Executive Summary

The healthcare sector enters March 2026 facing a professionalized and lethal threat landscape that has transcended traditional data theft to become a primary patient safety crisis. Adversaries are currently prioritizing operational paralysis and "extortion-only" models to maximize leverage. The first quarter of 2026 has been defined by high-impact ransomware incidents, resulting in it impacting a major healthcare organization in the US, and the continued fallout from massive third-party breaches impacting tens of millions of records. Nation-state actors, particularly those with a North Korea-nexus, are increasingly utilizing Ransomware-as-a-Service (RaaS) to generate illicit revenue while targeting critical clinical infrastructure. Organizations must immediately pivot from reactive patching to a risk-based strategy that emphasizes identity resilience, Operational Technology (OT) segmentation, and aggressive third-party risk management**.**

Active Threat Campaigns

Campaign	Type	Targets	Key Technique	Priority Action
Lazarus Group & Medusa RaaS Integration	Financial, Espionage	Healthcare (US)	A significant 2026 campaign involves the North Korea-linked Lazarus Group deploying Medusa ransomware against U.S. healthcare providers and non-profits. This campaign utilizes complex loaders like **SUBLIME.V2** to establish persistent access before deploying encryption. The average ransom demand observed in this campaign is approximately **$260,000**, with attackers specifically targeting medical research data and corporate employee information to facilitate secondary espionage objectives.	Patching with Windows Update
The Rise of Extortion-Only Syndicates (Insomnia)	Financial	Healthcare (US)	The emergence of the **Insomnia** data theft group represents a strategic shift in active campaigns. Unlike traditional ransomware, Insomnia focuses on stealthy exfiltration without system encryption. They leverage credentials sourced from infostealers and abuse legitimate cloud infrastructure for lateral movement. By early March 2026, they have listed multiple U.S. health entities, on their leak site to drive payouts through the threat of sensitive medical record exposure.	Patching, User education around phishing campaigns, MFA
OT-to-Clinical Lateral Movement	Financial	Healthcare (US)	Recent 2026 campaigns have demonstrated a refined ability to pivot from unpatched building management systems (HVAC and electrical controllers) into sensitive clinical networks. Adversaries are increasingly targeting **DICOM imaging networks** to cripple	Review network segmentation and micros-segmentation in addition to ensuring security monitoring with network intrusion detection tools

			radiology departments, targeting a major healthcare entity, which necessitated entity closures. These attacks often bypass traditional IT security because the targeted OT systems do not support standard endpoint detection agents.	
Supply Chain & Third-Party Fallout	Financial	Healthcare (US)	The fallout from breaches at administrative vendors remains an active threat vector. Notifications regarding breaches impacting over **25 million individuals**—continue to reach members of major health plans as of March 2026. Simultaneously, other incidents from March, have active data exposure notifications, highlighting the cascading risk where a single vendor compromise simultaneously affects hundreds of downstream healthcare delivery organizations.	Audit your high risk third party vendors handling PHI. Managing third party risk by ensuring they have adequate security controls in place through evidence based auditing.

Top Actions This Week

1. **Immediate Vulnerability Remediation**
   Organizations should prioritize patching CVE-2025-59287 (Windows Server Update Services) and CVE-2025-53770 (Microsoft SharePoint), both of which are being actively exploited in the wild to deploy web shells and ransomware in clinical environments. If immediate patching is not feasible, these systems should be isolated from the primary clinical network.
2. **Resilience Against AI-Enhanced Vishing**
   Given that 1 in 6 breaches in early 2026 involve AI-driven social engineering, IT help desks must be alerted to a surge in deepfake audio vishing. Attackers are successfully impersonating high-level executives or vendors to reset MFA tokens. Verification protocols for credential resets should move away from voice-only confirmation to out-of-band, multi-step physical verification.
3. **Segmentation of Imaging & OT Networks**
   Following the UMMC shutdown, security teams should immediately audit the connectivity between building automation systems and medical imaging (DICOM) networks. Implementing strict network segmentation and micro-segmentation around these assets is critical to prevent a compromise in non-clinical systems from escalating into a clinical diversion event.
4. **Business Associate (BA) Security Audit**
   Perform an emergency review of security requirements for all third-party business associates handling PHI. As over 50% of people affected by 2025-2026 breaches were compromised via third parties, organizations should require vendors to provide evidence of phishing-resistant MFA and recent penetration test results as a condition of continued data sharing prerequisite.

Resources: Google Threat Intelligence | MITRE ATT&CK (attack.mitre.org) | CISA Alerts (cisa.gov)