POLICY AND PROCEDURE

REACH for Tomorrow

Title: Security Policy

Effective Date: 07/01/2025

Approved By: Director of Medical and Clinical Services

Review Schedule: Annually or as Needed

Applies To: All Programs and Locations — Outpatient MH/SUD, IOP, Integrated Behavioral Health/Primary Care, and PHP

I. Purpose

The purpose of this Security Policy is to protect the safety, confidentiality, and integrity of REACH for Tomorrow's personnel, clients, facilities, and information systems. This policy establishes uniform procedures to prevent and respond to security risks—both physical and electronic—in compliance with CARF standards, the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, and other applicable federal and state regulations.

II. Scope

This policy applies to all employees, contractors, students, interns, and volunteers of REACH for Tomorrow. It governs the physical security of organizational property, electronic data protection, and staff responsibilities regarding the confidentiality and protection of organizational assets and client information.

III. Policy Statement

REACH for Tomorrow will maintain a secure environment that protects staff, clients, visitors, facilities, and all forms of data from theft, loss, unauthorized access, or misuse. The organization will employ administrative, technical, and physical safeguards appropriate to the level of risk.

IV. Objectives

1. Protect clients, staff, and visitors from harm or unauthorized access.
2. Ensure secure management of client information and records.
3. Prevent unauthorized disclosure or alteration of confidential data.
4. Establish consistent procedures for incident response and reporting.
5. Maintain compliance with CARF, HIPAA, and relevant state and federal security standards.

V. Responsibilities

Executive Director: Oversees the organization's security program and ensures compliance with applicable regulations. Appoints a Security Officer responsible for implementation and monitoring.

Security Officer (or Designee): Coordinates physical and data security programs, conducts risk assessments, ensures compliance, and investigates security incidents. Provides staff

training.

Supervisors and Program Directors: Ensure staff follow security procedures and report incidents promptly.

All Staff: Adhere to all security procedures, protect property and information, and report suspicious behavior or breaches immediately.

VI. Physical Security Measures

1. Facility Access:
- Access is limited to authorized personnel during business hours.
- Offices and file areas remain locked when not in use.

2. Environment and Equipment:
- Security cameras and lighting maintained as needed.
- Keys and access codes distributed only to authorized staff; lost keys must be reported.
- Computers and equipment secured when unattended.

3. Emergency Preparedness:
- Fire and security systems maintained and tested.
- Staff trained on evacuation, lockdown, and threat response.

VII. Information Security Measures

1. Access Control:
- EHR and data systems require unique user IDs and strong passwords.
- Access based on job role and minimum-necessary principle.
- Accounts deactivated upon staff termination.

2. Data Encryption and Storage:
- All electronic PHI encrypted in storage and transmission.
- Data backups occur daily and are securely stored offsite or in encrypted cloud systems.

3. Use of Technology:
- Staff may not share passwords or install unauthorized software.
- Personal devices used for work must meet security standards.

4. Email and Communication:
- Emails with PHI must be encrypted.
- Fax transmissions must include confidentiality disclaimers.
- Client information must never be disclosed on social media.

VIII. Incident Reporting and Response

Any suspected or actual security breach (e.g., theft, data loss, unauthorized access) must be reported immediately to the Security Officer and Director of Medical and Clinical Services.

An Incident Report must be completed within 24 hours. The Security Officer investigates, determines scope, and implements corrective actions. If PHI is compromised, notifications will be handled in accordance with HIPAA/HITECH requirements.

IX. Confidentiality and Privacy

All staff must sign a confidentiality agreement at hire. PHI and other sensitive data may not be shared with unauthorized individuals or discussed publicly. Violations may result in disciplinary action up to termination.

X. Training and Education

Security and confidentiality training will be provided at onboarding and annually. Topics include:

- Physical and data security
- Password management and access control
- HIPAA compliance and privacy standards
- Incident response and reporting

Attendance and competency verification will be documented in personnel files.

XI. Monitoring and Continuous Improvement

Security procedures are reviewed quarterly by the Security Officer and annually by the Executive Director. Findings from audits or incidents are integrated into the Continuous Quality Improvement (CQI) plan.

XII. Policy Review and Approval

This policy will be reviewed annually and revised as necessary to ensure compliance with evolving CARF, HIPAA, and technological standards.

Approved By: Leslie M Stegall MSN, APRN, NP-C, PMHNP-BC

Title: Director of Medical and Clinical Services

Date: 07/01/2025