HIPAA Policy and Procedures

1. Introduction - This Health Insurance Portability and Accountability Act (HIPAA) Policy is established to ensure compliance with the HIPAA regulations (45 CFR Parts 160, 162, and 164) and the Rule of Health Insurance Portability and Accountability Act of 1996 (HIPAA) 9 CSR 10-5.220.

2. Scope - This policy applies to all employees, contracted personnel, relief/respite providers, volunteers, and student workers who have access to personal and medical information in any form, including documentation, video, audio, or other computer-stored information.

3. HIPAA Compliance Procedures - All personnel shall adhere to the procedures outlined in the HIPAA regulations, specifically 9 CSR 10-5.220, to ensure the confidentiality, integrity, and availability of protected health information (PHI).

4. Safeguarding PHI (securing locations and equipment; implementing technical solutions to mitigate risks; and workforce training) - All personal and medical information, including documentation, video, audio, or computer-stored information, must be safeguarded to prevent unauthorized access or disclosure. Access to PHI is restricted to authorized personnel only. Employees must use unique login credentials, and access logs must be regularly reviewed.

5. Consent for Disclosure - PHI shall not be disclosed without the explicit consent of the participant and/or the individual's guardian or caregiver. Consent forms must be obtained, and the purpose of disclosure must be clearly communicated to the participant or their representative.

6. Annual Review - HIPAA policies and procedures will be reviewed annually to ensure their relevance and effectiveness. All employees, including contracted, relief/respite providers, volunteers, and student workers, are required to sign and date the annual review documentation, indicating their understanding and commitment to maintaining HIPAA compliance.

7. Training - All personnel with access to PHI will undergo regular training on HIPAA policies and procedures when hired. Training sessions will cover the importance of HIPAA compliance, the rights of participants, and the consequences of unauthorized disclosure.

8. Reporting Security Incidents - Any security incidents, breaches, or unauthorized disclosures of PHI must be reported immediately to the designated HIPAA Privacy Officer or supervisor. Investigations will be conducted, and appropriate corrective actions will be taken.

9. Disciplinary Measures - Violations of HIPAA policies may result in disciplinary action, including but not limited to verbal or written warnings, suspension, or termination of employment or contractual agreements.

10. Documentation Retention and Disposal - PHI will be retained only for the duration necessary for its intended purpose. Proper disposal methods, such as shredding or secure deletion, will be employed to ensure information is not accessible once it is no longer needed.