POLICY AND PROCEDURE

REACH for Tomorrow

RG-111

TITLE: P&P Confidential Admin Records

EFFECTIVE DATE: 8/31/25 AUTHORIZED BY: Board of Trustees

Policy Purpose

To establish and enforce a system for maintaining, securing, and protecting all confidential administrative records in accordance with **CARF Standard 1.E and 3.E**, **OHMAS certification requirements**, and all applicable federal, state, and local laws. This policy ensures that legal, regulatory, contractual, and ethical responsibilities are met consistently across all operational and personnel functions.

Scope

This policy applies to all REACH For Tomorrow administrative records—physical or electronic—that are not part of client clinical files but contain confidential, sensitive, or proprietary information. This includes HR files, financial documents, legal agreements, board records, personnel testing results, contracts, and operational documentation.

Policy Statement

REACH For Tomorrow is committed to protecting confidential administrative records and ensuring compliance with all relevant obligations related to:

- **a. Legal**
- **b. Regulatory**
- **c. Confidentiality**
- **d. Reporting**
- **e. Licensing**
- **f. Contractual**
- **g. Debt Covenants**
- **h. Corporate Status**
- **i. Rights of the Persons Served**
- **j. Privacy of the Persons Served**

- **k. Employment Practices**
- **l. Mandatory Employee Testing**

REACH recognizes that failure to protect confidential administrative information or comply with legal requirements may result in organizational, financial, and reputational harm.

Definitions

- **Administrative Records:** Records relating to personnel, operations, legal matters, finance, board governance, compliance, and external contracts—distinct from clinical or client-specific treatment documentation.
- **Confidential Records:** Any non-public information that, if disclosed, could harm individuals, breach contracts, or compromise the organization's legal or regulatory standing.

Procedures

1. Confidential Record Types and Protection Measures

- Confidential administrative records include but are not limited to:
    - Personnel files (employment history, performance reviews, background checks)
    - Drug and alcohol testing documentation (as required under OHMAS)
    - Board minutes and governance records
    - Contracts, grants, and MOUs
    - Financial records and debt agreements
    - Regulatory licensing documentation
    - Internal audits, compliance reviews, and incident reports
- These records are:
    - Stored in locked file cabinets or password-protected systems.
    - Accessible only to designated personnel (e.g., HR, compliance, executive leadership).
    - Retained according to state and federal retention laws (e.g., 7 years for most HR and financial documents).
    - Disposed of using shredding (paper) or secure deletion (digital) protocols.

2. Compliance with Legal and Regulatory Requirements (1.a.E, 1.b.E, 1.e.E)

- The Compliance Officer and Executive Director are responsible for:
    - Monitoring state and federal laws, including CARF and OHMAS updates.

  - Ensuring records are maintained to satisfy documentation requirements under OAC 5122-26 and 5122-29.
  - Ensuring licensure renewals, inspections, and certifications are recorded, filed, and accessible.

3. Confidentiality and Privacy (1.c.E, 1.j.E)

- Administrative records containing PHI or PII must follow HIPAA and 42 CFR Part 2 confidentiality protections.
- Staff must sign annual confidentiality agreements and complete privacy training.
- Records containing client identifiers in administrative functions (e.g., incident logs, billing disputes) are redacted or anonymized when shared outside the agency.

4. Mandatory Reporting Obligations (1.d.E)

- Administrative reports required by OHMAS, Medicaid, or other funders (e.g., incident reports, audits, investigations) are documented securely.
- All staff are trained on how to report and document reportable events in compliance with state and federal law.

5. Contractual and Debt Compliance (1.f.E, 1.g.E)

- Contracts with funders, partners, and vendors are reviewed annually for compliance.
- Grant terms and debt covenants are monitored by the Finance Director, and compliance reports are filed with leadership and funding agencies.
- Records related to loans or restricted grants are treated with heightened confidentiality.

6. Corporate Governance and Status (1.h.E)

- Articles of Incorporation, bylaws, Board resolutions, and 501(c)(3) status documentation are securely stored in the agency's corporate records archive.
- These records are reviewed during annual board governance reviews or as needed by auditors or funders.

7. Rights and Employment Practices (1.i.E, 1.k.E, 1.l.E)

- Personnel files are maintained securely by Human Resources and include:
  - Employment contracts, evaluations, complaints, and corrective actions.
  - Documentation of trainings in client rights and ethics.
  - Drug testing results stored in separate confidential folders accessible only to authorized HR staff.
- Staff are informed of their own rights, and the rights of persons served, during onboarding and through annual training.
- Mandatory employee testing records (e.g., pre-employment, random drug testing) are maintained in compliance with OHMAS certification rules.

Monitoring and Audits

- The Compliance Officer will:
    - Conduct semiannual audits of access logs and record storage.
    - Verify record retention and destruction practices.
    - Submit a report to the Executive Director and Board on record compliance.
- Deficiencies or violations will result in a written corrective action plan.

Training and Education

- All staff receive training during orientation and annually thereafter on:
    - Confidentiality of administrative records.
    - Applicable laws and CARF/OHMAS compliance expectations.
    - Data privacy, breach response, and ethical handling of sensitive information.

Retention and Destruction

- Confidential administrative records are retained per federal/state guidelines (e.g., 6–10 years depending on type).
- Disposal follows written protocol for secure shredding or digital deletion.
- Destruction is logged and reviewed by the Compliance Officer.

Breach Response

- Any breach involving administrative records must be reported to the Compliance Officer within 24 hours.
- A documented investigation and remediation process will follow, in compliance with breach notification requirements.

References

- **CARF Standards Manual – Sections 1.E & 3.E**
- **OHMAS Certification Rules (OAC 5122-26, 5122-29, 5122-27-08)**
- **HIPAA and 42 CFR Part 2**

- **Ohio Revised Code & Administrative Code**
- **Internal REACH Policies: Privacy, Records Retention, Personnel Files**