S^D Associates LLC

Behavioral Services **Assessment, Consultation, Training and Direct Service**

www.sdplus.org **NVT: (802) 662-7831**

HIPAA Privacy and Security Policy

Sd Associates

Purpose

Sd Associates is committed to complying with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations. This policy establishes safeguards to protect the confidentiality, integrity, and availability of electronic protected health information (ePHI).

1. Transmission Security

Sd Associates implements technical security measures to guard against unauthorized access to electronic protected health information transmitted over an electronic communications network. All devices that access our secured SdServer must be setup by our IT Admin (versed in HIPAA policies). If a staff device is lost or stolen, the data still remains inaccessible by any 3rd party who accesses the device as a series of passwords are required to both access the machine and then access the files on the server. Furthermore, if a device is lost or stolen, access keys are revoked remotely, thus immediately rendering the device incapable of accessing ePHI. Patient data is transmitted electronically only through secure platforms that provide **end-to-end encryption**. The primary platform we use to transmit ePHI is our SdCloud. Through this encrypted file sharing cloud, we set expiring passwords for folders and files that are then shared securely internally or externally (when necessary). The transmission of ePHI through unsecured or unauthorized systems is strictly prohibited.

2. Minimum Necessary Standard

Sd Associates limits workforce access to protected health information to the **minimum necessary** to accomplish the intended purpose of the workforce member's job duties. Access is role-based, reviewed periodically, and adjusted promptly when workforce roles change, client assignments change, or upon termination of employment.

3. Data Backup and Contingency Planning

Sd Associates maintains a **data backup and disaster recovery procedure** to ensure the availability and integrity of electronic protected health information. Patient data is backed up on a regular basis using secure systems, and backup data is protected from unauthorized access. The primary backup method we used is our SdServer. This is a highly encrypted file server with both physical security and digital security (AES 256-bit

encryption, or better). We stagger backups on multiple physical (not virtual) servers daily, weekly, monthly, and annually. Each server also contains a RAID 1 drive for redundancy. Per HIPAA requirements, we store data for at least 6 years after the last update to the data. Backup and restoration processes are tested periodically to ensure effective data recovery.

Enforcement

All workforce members are required to comply with this policy. Violations may result in disciplinary action, up to and including termination, in accordance with our company procedures and applicable law.