommendation is made to the Program Coordinator for possible disciplinary action.
- That a recommendation for department operating regulation review be initiated at the ADDS Privacy Officer level.
- That a recommendation be made for the establishment of a new ADDS operating regulation.

(16) The original complaint form shall be placed in the person served's record.

8.5. **Retention:** The Program Coordinator's primary responsibilities in the HIPAA Complaint process include logging and retaining complaints in a retrievable manner for a minimum or six (6) years, and identifying:

(1) Person or entity making the complaint;
(2) Date complaint was received;
(3) A list of what Protected Health Information was affected;
(4) Status of complaint;
(5) A list of business associates or facilities affected; and
(6) Actions taken.

8.6. **Retaliation:** There shall be no retaliation against any person served, or against a Program Coordinator or staff member for assisting a person served to file a HIPAA Privacy Complaint.

9. **Business Associates:**

9.1. **Purpose:** It is the policy of ADDS to obtain satisfactory assurances from business associates who will use the information only for the purpose for which it was engaged by ADDS, will safeguard the information from misuse and will help ADDS comply with its duties under HIPAA to help carry out its health care functions. 45 CFR 502(e), 504(e).

9.2. **Application:** ADDS

(1) Definitions
(2) General Provisions
(3) Business Contracts

9.3. **Definitions:**

(1) **Person served:** Any individual who has received or is receiving services from ADDS.

(2) **Protected Health Information:** Individually identifiable health information as defined at HIPAA Procedure 1.005, 1.b. and c

(3) **Business Associate:** A person or entity who performs functions or activities that involve the use or disclosure of Protected Health Information on behalf of, or provide services to, ADDS, including claims processing or administration, data analysis, processing or administrative utilization review, quality assurance, billing, benefit management, practice management, and other services involving disclosure of Protected Health Information. A member of the ADDS workforce is not a business associate.

9.4. **General Provisions:**

(1) IPAA requires that ADDS obtain satisfactory assurances from its business associates that the business associate will appropriately safeguard the Protected Health Information it receives or creates on behalf of the covered entity. The satisfactory assurances must be in writing, whether in the form of a contract or other agreement between the covered entity and the business associate.

(2) Business associate functions and activities include: Claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management; and repricing.

(3) Business associate services are: Legal; actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; and financial.

(4) Examples of Business Associates:

- A third party administrator that assists a health plan with claims processing.
- A CPA firm whose accounting services to a health care provider involves access to protected

health information.

- An attorney whose legal services to a health plan involve access to protected health information.
- A consultant that performs utilization reviews for a hospital.
- A health care clearinghouse that translates a claim from a non-standard format into a standard transaction on behalf of a health care provider and forwards the processed transaction to a payer.
- An independent medical transcriptionist that provides transcription services to a physician.
- A pharmacy benefits manager that manages a health plan's pharmacist network.

9.5. **Business Associate Contracts:**

(1) ADDS contract or other written arrangement with its business associate must contain the elements specified at 45 CFR 164.504(e). For example, the contract must:

- Describe the permitted and required uses of protected health information by the business associate;
- Provide that the business associate will not use or further disclose the protected health information other than as permitted or required by the contract or as required by law; and
- Require the business associate to use appropriate safeguards to prevent a use or disclosure of the protected health information other than as provided for by the contract.

(2) Where a covered entity knows of a material breach or violation by the business associate of the contract or agreement, the covered entity is required to take reasonable steps to cure the breach or end the violation, and if such steps are unsuccessful, to terminate the contract or arrangement. If termination of the contract or agreement is not feasible, a covered entity is required to report the problem to the Department of Health and Human Services (HHS) Office for Civil Rights (OCR).

(3) Sample business associate contract language is available as HIPAA Procedure 1.160.

9.6. **Transition Provisions for Existing Contracts:** ADDS when having an existing contract (or other written agreement) with a business associate prior to October 15, 2002, is permitted to continue to operate under that contract for up to one additional year beyond the April 14, 2003, compliance date, provided that the contract is not renewed or modified prior to April 14, 2003. This transition period applies only to written contracts or other written arrangements. Covered entities with contracts that qualify are permitted to continue to operate under those contracts with their business associates until April 14, 2004, or until the contract is renewed or modified, whichever is sooner, regardless of whether the contract meets the Rule's applicable contract requirements at 45 CFR 164.502(e) and 164.504(e). A covered entity must otherwise comply with HIPAA, such as making only permissible disclosures to the business associate and permitting individuals to exercise their rights under HIPAA.

9.7. **Exceptions to the Business Associate Standard:** In these situations, ADDS is not required to have a business associate contract or other written agreement in place before protected health information may be disclosed to the person or entity:

(1) Disclosures by a Home to a health care provider for treatment of the individual.

(2) Disclosures to a health plan sponsor, such as an employer, by a group health plan, provided that the group health plan' s documents have been amended to limit the disclosures or one of the exceptions at 45 CFR 164.504(f) have been met.

(3) The collection and sharing of protected health information by a health plan that is a public benefits program, such as Medicare, and another agency to determine eligibility or enrollment.

(4) Other Situations in Which a Business Associate Contract Is NOT Required:

- When a health care provider discloses protected health information to a health plan for payment purposes. A Home that submits a claim to a health plan and a health plan that assesses and pays the claim are each acting on its own behalf as a covered entity, and not as the "business associate" of the other.
- With persons or organizations (e.g., janitorial service or electrician) whose functions or services do not involve the use or disclosure of protected health information, and where any access to protected health information by such persons would be incidental, if at all.
- With a person or organization that acts merely as a conduit for protected health information, for example, the US Postal Service, certain private couriers, and their electronic equivalents.
- Among covered entities who participate in an organized health care arrangement (OHCA) to make disclosures that relate to the joint health care activities of the OHCA.
- Where a group health plan purchases insurance from a health insurance issuer or HMO.
- Where one covered entity purchases a health plan product or other insurance, for example, reinsurance, from an insurer.
- To disclose protected health information to a researcher for research purposes, either with patient authorization, pursuant to a waiver under 45 CFR 164.512(I), or as a limited data set pursuant to 45 CFR 164.514(e). See HIPAA Procedure 1.055.
- When a financial institution processes consumer-conducted financial transactions by debit, credit, or other payment card, clears checks, initiates or processes electronic funds transfers, or conducts any other activity that directly facilitates or effects the transfer of funds for payment for health care or health plan premiums.

Audrain Developmental Disability Services

REQUEST FOR AMENDMENT FORM

NAME AND SSN: _____
PERSON SERVED NUMBER: _____
ADDRESS: _____
_____

DATE OF ENTRY TO BE AMENDED: _____
TYPE OF ENTRY TO BE AMENDED: _____

Describe how the entry is incorrect or incomplete:

- What should the entry say to be accurate or complete?

_____

- You will need to attach any verification or evidence to this form documenting that the information is incorrect or incomplete.
- If granted, would you like this amendment sent to anyone to whom we may have disclosed the information in the past? If so, please specify the name and address of the organization or individual:

_____

Signature of Person served or Legal Representative and Date: _____ / _____
Signature Date

For ADDS Use Only

Date Received: _____

Amendment has been (circle choice): Accepted

Denied (If denied, check reason for denial)
__PHI was not created by this facility
__PHI is not part of patient's designated record set
__PHI is not available to the patient for inspection as required by federal law
__PHI is accurate and complete

Comments:

If the request is denied, you may file a complaint with the Secretary of the Dept. of Health and Human Services by calling 877-695-6775, or writing them at 200 Independence Ave. S.W., Washington, DC 20201. You may also file a grievance with the Office of Civil Rights by calling 866-627-7748, or TTY at 886-788-4989. You may also file a complaint with AUDRAIN DEVELOPMENTAL DISABILITIES SERVICES by contacting the Privacy Office.

Audrain Developmental Disability Services

REQUEST TO RESTRICT PROTECTED HEALTH INFORMATION

Person served Name and SSN: _____
Person served ID Number: _____
Person served Address: _____
_____

Please specify the information to be restricted: _____

Please explain why the disclosure of the above-specified information may not be appropriate: _____

Please indicate the individual or agency to which access should be denied:

Name: _____ Relationship: _____
Name: _____ Relationship: _____
Name: _____ Relationship: _____

Signature of Person served or Guardian: _____ / _____
Signature Date

For ADDS USE ONLY

Date Received: _____

Restriction has been (circle choice): Accepted Denied

Comments: _____

Completed copy of this form provided to Person served on: _____ (date)

Condition Upon Which Restriction will Expire (check one):
__Person served request
__Justification for the restriction no longer exists
__Other (specified): _____

Name and Title of Staff Member processing request: _____ _____
Name Title

Signature of Privacy Officer or designee: _____ / _____
Signature Date

Audrain Developmental Disability Services

REQUEST FOR PERSON SERVED ACCESS TO PROTECTED HEALTH INFORMATION

Person served Name: _____
SSN: _____
Person served ID Number: _____
Address: _____
_____

Please specify the format for information requested (circle one): Paper Fax
I agree to accept a summary of the PHI (circle one): Yes No
I agree to pay the costs associated with this request
for access to PHI (circle one): Yes No

Please indicate the person served, parent of minor, or any legal guardian who is requesting access:

Name: _____ Relationship: _____
Name: _____ Relationship: _____
Name: _____ Relationship: _____

Signature of Person served or Legal Representative and Date: _____ / _____
Signature Date

ADDS Use Only

Date Received: _____

Access has been (circle one): granted denied
Comments: _____

If denied, letter of denial provided to person served on: _____ (date)

Reason for denial without right to review (check all that apply):
__Psychotherapy Notes
__Patient agreed to denial while in research project
__Information for use in civil, criminal or administrative proceedings
__Access would identify the source
__Other: _____

Reason for denial with right to review (check all that apply):
__Reasonably likely to endanger life or physical safety of Person served or others
__Documentation makes reference to third party and granting access is likely to cause harm
__Personal representative is requesting Party, and Person served has been or may be subject to domestic violence

Audrain Developmental Disability Services

AUTHORIZATION FOR DISCLOSURE OF PERSON SERVED MEDICAL/HEALTH INFORMATION

I, _____ (Name of Person served/Guardian) authorize and request _____ (Name of Facility, Agency or Person) to disclose/release the below specified information of _____ (name), _____ (DOB), ____-__-____ (SSN) who received services from _____ to _____ (dates) to _____ (person, facility, agency) with the address of: _____

The Purpose of the Disclosure is (check one):

__After Care __Placement __Transfer/Treatment
__Treatment Planning __Eligibility Determination __Continuity of Service/Care
__Assessment __At Person served's Request __Conditional/Unconditional Release Hearing
__To share or refer my information to other Missouri state agencies (DOSS, DHSS, DMH, DESE, DOC etc.,) to obtain services consistent with the _____ program (please complete the name of the program in which you want to participate).
__Other (Specify) _____

The Specific Information to be Disclosed is (check all that apply):

__Discharge Summary __Progress Notes __Treatment Plan and/or Reviews
__Medical/Psychiatric Assessment(s)
__Other (Specify) _____

READ CAREFULLY

1. I understand that my medical/health information records are confidential. I understand that by signing this authorization, I am allowing the release of my medical/health information. The PHI in my medical record includes mental/behavioral health information. In addition, it may include information relating to sexually transmitted diseases, acquired immunodeficiency syndrome (AIDS), human immunodeficiency virus (HIV), other communicable diseases, and/or alcohol/drug abuse.

2. Alcohol and drug abuse information records are specifically protected by federal regulations and by signing this authorization without restrictions I am allowing the release of any alcohol and/or drug information records (if any) to the agency or person specified above. Please sign if you are authorizing the release of alcohol and drug abuse information: _____

3. This authorization includes both information presently compiled and information to be compiled during the course of treatment at the above-named facility during the specified time frame.

4. This authorization becomes effective on _____. This authorization automatically expires on the following date, event or special condition _____.

5. If I fail to specify an expiration date, this authorization will expire in one year.

6. I understand that I have a right to revoke this authorization at any time. I understand that if I revoke this authorization I must do so in writing and present my written revocation to the Executive Director or Privacy Officer. I further understand that actions already taken based on the authorization, prior to revocation, will not be effected.

7. I understand that I have the right to receive a copy of this authorization. A photographic copy of this authorization is as valid as the original.

8. I understand that authorizing the disclosure of this medical/health information is voluntary. I can refuse to sign this authorization. I need not sign this form in order to assure treatment. I understand that I may request to inspect or request a copy of information to be used or disclosed. I understand that any disclosure of information carries with the potential for an unauthorized re-disclosure and the information may not be protected by federal confidentiality rules. If I have questions about disclosure of my medical/health information, I can contact the Executive Director or Privacy Officer.

The following applies to alcohol and/or drug abuse treatment information records: This information has been disclosed to you from records that confidentiality is protected by Federal law. Federal regulations prohibit you from making further disclosure of it without the specific written authorization of the person to whom it pertains, or as otherwise specified by such regulations. A general authorization for disclosure of medical or other information is not sufficient for this purpose.

My signature below acknowledges that I have read, understand and authorize the release of my PHI.

Signature of Person served or Guardian: _____ / _____
Signature Date

WITNESS: _____ / _____
Signature Date

Notice of Revocation

I, _____ (the Person served), herby revoke my authorization of this disclosure of information to the agency/person listed above. This revocation effectively makes null and void any permission for disclosure of information expressly given by the above authorization. I understand that any actions based on this authorization, prior to revocation, will not be affected.

Signature of Person served or Guardian: _____ / _____
Signature Date

WITNESS: _____ / _____
Signature Date

If you choose to revoke your authorization, please provide a copy of the completed revocation to the Privacy Officer or Executive Director.

Audrain Developmental Disability Services

REQUEST FOR ACCOUNTING OF DISCLOSURES OF PERSON SERVED'S PROTECTED HEALTH INFORMATION

Person served Name and SSN: _____
DOB: _____
Person served's Address: _____
_____

Please specify the time period for which you are requesting the accounting of disclosures:

_____

This is the first request for an accounting of disclosures (circle): Yes No

If NO, I agree to pay cost associated with this request for an accounting of disclosures: Yes No

The first request in a 12-month rolling period is free of charge. Charges accrue for more than one request within that 12-month period.

Please indicate the Person served, parent or guardian who is requesting the accounting of disclosure.
Name: _____
Relationship to Person served: _____

Signature of Person served or Legal Guardian and date: _____ / _____
Signature Date

ADDS Use Only

Date Received: _____

Copy Provided to Person served on (date):_____

Signature of Privacy Officer or Designee and Date: _____ / _____
Signature Date

Audrain Developmental Disability Services

MEDICAL AUTHORIZATION
(HIPAA COMPLIANT)

Patient Name: _____
Date of Birth / SSN: _____
Address: _____
_____

TO: _____

You are hereby authorized to furnish to ADDS, or its agent(s), at 222 East Jackson St., Mexico, MO 65265 the above- named patients health information, as described below for the purpose of:

At the request of the individual. you are also authorized to permit a representative of ADDS to conduct a personal review of all medical information pertaining to the above-named patient and to orally discuss this information with you. The following type of information to be used or disclosed is as follows:

___ complete health records for ALL dates, including documents and records received from or that were created by another provider or physician.
___ abbreviated set from ALL dates including:

___ Admission	___ dictation reports	___ physician orders, intake/out take
___ clinical tests	___ medication sheets	___operative info.
___discharge/death summaries	___ labs	___flow sheets/assessment sheets
___Special test/therapy	___ rhythm/ECG strips	___ nursing information
___ transfer/consent forms	___ ER info.	___ labor/delivery
___ x-ray reports	___ consultation reports	___ OB nursing assess.
___ postpartum flow sheets	___ other: _____	

I understand that by signing this authorization I am allowing the release of any requested medical information to the firm of ADDS, LLC. By signing this authorization I am allowing the release of any drug and/or alcohol information, psychiatric, HIV testing and/or results or AIDS information contained within the records to the above named attorneys. I understand that this authorization is voluntary and that I may revoke this medical release in writing at any time. I understand that the information used or disclosed may be subject to re-disclosure by ADDS, LLC and would then no longer be protected by federal privacy regulations. A photocopy of this authorization may be used in place of this original. This authorization will expire one year from the date of this authorization and will no longer be valid for use after such date.

Print Name here _____ Signature / Date _____ / _____

Address: _____ Phone _____

STATE OF MISSOURI)
(SS.
COUNTY OF AUDRAIN)

Sworn to and subscribed before me this _____ day of _____, 20___.

_____
Notary Public

My commission expires: _____.

Audrain Developmental Disability Services

AUTHORIZATION FOR RELEASE OF WORKERS' COMPENSATION RECORDS

TO:	REGARDING:
Missouri Department of Labor and Industrial Relations; Division of Workers Compensation 3315 West Truman Boulevard Room 131 PO Box 58 Jefferson City 65102-0058	Name: Date of Birth: SSN:

I hereby authorize any and all of my workers' compensation records to be sent to ADDS, as well as any and all information which relates to my education. It is understood that no one from ADDS, or any of their representatives will discuss this information personally with anyone from the Division of Workers' Compensation.

It is further agreed that a true copy of all workers' compensation records or information which is received by way of this authorization will immediately be forwarded directly to ADDS, 222 East Jackson St., Mexico, Missouri, 65265.

A photocopy of this authorization shall be considered as effective and valid as the original.

Signature / Date _____ / _____

Print Name here _____

Address: _____ Phone _____

STATE OF MISSOURI)
(SS.
COUNTY OF AUDRAIN)

Sworn to and subscribed before me this _____ day of _____, 20___.

_____
Notary Public

My commission expires: _____.

Audrain Developmental Disability Services

AUTHORIZATION FOR RELEASE OF SCHOOL RECORDS

TO:	REGARDING:
Name of School: Address: City: State: Zip Code:	Name: Date of Birth: Address: City: State: SS#:

I hereby authorize any and all of my school records and transcripts to ADDS, and any and all information which relates to my education with them.

It is understood that no one from ADDS, or any of their representatives will discuss this information personally with anyone from the school listed above.

It is further agreed that a true copy of all school records or information which is received by way of this authorization will be immediately forwarded directly to ADDS, 308 East Jackson St., Mexico, Missouri, 65265.

A photocopy of this authorization shall be considered as effective and valid as the original.

Signature / Date _____ / _____

Print Name here _____

Address: _____ Phone _____

STATE OF MISSOURI)
(SS.
COUNTY OF AUDRAIN)

Sworn to and subscribed before me this _____ day of _____, 20___.

_____
Notary Public

My commission expires: _____.

Audrain Developmental Disability Services

FACE SHEET

NAME: _____
(As it appears on Social Security Card)

DATE OF BIRTH: _____

SOCIAL SECURITY NO: _____

HOME ADDRESS: _____

HOME TELEPHONE NO.: _____

VALID MISSOURI DRIVER'S/CHAUFFEUR'S LICENSE: YES / NO

If yes, number: _____

Have you had an automobile accident or received a traffic citation within the last three years? YES / NO

If yes, state location and date: _____

DATE OF LAST PHYSICAL: _____

INITIAL DATE OF EMPLOYMENT: _____

DATE PERSONNEL EVALUATION COMPLETED: _____

Audrain Developmental Disability Services

COMPLAINT RESOLUTION PLAN

Employee Name: _____
Date of Meeting: _____
Date of Plan: _____
Program / Supervisor: _____

Background:

_____

_____

_____

_____

Concerns/Complaints:

1._____

2. _____

3. _____

4. _____

Resolution Plan(s):

Complaint 1

Discussion:

_____

_____

_____

Plan of Action:

_____

_____

_____

Responsible Party:

_____

_____

Complaint 2

Discussion:

_____

_____

_____

Plan of Action:

_____
_____
_____

Responsible Party:

_____
_____

Complaint 3

Discussion:

_____
_____
_____

Plan of Action:

_____
_____
_____

Responsible Party:

_____
_____

Complaint 4

Discussion:

_____
_____
_____

Plan of Action:

_____
_____
_____

Responsible Party:

_____
_____

I believe this summary fairly represents information discussed and the resolution(s) planned.

_____ _____
Employee Date

_____ _____
Supervisor Date

_____ _____
Executive Director Date