SERKET-TECH SECURITY

Securing Healthcare in a Connected World

Cybersecurity, compliance, and resilience services for providers, practices, digital health companies, and healthcare-adjacent organizations.

Protect ePHI, reduce compliance friction, and strengthen resilience across healthcare operations.

Healthcare organizations and business associates manage ePHI, clinical records, payment data, and other sensitive information across EHRs, cloud platforms, collaboration tools, connected technologies, and third-party providers. Regulators, payers, partners, patients, and leadership now expect stronger security evidence, faster readiness for response, and tighter control over vendor risk.

Serket-Tech Security helps healthcare teams build practical security programs that align with how care delivery, claims, and digital workflows maneuver through the business. Our work spans governance, assurance, testing, response, managed protection, and executive guidance without losing sight of patient care, operations, or growth.

Protect ePHI and Patient Trust

Secure email, collaboration, endpoints, and clinical or business data flows with controls that fit healthcare operations and protect regulated information.

Reduce Audit and Partner Friction

Prepare for HIPAA reviews, payer and partner questionnaires, cyber insurance reviews, and customer diligence with clearer evidence and stronger program structure.

Strengthen Business Associate and Vendor Oversight

Evaluate EHR, revenue cycle, telehealth, imaging, cloud, and other third-party platforms that handle regulated data or support core operations.

Prepare for Ransomware and Care Disruption

Improve incident response, downtime planning, executive decision-making, and recovery before a breach or outage affects patients, staff, scheduling, claims, or revenue operations.

Best fit for health systems, hospitals, physician groups, specialty clinics, ambulatory and behavioral health organizations, digital health companies, healthcare IT vendors, MSOs, and business associates handling regulated data or critical operations.

SERKET-TECH SECURITY

Comprehensive Service Portfolio

A single partner that can support program development, technical validation, response readiness, and ongoing operations across the healthcare security lifecycle.

Governance, Risk, and Compliance

- HIPAA security and privacy program support
- Risk analysis, policy development, and control design
- Regulatory, contractual, and partner requirement mapping

Data Protection and Workflow Security

- Identity, endpoint, email, and collaboration hardening
- Encryption, access control, segmentation, and least privilege design
- EHR, cloud, and sensitive data workflow protection

Third-Party and Business Associate Risk

- Vendor due diligence and business associate review support
- Stronger oversight workflows for outsourced services and SaaS platforms
- Remediation tracking, reporting, and evidence collection

Security Assessments and Testing

- Security posture and maturity assessments
- Architecture and control reviews
- Vulnerability assessments and remediation planning

Assurance and Trust Support

- SOC 2 readiness and attestation support for healthcare tech and service providers
- HITRUST readiness and certification path support where validated assurance is required
- Evidence planning, remediation, and control ownership

Executive Leadership and Program Development

- Fractional CISO support
- Cybersecurity strategy and roadmap reviews
- Executive briefings, board reporting, and program governance

Incident Response, Resilience, and Managed Services

- Tabletop exercises, breach support, and forensic coordination
- Monitoring, detection, and response support
- Ongoing control monitoring and issue tracking

Penetration Testing and Validation

- External and internal network testing
- Web application, cloud, and identity testing
- Prioritized findings and retest support

Programs can be tailored to HIPAA, HITECH, OCR audit readiness, HICP/405(d), NIST, HITRUST, payer and partner requirements, and integration activity.

SERKET-TECH SECURITY

Built for Healthcare Sector Realities

Serket-Tech Security focuses on the issues healthcare leaders and adjacent service providers are under pressure to solve now, while keeping the full service set broad enough to support one-time projects or ongoing programs.

- **ePHI Protection and Care Operations**
  Protect EHR-connected systems, collaboration tools, mobile endpoints, and shared workflows that store, move, or expose patient and employee data.
- **Ransomware, Downtime, and Patient Safety**
  Reduce exposure to phishing, identity compromise, unpatched systems, and recovery gaps that can disrupt care delivery, scheduling, claims processing, or revenue cycle operations.
- **Business Associate and Partner Expectations**
  Respond to hospital, payer, and enterprise customer diligence with clearer controls, stronger evidence, and better follow-through on remediation.
- **AI, Telehealth, and Connected Care Governance**
  Set guardrails for AI, remote care, third-party platforms, and connected technologies to ensure security, privacy, access, and oversight remain in focus.

How Clients Engage Serket-Tech Security

Engagements can start with a readiness review, targeted assessment, tabletop exercise, penetration test, assurance initiative, or recurring advisory and managed support program.

1. Assess
Review current posture, obligations, gaps, and business priorities.

2. Prioritize
Define the roadmap, sequence remediation, and assign owners.

3. Implement
Deploy controls, perform testing, support reviews, and close gaps.

4. Operate
Monitor, report, respond, and keep the program up to date.

Representative clients include hospitals and health systems, physician and specialty practices, ambulatory and behavioral health organizations, digital health companies, healthcare IT vendors, MSOs, revenue cycle providers, and other business associates serving covered entities.

Build a healthcare security program that is audit-ready, incident-ready, and aligned to patient care and business operations.