

Policy

The Poverello Center, Inc. (TPC) is committed to protecting the privacy and security of Protected Health Information (PHI) and electronic Protected Health Information (ePHI) in compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act and subsequent regulations. As a covered entity providing health-related services (e.g., HIV/AIDS case management, nutrition counseling, and wellness programs under Ryan White funding), TPC must safeguard PHI to maintain client trust, prevent unauthorized access, and ensure continuity of care.

This policy establishes standards for the use, disclosure, and protection of PHI/ePHI, aligning with:

- HIPAA Privacy Rule (45 CFR Part 160 and Subparts A and E of Part 164)
- HIPAA Security Rule (45 CFR Part 160 and Subparts A and C of Part 164)
- HIPAA Breach Notification Rule (45 CFR §§ 164.400–414)
- 2025 Proposed Amendments to the Security Rule (Federal Register, January 6, 2025), emphasizing enhanced cybersecurity measures, risk analysis, and inventory of ePHI systems
- Florida Statutes (e.g., §381.004 for HIV confidentiality)
- HRSA/Ryan White Program requirements for data security in health services

PHI includes any individually identifiable health information (e.g., diagnoses, treatment plans, HIV status) created or received by TPC, whether oral, written, or electronic. ePHI is PHI transmitted or maintained in electronic form (e.g., via AthenaNet EHR). TPC will use the minimum necessary PHI/ePHI and limit access to those with a legitimate need-to-know.

Procedure

Covered Individuals

This policy applies to all staff (full-time, part-time, contractors), volunteers, interns, board members, business associates (e.g., EHR vendors like AthenaNet), and agents handling PHI/ePHI across Broward, Palm Beach, and Miami-Dade counties.

Privacy Rule Requirements

- **Uses and Disclosures of PHI:** PHI may be used/disclosed without authorization for treatment, payment, and health care operations (e.g., sharing with providers for client care, billing Ryan White services, quality audits). Other disclosures require written authorization or fall under exceptions (e.g., public health reporting for HIV per Florida law). Minimum necessary standard applies—disclose only essential information.
- **Individual Rights:** Clients have the right to:
 - Access and copy their PHI within 30 days (electronic format if requested).
 - Request amendments/corrections to inaccurate PHI.

- Request restrictions on certain uses/disclosures (TPC must agree if for payment/operations and client pays out-of-pocket).
- Receive an accounting of disclosures (up to 6 years).
- Opt out of fundraising communications.
- Direct electronic transmission of ePHI to a third party.
- **Administrative Requirements:** TPC will:
 - Designate a Privacy Officer (CEO or designee) to oversee compliance.
 - Provide a Notice of Privacy Practices to clients upon intake, detailing rights and PHI uses.
 - Maintain policies, training records, and documentation for 6 years.

Security Rule Requirements

- **Risk Analysis and Management:** Conduct annual security risk assessments using tools like the HHS Security Risk Assessment Tool or NIST HIPAA Toolkit. Identify and mitigate threats to ePHI (e.g., via encryption, firewalls). Per 2025 amendments, maintain an accurate inventory of all systems handling ePHI (e.g., AthenaNet, computers, mobile devices).
- **Administrative Safeguards:** Implement workforce security (e.g., role-based access, termination procedures), information access management, security awareness training (annual for all covered individuals), and contingency plans (e.g., data backups, disaster recovery).
- **Physical Safeguards:** Secure facilities (e.g., locked servers, access controls at Wilton Manors and Palm Beach sites), workstations (e.g., auto-logout), and devices (e.g., encryption on laptops).
- **Technical Safeguards:** Use access controls (e.g., unique user IDs, multi-factor authentication in AthenaNet), audit controls (e.g., logging access), integrity measures (e.g., ePHI alteration detection), transmission security (e.g., TLS encryption), and person/entity authentication.

Breach Notification

- **Definition of Breach:** Impermissible use/disclosure of unsecured PHI/ePHI compromising privacy/security (e.g., lost laptop with unencrypted data). Presumed a breach unless risk assessment shows low probability of compromise.
- **Notification Timelines:**
 - **To Individuals:** Without unreasonable delay, no later than 60 days from discovery; via first-class mail/email. Include breach description, affected PHI, mitigation steps, and protective advice (e.g., credit monitoring).
 - **To HHS:** For breaches affecting 500+ individuals, notify within 60 days via HHS portal; for <500, annually by March 1.
 - **To Media:** If 500+ residents in a state/jurisdiction affected, notify prominent media within 60 days.
- **Business Associates:** Must notify TPC within 60 days of breaches; TPC handles client/HHS notifications.

Prohibited Behavior**Training and Oversight**

- All covered individuals receive mandatory HIPAA training upon onboarding and annually, including PHI handling, breach response, and cybersecurity (e.g., phishing awareness).
- The Privacy/Security Officer conducts periodic audits, risk assessments, and updates policies as laws change (e.g., 2025 Security Rule amendments).

Consequences

Violations may result in disciplinary action (up to termination/dismissal), civil/criminal penalties (e.g., up to \$50,000 per violation under HIPAA), and reporting to authorities.

Shared Responsibility

Protecting PHI/ePHI requires cooperation:

- Report breaches or risks immediately to the Privacy Officer without fear of retaliation.
- Supervisors enforce safeguards and monitor compliance.

Communication

- This policy is distributed upon onboarding, posted digitally, and reviewed annually.
- Integrated into Volunteer Handbook, Emergency Plan (for data recovery), and client Notice of Privacy Practices.

Resources

- HHS HIPAA Guidance ([hhs.gov/hipaa](https://www.hhs.gov/hipaa))
- Security Risk Assessment Tool (healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool)
- Florida Department of Health HIV Confidentiality (floridahealth.gov/diseases-and-conditions/aids)

Approvals

Staff/Volunteer Signature:

Date:

Manager's Signature: Thomas Pietrogallo **Date:** 12/15/2025 **CEO**

Signature: Thomas S. Pietrogallo, MSW, LCSW, MBA **Review Date:** 12/15/2025 **BOD**

Approved Date: Revision Pending **Date Established:** 08/15/2016