cowbell

Cyber Threats Targeting the Healthcare Sector

Notable incidents, threat actors, and mitigations for healthcare organizations across the US, UK, and Australia

Executive Summary

Ransomware and social engineering remain the most prominent attack vectors against healthcare organizations across the United States, United Kingdom, and Australia. Healthcare organizations continue to be high-value targets for data theft operators due to their valuable patient data and high-level of operational dependence on connected medical devices (IoMT).

Cowbell's intelligence reveals an increasing threat of third-party compromises impacting healthcare organizations, driven by vendor breaches stemming from the sector's complex supply chains. These attacks have critical consequences that go far beyond financial losses, directly impacting patient safety, resulting in class action lawsuits, regulatory penalties, bankruptcies, and potential loss of life. This white paper outlines the regional threat landscapes, profiles notable incidents, and provides a sound approach to digital resilience for the healthcare sector.

Matthieu Chan Tsin
SVP & General Manager, Cowbell Resiliency Services

Strengthening cyber resilience alongside tailored cyber insurance is crucial to avoiding catastrophic losses. Cowbell Resiliency Services equips policyholders with the tools and expertise to proactively detect and mitigate vulnerabilities, fortify infrastructure, and counter evolving threats.

Additional questions? Request a consultation.

Our experts are happy to explain the process in more detail and address any issues you may have.

Notable Cyber Incidents: United States

For US businesses, a cyber incident in healthcare is no longer just an IT issue; it is an existential business threat. The average daily loss associated with a cyber incident in US healthcare can cost close to $1,000,000 due to operational downtime, and class-action lawsuits are becoming the standard aftermath of any patient data exposure.

We must help our healthcare and medical billing policyholders structure the right Cyber and Professional Lines coverage to survive these third- party vendor breaches, secure their operations, and protect patient trust.

Pecan Tree Dental

In January 2026, the ransomware group Sinobi breached this Texas-based dental practice, affecting approximately 13,300 individuals. The group demanded a $5 million ransom and published sensitive Protected Health Information (PHI), financial documentation, and patient data on their dark web leak site.

Susan B. Allen Memorial Hospital

In July 2025, ransomware collective Kawa4096 forced a broad system outage at this Kansas-based hospital to contain a threat, compromising the personal information of 12,097 individuals. The attack triggered multiple class-action lawsuits alleging the hospital failed to implement adequate security measures and delayed HIPAA breach notifications.

Medusind Solutions (Third-Party Breach)

A prominent Florida healthcare revenue cycle management firm discovered an unauthorized access incident that impacted more than 701,000 patients. In June 2025, Medusind agreed to a $5 million settlement to resolve consolidated class action lawsuits.

H2-Pharma (BEC Fraud)

In 2026, this US-based pharmaceutical company experienced a sophisticated business email compromise (BEC) attack resulting in losses over $7.3 million. Attackers used a deceptive homoglyph domain to trick an employee into sending payments to a fraudulent account instead of the intended vendor.

Notable Cyber Incidents: United Kingdom

The decentralized structure of NHS Trusts, combined with shared IT infrastructure and legacy systems, provides significant opportunities for ransomware operators. For UK brokers, the tragic real-world consequences of these attacks - such as the operational paralysis stemming from the Synnovis breach - highlight why proactive risk management is essential. Our role is to provide healthcare organizations and their critical supply chain vendors with the clear, adaptive coverage required to maintain patient safety and operational continuity.

Claud Bilbao
VP, Underwriting & Distribution UK & Australia

Synnovis Supply Chain Attack Fallout

Following the June 2024 ransomware attack on London pathology services provider Synnovis, King's College Hospital NHS Foundation Trust confirmed in June 2025 that the cyberattack was a contributing factor leading to a patient's unexpected death due to a long wait for a blood test result.

UCLH and Southampton NHS Trusts

In May 2025, attackers exploited the CVE-2023-35078 vulnerability in Ivanti Endpoint Manager Mobile (EPMM) to target mobile device management systems across these NHS Trusts. The attack focused on long-term data exfiltration rather than encryption.

Vishing Campaigns

In 2025, the NHS Counter Fraud Authority warned of fraudulent automated calls impersonating NHS staff. Attackers used high-pressure language to manipulate patients into revealing personal and financial information, such as National Insurance Numbers.

NRS Healthcare Liquidation

Following a 2024 ransomware attack that compromised 578GB of sensitive patient data, this medical equipment provider faced an expensive recovery process that contributed to its deteriorating financial situation. In mid-2025, NRS Healthcare entered compulsory liquidation.

Notable Cyber Incidents: Australia

The Australian healthcare sector is increasingly targeted by threat actors aiming at third-party vendors and smaller connected systems to access highly sensitive medical records. The financial and reputational fallout is severe; we saw MediSecure pushed into total insolvency following a breach. Australian brokers play a vital role in simplifying these complex, emerging risks, ensuring that clinics, hospitals, and medical software providers have the resilient protection they need to operate confidently.

Anthony Wall
Head of Underwriting (Australia)

Genea

In February 2025, the Termite ransomware group breached Genea, one of Australia's largest IVF and fertility providers, via a Citrix server. The threat actors exfiltrated approximately 940.7 GB of patient data, including sensitive genetic information, donor details, and family records from the BabySentry patient management system.

Hyperdome Doctors and Skin Clinic

In December 2025, the SafePay ransomware group targeted this Queensland-based clinic, compromising practitioner files and patient-related personal information. The release of this data on SafePay's leak site created significant secondary exposure for patients.

Harbour Town Doctors

In December 2025, the Rhysida ransomware group attacked this medical clinic, demanding a ransom of approximately AUD $496,343 to prevent the full release of over 3.8 million files, including patient health summaries and pathology records.

Threat Actor Profiles

Threat actors targeting healthcare organizations operate predominantly under ransomware-as-a-service (RaaS) models and are primarily financially motivated.

- **Sinobi:** An aggressive RaaS group that emerged in mid-2025, ranked among the top operators targeting healthcare. Sinobi focuses on mid-market organizations and outpatient settings, using double-extortion tactics.
- **Termite:** This group aggressively targets environment-specific vulnerabilities and has recently attacked several organizations globally, combining data exfiltration with file encryption to maximize pressure.
- **SafePay & Kawa4096:** Emerging groups demonstrating the volatility of the ransomware ecosystem, quickly launching data-theft extortion campaigns against clinics and hospitals.

Intelligence Sharing & Resources

- **ISACs (Global/Regional):** Participating in groups like Health-ISAC and CI-ISAC Australia provides real-time threat intelligence and critical alerts tailored to healthcare.
- **Aus3C (Australia):** The Australian Cyber Collaboration Centre provides advanced training and testing facilities to foster a secure cyber ecosystem.
- **NHS England Digital (UK):** Safeguards patient data through the Data Security and Protection Toolkit (DSPT) and Cyber Security Operations Centre (CSOC).

The Sound Approach to Risk: Recommendations

Digital risks are real, but they are manageable with sound protection. Healthcare organizations must adopt a proactive, resilience-focused posture.

- **Implement Robust Third-Party Risk Management (TPRM):** Regular risk analysis is required to understand how PHI is shared with external partners. Enforce regular evaluations of vendors' cybersecurity practices to ensure they meet industry security standards.
- **Introduce Endpoint Protection and Security Software:** Deploy comprehensive endpoint detection and response (EDR) tools and centralized monitoring systems across all devices to identify suspicious activity early.
- **Conduct Regular Backup and Recovery Testing:** Creating backups is insufficient; organizations must test the restoration process regularly to verify data integrity and confirm that recovery procedures can be executed effectively in real-world scenarios.

Cowbell: The Sound Approach to Risk

Cowbell delivers insurance that cuts through complexity and adapts as risks evolve. With streamlined quoting, expert guidance, and protection designed for the realities of today's threats, we make coverage easier to understand and more reliable when it matters most. Behind it all is the Hum—our constant, quiet vigilance—building stronger businesses, trusted partnerships, and the quiet confidence to keep moving forward.

cowbell®

US0067 0726