IT Manager - Healthcare Systems & Security (M365/Entra, Intune, SonicWall, PACS/DICOM, HIPAA)

SUMMARY

- Operate HIPAA-aligned identity, endpoint, email security, and networks for 12 practices and 3 surgery centers across 30+ clinical/office locations.
- Enforced Entra ID Conditional Access with MFA for 100% of users; standardized Intune compliance and device provisioning; SonicWall segmentation; zero-trust patterns (802.1X/RADIUS, VPN).
- Deployed and administered kiosk systems for clinical use and patient check-in with locked-down profiles to protect ePHI.
- Mapped controls and maintained audit artifacts for HIPAA Security Rule (45 CFR Part 164), 405(d) HICP, NIST CSF, CIS Controls v8; verified RPO <= 2 hours for EMR/PACS; zero reportable PHI incidents since 2017.

CORE SKILLS

Entra ID (Conditional Access, MFA, SSO) | Intune (compliance, provisioning) | Microsoft Defender for Endpoint & Office 365 | Exchange Online hygiene (SPF/DKIM/DMARC)
SonicWall (SD-WAN, DPI-SSL) | VLAN / 802.1X / RADIUS | Site-to-site VPN, DNS filtering | PACS/DICOM (Orthanc, dcm4chee, Horos/OsiriX)
Microsoft Sentinel (analytics and alert triage) | CIS Controls v8 / NIST CSF | HIPAA Security Rule / 405(d) HICP | Business Continuity & DR (RPO <= 2h) | Incident Response playbooks

PROFESSIONAL EXPERIENCE

Small MSP - Senior IT Consultant & Team Lead | 2015 - Present

Scope: 12 practices + 3 surgery centers | 30+ locations | multi-site healthcare network
- Identity & Email: Enforced Entra ID Conditional Access and MFA for 100% of users; closed legacy protocols; aligned SPF/DKIM and enforced DMARC to reduce spoofing/BEC risk.
- Endpoint: Standardized Intune compliance (BitLocker, AV, firewall, baselines); removed local admin; strengthened device posture.
- Clinical Kiosks: Deployed and administered kiosk systems (locked-down profiles via MDM) for clinics and surgery centers to minimize ePHI exposure during check-in and clinical workflows.
- Network & Segmentation: Delivered SonicWall SD-WAN and site-to-site VPN; segmented PACS/EMR/guest VLANs; implemented 802.1X/RADIUS on staff networks to reduce lateral movement.
- Detection & Response: Tuned Microsoft Defender for Endpoint/Office 365 alerts; Microsoft Sentinel basic analytics and alert triage; exercised incident runbooks in tabletop sessions.
- Business Continuity & DR: Documented and tested recovery procedures with RPO <= 2 hours for EMR and PACS; validated backups and restores.
- Compliance & Outcomes: Mapped controls to HIPAA Security Rule (45 CFR Part 164), 405(d) HICP, NIST CSF, CIS Controls v8; maintained access reviews, asset inventory, backup logs, and risk register; zero reportable PHI incidents 2017 - 2025.

EARLY CAREER (MSP & Transportation) | 2012 - 2015

Small MSP - IT Support / Network & Security

- Hardened Windows/Linux servers and enforced security protocols; managed firewalls and VPN access for multi-site clients.
- Secured GPS/tracking software and web applications used in fleet/operations; applied access control, patching, and AV/EPP standards.
- Supported communications and line-of-business applications; triaged tickets and escalations across network, systems, and cybersecurity.
- Assisted with incident response activities and post-incident reviews; improved SOPs for change control and backup verification.

EDUCATION & CERTIFICATIONS

- University of Gujarat - B.Sc. IT | 2005 - 2011
- CCNA - Cisco | 2012
- Certified HIPAA Privacy Security Expert - CHPSE - valid through 2026