HIPAA Privacy and Security Policy

Purpose

This policy outlines how All Care Therapies protects the privacy and security of client health information in compliance with the Health Insurance Portability and Accountability Act (HIPAA) and applicable state laws. Our goal is to ensure that all Protected Health Information (PHI) is handled with integrity, confidentiality, and professionalism.

Scope

This policy applies to all employees, contractors, students, and vendors who may have access to PHI in any form—oral, written, or electronic. It covers both in-person and telehealth services provided by ACT.

Definitions

- **PHI (Protected Health Information):** Any individually identifiable health information, whether electronic, paper, or verbal, that relates to a client's health status, treatment, or payment for care.
- **Minimum Necessary Standard:** Only the minimum amount of PHI necessary to perform a job duty may be accessed, used, or disclosed.

Policy Statements

1. Privacy of Client Information

All PHI is confidential. It may only be accessed, used, or shared for the purposes of treatment, payment, or healthcare operations unless the client provides written authorization or as otherwise permitted by law.

2. Client Rights

Clients have the right to:

- Receive a Notice of Privacy Practices.
- Access and request copies of their records.
- Request amendments or corrections.
- Request restrictions on the use or disclosure of their PHI.
- Request confidential communication methods.
- File a complaint without fear of retaliation.

3. Safeguards

- **Physical Safeguards:** Paper records are stored securely and accessible only to authorized staff.
- **Technical Safeguards:** Electronic records are password protected and stored in HIPAA-compliant systems.
- **Administrative Safeguards:** Staff receive HIPAA and privacy training annually. Access to PHI is role-based.

4. Telehealth

All telehealth services are delivered through HIPAA-compliant platforms. Providers must ensure privacy during sessions by using secure devices, private spaces, and encrypted connections.

5. Disclosures

PHI may be disclosed without client authorization in limited situations, such as:

- To the client or their authorized representative.
- For treatment, payment, or healthcare operations.
- As required by law (e.g., public health reporting, court orders, child/elder abuse reporting).

6. Breach Notification

Any suspected or confirmed breach of PHI must be reported immediately to the Compliance Office. ACT will follow HIPAA breach notification rules, including notifying affected clients and regulators when required.

7. Employee Responsibilities

All workforce members must:

- Protect PHI at all times.
- Follow the minimum necessary rule.
- Refrain from discussing PHI in public areas.
- Report suspected breaches or violations promptly.

8. Enforcement

Violations of this policy may result in disciplinary action, up to and including termination or termination of contract. Serious violations may also be reported to licensing boards or legal authorities.