Case Study — Mental Healthcare Center

Accelerating HIPAA-Ready Security & Resilience — Fidantis Strategies

Client

A multi-site mental healthcare center serving outpatient behavioral health patients. Core stack includes Microsoft 365 Business Premium, Paubox secure email, and MFA across key services.

Situation

Strong foundations are in place (M365 + Paubox + MFA), but there is no centralized visibility or unified governance. Without correlated monitoring, incidents or compliance violations could go undetected. HIPAA risk analysis is not formally documented; endpoint/device visibility is fragmented across Mac/Windows; there is no SIEM/centralized audit trail; control documentation and BAAs are scattered; and no tested DR plan exists.

- No unified risk visibility across EHR, telehealth, and collaboration tools
- HIPAA Security Risk Analysis (45 CFR §164.308(a)(1)) not formally documented
- No centralized endpoint/device visibility (mixed Mac/Windows)
- No SIEM or centralized audit trails to satisfy HIPAA/insurer audits
- BAA and control documentation dispersed across tools
- No documented ransomware recovery or DR plan

What We Implemented (Phased)

Phase 1 — M365 Security Hardening (Zero New Cost)

- Conditional Access with device compliance gating for PHI
- Encrypt OneDrive/SharePoint; tune Defender for Office 365 (phish/malware)
- Enable Entra ID risk policies (credential/sign-in risk)

Phase 2 — Unified Endpoint Security & Compliance

- Deploy Intune for MDM and compliance enforcement (Mac + Windows)
- Enable FileVault/BitLocker; automate OS/software patching
- Activate Defender for Endpoint for EDR and remote wipe

Phase 3 — Automated GRC & Audit Readiness (HIPAA + NIST)

- Map policies → controls; validate HIPAA safeguards (admin/physical/technical)
- Run NIST SRA Tool assessment; CMS Promoting Interoperability (optional)
- GRC dashboard (BAAs, incidents, training, reviews); quarterly phishing sims
- VA/PT; Incident Response tabletop and quarterly light tabletops

Phase 4 — Recovery Planning & Resilience

- Define RTO/RPO and document DR/Continuity playbooks
- Backup/restore verification with evidence capture; named owners and runbooks
- Schedule periodic restore drills and plan updates

Expected Outcomes

- HIPAA defensibility: documented evidence and audit trail
- Operational efficiency: automated patching, monitoring, risk tracking
- Resilience: DR/IR procedures and tested recovery readiness
- Governance: unified risk register, policy mapping, quarterly dashboards
- Zero-cost optimization: maximize existing M365 Business Premium controls

At-a-Glance

Industry: Behavioral Health

Stack: M365 BP, Paubox

Endpoints: Mac/Windows via Intune

Controls: MFA, Conditional Access

Scope: M365 hardening, Endpoint mgmt, HIPAA+NIST GRC, DR plan

Next Steps

- Approve scope and designate a single point of contact (SPOC)
- Schedule 2-hour kickoff workshop
- Provide M365 admin access for configuration review
- Confirm optional components (SRA, CMS PI, tabletops, VA/PT)