MORPHISEC | omega systems technology managed

Top 10 Cyber Crises That Shook Healthcare

How attacks impacted millions of patients and reshaped healthcare cybersecurity in 2024-2026.

Over 25 million records compromised.
Entire hospitals forced to shut down.
These are the attacks that changed the healthcare landscape.

THE TOP 10 ATTACKS (WITH ROOT CAUSES)

Each attack entry will include the following structured details:

1 PIH HEALTH HOSPITALS RANSOMWARE ATTACK

Date:	December 2024
Impact:	Disruption of operations across all branches serving 3 million patients, with critical health record systems becoming inaccessible.
Root Cause:	Ransomware exploited outdated endpoint security across hospital networks.
Key Lesson:	Implement advanced endpoint detection tools to neutralize ransomware before execution.
Source:	https://www.hipaajournal.com/pih-health-data-breach-ransomware/

2 SIMONMED IMAGING BREACH

Date:	January 2025
Impact:	1.27 million patient records locked, causing delays to critical imaging services and diagnostics.
Root Cause:	Ransomware infiltrated due to a lack of segmentation between diagnostic servers and core IT services.
Key Lesson:	Network isolation for high-traffic imaging services can reduce lateral ransomware movement.
Source:	https://www.hipaajournal.com/simonmed-imaging-confirms-january-2025-cyberattack/

3 ANNE ARUNDEL DERMATOLOGY BREACH

Date:	Early 2025
Impact:	Breach exposed records of 1.9 million patients (second attack in a year).
Root Cause:	Weak internal security practices and insufficient patch management left exploitable gaps.
Key Lesson:	Establish continuous vulnerability management programs to address recurring risks.
Source:	https://www.hipaajournal.com/anne-arundel-dermatology-data-breach-settlement/

4 MCLAREN HEALTH CARE RANSOMWARE ATTACK

Date:	August 2024
Impact:	743,000 patient files encrypted by ransomware, delaying patient treatments and outcomes.
Root Cause:	Insider threats and poor logging allowed attackers to exfiltrate admin credentials.
Key Lesson:	Implement tighter identity governance and user access controls (e.g., MFA).
Source:	https://www.hipaajournal.com/mclaren-health-care-investigating-potential-cyberattack/

5 COVENANT HEALTH BREACH

Date: May 2025

Impact: Affected 478,000 patients, targeting the hospital's electronic medical records (EMR) system, causing delays in operations.

Root Cause: Insufficient monitoring of EMR servers allowed entry points for malware injection.

Key Lesson: Deploy proactive AI-based monitoring to enhance network defense.

Source: https://www.hipaajournal.com/covenant-health-cyberattack/

6 DAVITA LABS RANSOMWARE INCIDENT

Date: April 2026

Impact: 2.69 million patients patients impacted as labs were rendered inoperable due to encryption of key databases.

Root Cause: Phished credentials exploited to infiltrate lab environments housing personal data.

Key Lesson: Continuous phishing simulation and anti-spoofing technologies are vital for resilience.

Source: https://www.hipaajournal.com/davita-ransomware-attack/

7 DUTCH CHIPSOFT RANSOMWARE ATTACK

Date:	April 2026
Impact:	Operations across 70% of Dutch hospitals disrupted, forcing clinicians to use manual methods for weeks.
Root Cause:	Attackers targeted vulnerabilities in the HiX EHR system, connected to cloud resources.
Key Lesson:	Third-party vendor systems require independent penetration tests before deployment.
Source:	Dutch healthcare software vendor ChipSoft hit by ransomware attack | brief | SC Media

8 AFLAC DATA BREACH

Date:	June 2025
Impact:	22.6 million patients exposed globally, with 14 million in the U.S., making it the largest healthcare breach of the year.
Root Cause:	Exploitation of cloud vulnerabilities to target improperly monitored cloud-based HR databases.
Key Lesson:	Leverage logging tools and periodic cloud penetration tests for security maturity.
Source:	https://www.hipaajournal.com/aflac-data-breach/

9 CONDUENT VENDOR BREACH

Date:	2024 to 2025
Impact:	Breach exposed 25 million patient records across multiple healthcare clients due to vendor compromise.
Root Cause:	Poor third-party vendor guidelines and lack of security assessments before integration.
Key Lesson:	Periodic vendor security audits and stronger contractual requirements are critical.
Source:	https://www.hipaajournal.com/conduent-business-solutions-data-breach/

10 SIGNATURE HEALTHCARE CYBERATTACK

Date:	April 2026
Impact:	Forced ambulance diversions, cancellation of chemotherapy, and closures of pharmacies. Critical systems offline for weeks.
Root Cause:	Attack leveraged vulnerabilities in systems running unsupported software, but the exact nature of the attack remains under investigation.
Key Lesson:	Prioritize regular software lifecycle upgrades to avoid zero-day exposure.
Source:	https://www.hipaajournal.com/signature-healthcare-brockton-hospital-cyberattack/

MORPHISEC | omega systems technology managed

WHAT CAN WE LEARN FROM THESE ATTACKS?

Healthcare organizations must adopt proactive measures like Automated Moving Target Defense (AMTD), comprehensive endpoint solutions, and robust user access governance.

Legacy systems and unpatched vulnerabilities remain a central theme across these high-profile cases.

WEBINAR:

Want in-depth insights on preventing these very attacks?

Date: May 7, 2026

Time: 11:00 AM ET

Register Now