For General Distribution

⚠ CURRENT THREAT LEVEL: HIGH — IMMEDIATE ACTION RECOMMENDED

Executive Summary

Escalating U.S.-Iran military tensions have produced a materially elevated cyber threat to U.S. healthcare. **Healthcare is a primary target** — its operational sensitivity, vast PHI stores, and interconnected clinical systems make it ideal for Iranian actors seeking asymmetric leverage. Compounding this risk: CISA is operating with **significantly reduced capacity** due to recent staffing cuts, limiting the early-warning support the sector normally relies upon.

Healthcare organizations are prime targets for cyberattacks due to the life-or-death impact of downtime, the high value of PHI and PII, complex third-party integrations, and historically under-resourced security programs. Confirmed intrusions by groups such as Pioneer Kitten, combined with mandatory breach reporting requirements, further increase both the likelihood and strategic visibility of attacks.

All recommendations below are vendor-neutral and prioritize timely action.

Key Iranian Threat Actors

Actor	Healthcare Relevance
Charming Kitten (APT35/42)	**HIGH —** Spear-phishing of clinical and admin staff
Pioneer Kitten (Fox Kitten)	**CRITICAL —** Confirmed U.S. healthcare intrusions via VPN exploitation
Agrius (Pink Sandstorm)	**HIGH —** Wiper malware disguised as ransomware; recovery without backups may be impossible

Expected Attack Methods

Spear-phishing of clinical, admin, and IT staff · Credential theft targeting VPN and cloud access · **Unpatched VPN/firewall exploitation (cross-ref CISA KEV)** · Third-party/MSP/EHR supply chain compromise · **Wiper malware disguised as ransomware** · DDoS against patient portals and scheduling systems

Recommended Immediate Actions

1	**Patch internet-facing systems immediately** Prioritize VPN appliances, firewalls, and web servers. Cross-reference CISA KEV (cisa.gov/kev). Patch now — do not wait for maintenance windows.	2	**Issue a phishing awareness alert to all staff** Alert all clinical, admin, and IT staff. Spear-phishing is Iran's primary entry vector. Provide examples of lures tied to geopolitical news and HR notifications.
3	**Audit and restrict all third-party vendor access** Review all MSP, billing, and EHR connections. Revoke unnecessary access. Enforce MFA for every vendor account. No exceptions.	4	**Verify and test backup and recovery posture** Ensure offline or air-gapped backups exist for critical systems. Confirm RTO and RPO. Run a restoration test — wiper attacks make recovery impossible without backups.
5	**Activate enhanced monitoring and detection** Increase log retention. Alert on unusual auth events, lateral movement, and anomalous transfers. Focus on privileged accounts and after-hours logins.	6	**Review and rehearse your incident response plan** Confirm escalation paths and vendor contacts are current. Conduct a tabletop exercise if none in the past six months. Know who calls whom first.
7	**Subscribe to H-ISAC for sector intelligence** H-ISAC (h-isac.org) is the authoritative healthcare threat intel source. Subscribe to TLP:AMBER feeds for actionable IOCs and healthcare-specific advisories.	8	**Implement geographic network restrictions** Block or alert on inbound traffic from high-risk geographies. Monitor outbound for suspicious foreign connections. Geo-blocking is one layer only — state actors route through U.S. infrastructure.

Additional Resources and Ongoing Monitoring

Resource	Description
H-ISAC *h-isac.org*	Authoritative healthcare-specific threat intelligence. Subscribe to TLP:AMBER feeds for actionable IOCs and healthcare-targeted advisories. Where relevant indicators surface first.
CISA Healthcare *cisa.gov/healthcare*	CISA healthcare cybersecurity resources and the Known Exploited Vulnerabilities (KEV) catalog. Note: CISA is currently operating with reduced capacity. Supplement with H-ISAC monitoring.
CISA KEV Catalog *cisa.gov/kev*	Definitive list of vulnerabilities under active exploitation. Cross-reference your exposed systems immediately and patch in priority order before any other vulnerability management work.
MITRE ATT&CK *attack.mitre.org*	Reference the APT35 (Charming Kitten) and Pioneer Kitten group pages for detailed TTPs, detection opportunities, and defensive mitigations mapped to your security tooling.

This is not a theoretical risk.

The current geopolitical environment represents an active, elevated threat period. Healthcare organizations should treat this bulletin as a call to verify readiness — not wait for an incident to occur.

This bulletin is prepared for informational purposes for healthcare executive and security leadership. Distribution to relevant internal stakeholders is encouraged. All recommendations are vendor-neutral and do not constitute legal, regulatory, or product-specific guidance. Based on publicly available threat intelligence current as of issue date.

Resources: H-ISAC (h-isac.org) · CISA Healthcare (cisa.gov/healthcare · CISA KEV (cisa.gov/kev) · MITRE ATT&CK (attack.mitre.org)