REFUGE HOUSE, INC. · FY-26 SSCC JOINT MONITORING

# HIPAA, Privacy & Email Encryption — Measures & References

**Purpose:** a single-page map of how Refuge House safeguards protected health information (PHI), protects privacy, and secures electronic transmission, with links to each governing policy/procedure and its regulatory basis. · **Covers Desk Review items:** #12 HIPAA Policy · #18 Encrypted Email Policy/Procedure. · **Updated:** June 16, 2026

PHI safeguards, privacy, and email/transmission encryption are addressed across current, governing sources — the **IT Data Management & Security Policy** and its procedure, the **Personnel Manual & HR Handbook** (E-Mail/Computer Usage, Employee Privacy, Confidentiality & Non-Disclosure, Remote-Work Technology & Security incl. mandatory WPA3 encryption), and the caregiver-facing **Foster/Adoptive Parent Agreement** — supported by workforce training. A comprehensive **2021 HIPAA/IT/Encryption manual** (previously submitted) supplies additional HIPAA-specific detail (email-PHI handling, fax, breach response, minimum-necessary); it is **dated and not the current authority**. No single standalone "HIPAA policy" document is currently maintained in the T3C set; these layered current measures together satisfy the requirement. Refuge House's working standard is to **eliminate PHI transmission by email entirely**, using **Egnyte** secure folders, the **Foster Parent Portal**, and **Pulse** for gated document exchange.

## 1 Administrative, Technical & Physical Safeguards

HIPAA SECURITY RULE

### Multi-layered system security

Azure Active Directory with multi-factor authentication; two-stage authentication (Azure + Radius); Azure Virtual Desktop as the exclusive access method; IP-whitelisted SQL; jurisdiction-based access controls; continuous monitoring via Azure Security Center.

**Governing:** IT Data Management & Security Policy §1.1 | **Reg:** 45 CFR §164.312 (technical safeguards) · §164.310 (physical)

### Access provisioning, role review & termination

System Access Request workflow with supervisor approval; quarterly access attestation; immediate disabling of all accounts on termination (within 1 hour); audit trails and automatic logoff.

**Governing:** IT System Access & Security Procedures | **Reg:** 45 CFR §164.308(a)(3)–(4) (administrative safeguards / access management)

### Device, network & remote-work security (current)

Work performed on Refuge House-managed secure environments — VDI, **Pulse**, and approved Google-secured browser (the agency is transitioning away from VDI-exclusive access toward Pulse and related secure technologies); BYOD restricted; public Wi-Fi prohibited for case data; **WPA3 encryption mandatory** on home networks; physical-document and secure-disposal protocols; company-issued smartphones locked to business use with IT-managed security features; quarterly security training.

**Governing:** Personnel Manual — Remote Work: Technology & Security Requirements; Company-Issued Smartphone Policy | **Reg:** 45 CFR §164.310 (device & media controls)

### Detailed safeguards baseline (reference)

Administrative/technical/physical safeguards, workstation practices, automatic logoff, audit control, data backup/retention, intrusion detection — documented in depth in the prior manual. *Comprehensive but dated (rev. 2021); referenced pending T3C refresh.*

**Reference:** Management of Information — Security & Availability (2021), §§ Safeguards, Security of Information, Audit Control, Automatic Logoff, Data Backup

## 2 Privacy & Confidentiality of PHI

HIPAA PRIVACY RULE

### Confidentiality of records & minimum-necessary use

All childcare records that identify a client are kept confidential; PHI/PII confidentiality and integrity protected; minimum-necessary use and disclosure; uses/disclosures of PHI governed.

**Governing:** IT Policy (PHI/PII protection) | FP Agreement — Confidentiality | Personnel Manual — Confidentiality & Non-Disclosure; Employee Privacy | **Reference:** 2021 manual — Minimum Necessary; Uses & Disclosures of PHI | **Reg:** 45 CFR §164 Subpart E (Privacy)

### Release authorization, privacy statement & social-media limits

Caregiver-facing privacy statement; written release authorization required for non-permitted disclosures; social-media posting about foster children requires DFPS Media Relations pre-approval; no biological-family social-media contact without written approval.

**Governing:** FP Agreement — Privacy Statement & Release | **Reg:** Texas confidentiality of CPA records; 45 CFR §164.508 (authorizations)

### Privacy complaints & non-retaliation

Process for filing privacy/HIPAA complaints with investigation; retaliation prohibited; whistleblower protections.

**Governing:** FP Agreement — Filing a Complaint or Grievance | **Reference:** 2021 manual — Privacy Complaints; Enforcement/Sanctions; Non-Retaliation | **Reg:** 45 CFR §164.530(d),(g)

## 3 Electronic Mail & Transmission Encryption

ITEM #18

### No PHI by email — secure submission channels (current standard)

Refuge House's working standard is to **eliminate transmission of PHI/PII by email**, including between foster parents and Refuge House staff. Documents are submitted instead through gated secure channels: **Egnyte** direct upload to an assigned secure folder (upload-only; no access to other documents) or password-protected, time-limited share links; the **Foster Parent Portal** (gated by a signed privacy & security agreement; device-/email-based token or challenge authentication); **Pulse** secure sharing (token- and challenge-based with 2FA); or physical delivery. The remaining obstacle is behavioral, addressed through the FP Agreement commitment and training.

**Governing:** FP Agreement — Documentation & Reporting §5 (No PHI by Email) | **Reg:** 45 CFR §164.312(e) (transmission security)

### Secure email & data encryption

Secure email is the required channel for access requests, terminations, and external-access provisioning; data encryption is verified for system integrations (SSO); cloud infrastructure on Microsoft Azure with enterprise encryption in transit and at rest.

**Governing:** IT System Access & Security Procedures (secure email; data-encryption verification) | IT Policy §1.1 (Azure security) | Personnel Manual — E-Mail & Computer Usage | **Reg:** 45 CFR §164.312(e) (transmission security)

### Electronic mail containing PHI & fax transmission

Dedicated handling rules for email containing PHI (user responsibilities, prohibited uses, confidentiality, retention) and for fax transmission/misdirected faxes — documented in depth in the prior manual. *Dated (2021); referenced pending T3C refresh.*

**Reference:** 2021 manual — Policy for Electronic Mail Containing PHI; Policy for Fax Transmission | **Reg:** 45 CFR §164.312(e)(2)(ii) (encryption)

## 4 Breach Notification & Incident Response

HIPAA BREACH RULE

### Data-breach detection & response

Staff report suspicious activity/phishing immediately to the **Security Lead** (Director of Operational Development — Jeannie Duarte — with F1IT technical support) and **Privacy Co-Leads** (Lindsay Reed — Compliance & Cross System; Brittney Wilson — HRQAD/QA); intrusion detection; defined response to a suspected or confirmed data breach.

**Governing:** IT System Access & Security Procedures (incident reporting) | **Reference:** 2021 manual — Intrusion Detection; Response to a Suspected/Confirmed Data Breach | **Reg:** 45 CFR §164 Subpart D (Breach Notification)

## 5 Workforce Training

ANNUAL

### HIPAA & cybersecurity training

HIPAA training (2 hrs) and Cybersecurity training (1 hr) are part of the required caregiver/staff curriculum; pre-service and annual.

**Governing:** FP Agreement — Appendix IV (Training) | FC-16 Staff & Caregiver Training |
**Reg:** 45 CFR §164.308(a)(5) (security awareness training)

### REQUIREMENT → SOURCE MAP (AT A GLANCE)

| REQUIREMENT | CURRENT GOVERNING SOURCE | BASIS |
|---|---|---|
| System security safeguards (access, MFA, monitoring, logoff, audit) | IT Policy §1.1 + IT System Access Procedures | 45 CFR §164.308/.310/.312 |
| Confidentiality & minimum-necessary use of PHI/PII | IT Policy + FP Agreement (Confidentiality) | 45 CFR §164 Subpart E |
| Privacy statement, release authorization, social-media limits | FP Agreement (Privacy Statement & Release) | 45 CFR §164.508; Texas confidentiality |
| Privacy/HIPAA complaints & non-retaliation | FP Agreement (Grievance) + 2021 manual | 45 CFR §164.530(d),(g) |
| Secure email / transmission encryption | IT System Access Procedures + IT Policy (Azure) | 45 CFR §164.312(e) |
| Email containing PHI; fax transmission | Personnel Manual (E-Mail & Computer Usage); 2021 manual detail | 45 CFR §164.312(e)(2)(ii) |
| Breach detection & notification | IT System Access Procedures + 2021 manual | 45 CFR §164 Subpart D |
| HIPAA & cybersecurity workforce training | FP Agreement Appendix IV + FC-16 | 45 CFR §164.308(a)(5) |



**Note** The 2021 manual is referenced for its detailed safeguards only and is **not** the current governing authority; where it conflicts with the T3C IT Policy or the FP Agreement, the current documents control.