TECHGUARD LABS FOUNDATION

Healthcare Cybersecurity

Israel-India HealthSecure · Coimbatore, Tamil Nadu

~22%

of All Cyberattacks in India

target healthcare — more than any other sector. (Seqrite 2025)

38%

Rise in Patient Mortality

linked to ransomware attacks on hospitals. (HIPAA 2025)

₹450 Cr

Maximum DPDP Act penalties

For failure to safeguard and notify within 6-hour (DPDP 2025)

TECHGUARD HEALTHSECURE

PHI Data Protection Controls

Automated discovery tooling maps every system, application, and integration touching PHI — including shadow IT. Access rights are audited against the HIPAA minimum necessary standard and least-privilege principles, with excess privileges removed and role-based controls enforced. Audit logging is configured to capture every PHI interaction in a HIPAA-compliant, investigation-ready format.

✓ **PHI data map, access control remediation, and audit-ready logging.**

Secure Network Segmentation

Current network architecture is mapped and assessed against the NIST healthcare segmentation guidelines and zero-trust principles. A segmentation blueprint is produced specifying VLAN structure, firewall rule logic, and access policy at each boundary, with a phased rollout sequence designed to avoid disruption to live clinical systems.

✓ **Segmentation blueprint with VLAN design, firewall rules, and phased rollout plan.**

Medical Device / IoMT Security Assessment

Smart network scanning builds a full inventory of every connected device — clinical and non-clinical. Each device is assessed for firmware vulnerabilities, open ports, default credentials, and vendor patch support. Risk is ranked by exploitability and clinical impact; unpatchable devices are marked and specific network-level compensating controls are recommended.

✓ **Device inventory, CVE-ranked risk register, and compensating control recommendations**

Ransomware Readiness and Downtime Procedures

Backup architecture and recovery timelines are tested against real ransomware attack scenarios to identify where recovery assumptions break down. Written downtime procedures are developed per critical unit — pharmacy, ICU, ED, imaging — covering how staff operate without system access. Validated in a live incident-response drill.

✓ **Unit-level downtime procedures and recovery gap report.**

Quick Self-Check

☐ How long would our operations be down after a ransomware attack?

☐ What's the level of access that our third-party vendors have to our systems?

☐ Are our medical devices running updated, supported software?

☐ Would we know if a staff member was exfiltrating patient data?

"No" = you have an open door.

Why TechGuard

- **Israeli Battle-tested cyber methodologies**
  ERA IT Consulting & Audit (est. 2008) + Ariel University partnership
- **Local Coimbatore team**
  On-site delivery — no international consultant travel costs
- **Clinical-Environment Expertise**
  Cybersecurity assessments built for hospitals, developed in partnership with SNR Hospital (Coimbatore)
- **Legal compliance**
  DPDP Act, HIPAA, and CERT-In compliance integrated into every engagement

What Happens Without Protection — Real India Cases

Sant Parmanand & NKS Hospitals | Jun 2025

Ransomware attack across two North Delhi hospitals overnight. 60,000+ patient records encrypted. Billing, EMR, and appointment systems knocked offline — staff forced to manual operations. FIR filed under IT Act Section 66.

Entry: *Phishing email; spread through unsegmented network*

AIIMS Delhi | Mar 2022

40 million patient profiles stolen, ransom demand of ₹200 crore, hospital offline for 15 days.

Entry: *Phishing email attachment*

DavaIndia Pharmacy | Feb 2026

883 store profiles, 17,000+ customer orders, pharmacist PINs, drug control functions all accessible

Entry: *Exposed API - no authentication required; discovered externally*

Protect Your Cyber Health Today.

techguardlabs.com · info@techguardlabs.com · Coimbatore, Tamil Nadu | Israel

Ariel University (Israel) | ERA IT Consulting & Audit | SNR Sons Charitable Trust | SREC | Promitei Ltd