INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:34 UTC

2025 Healthcare Cybersecurity Year in Review: Breaches and Defensive Measures

SECURITY ANALYSIS | HIGH

SCC Item ID	SCC-STY-2026-0019
Type	Security Analysis
Severity	HIGH
Affected Products	Healthcare sector, hospitals, health systems, and related organizations (U.S.-focused)
Published	2025-10-07
Discovery Source	Rss

Executive Summary

The American Hospital Association's 2025 cybersecurity year-in-review documents a sustained wave of breaches and ransomware campaigns across U.S. hospitals and health systems, reinforcing that healthcare remains among the most targeted and least resilient sectors in critical infrastructure. The report, published under AHA's cyber intelligence mission and coordinated through Health-ISAC and HHS partnership frameworks, synthesizes breach patterns and defensive posture shifts observed through 2025. For CISOs and boards, the central signal is structural: healthcare's combination of operational technology dependencies, patient safety constraints on downtime, and fragmented vendor ecosystems continues to expand the attack surface faster than most organizations can close it.

Technical Analysis

The AHA's October 2025 year-in-review synthesizes breach patterns observed throughout 2025, building on lessons from high-profile 2024 incidents including the Change Healthcare breach, which disrupted prescription processing for hundreds of health systems for weeks and demonstrated at scale what security teams had long modeled in tabletop exercises: that a single chokepoint in the healthcare supply chain can produce operational failure far beyond the initially compromised organization.

Based on available source material and AHA's established advisory posture under the Health-ISAC and HHS 405(d) program, the report's focus areas reflect trends consistent with what security teams observed throughout the year: ransomware disrupting clinical operations, third-party vendor compromises cascading across health system networks, and persistent gaps in identity and access management enabling lateral movement.

Healthcare's defensive challenge is often framed as architectural rather than purely technical. Hospitals operate under patient safety mandates that constrain how aggressively they can isolate or shut down compromised

systems. Ransomware actors have long recognized this constraint and price their demands accordingly.

Defensive posture shifts noted in AHA's reporting trajectory include increased emphasis on incident response pre-planning, backup integrity validation, and coordination with federal partners including CISA and HHS. The Health-ISAC sharing model continues to mature, though adoption of actionable threat intelligence at smaller and rural hospitals remains inconsistent. The 2025 period also reflects accelerating regulatory pressure, including HHS signals of interest in more prescriptive HIPAA Security Rule requirements, though proposed timelines remain under agency development.

For security professionals, the practical implication is that the breach patterns documented in this review are not novel; they are recurring. Organizations that have not completed network segmentation between clinical and administrative environments, implemented tested offline backup recovery, or established third-party risk management programs with contractual security baseline requirements remain exposed to the same attack chains that drove 2024's most damaging incidents. Current defensive posture gaps carry both immediate operational risk and potential future regulatory exposure.

Action Checklist

1. Step 1: Assess third-party exposure, audit which vendors have network access to clinical or administrative systems and whether those connections are scoped to least-privilege; prioritize vendors touching billing, pharmacy, and imaging workflows given demonstrated cascade risk from supply chain compromises.
2. Step 2: Validate backup integrity and recovery timelines, confirm that offline or air-gapped backups exist for critical clinical systems, that restoration procedures are documented, and that recovery time objectives have been tested against actual ransomware disruption scenarios, not theoretical ones.
3. Step 3: Review network segmentation between clinical OT environments and administrative IT, if electronic health record systems, medical devices, and corporate networks share flat or lightly segmented architecture, prioritize segmentation projects using NIST SP 800-82 guidance for healthcare OT environments.
4. Step 4: Evaluate identity and access management controls, verify MFA enforcement across remote access points, review privileged account inventories, and confirm that third-party vendor accounts are managed through a dedicated access provisioning process with time-limited credentials.
5. Step 5: Brief leadership on regulatory trajectory; HHS has signaled interest in more prescriptive HIPAA Security Rule updates, though proposed timelines remain under development. Boards should understand that compliance timelines and capital investment needs may increase, and that current defensive posture gaps carry both operational and regulatory risk. Monitor HHS.gov and Federal Register for announcements.
6. Step 6: Engage with Health-ISAC or AHA cyber intelligence channels, smaller and mid-size health systems that are not active threat intelligence consumers should establish membership or liaison relationships to receive sector-specific IOCs and incident notifications before they appear in public reporting.

IR / Forensic Enrichment

Triage Priority	URGENT

Escalation Criteria	If any step reveals that critical clinical systems lack MFA, offline backups, or network segmentation from administrative systems, or if vendor accounts have unaudited access to EHR/pharmacy/imaging systems, escalate to CISO and Board within 48 hours with remediation timeline and cost estimate.
Recovery Notes	Post-containment recovery for a healthcare ransomware incident requires validated restoration from air-gapped backups to a isolated recovery environment, followed by phased re-introduction to production with continuous integrity monitoring (checksums, row counts, transaction logs). Validate that all clinical functions (EHR, medical devices, pharmacy) are operational and synchronized before patient care resumes. Conduct a post-incident review following NIST 800-61r3 §3.5, focusing on where segmentation, backup procedures, and third-party access controls failed to prevent the initial compromise and lateral movement.
Forensic Artifacts	Windows Event Log Security (Event ID 4688 process creation, 4768 Kerberos authentication, 4720 user account creation) and System logs covering 7 days before and after first detection | Active Directory Directory Service logs (Event ID 5136 directory modification, 5140 object access) filtered for EHR, medical device, and vendor accounts | VPN/RDP access logs covering authentication events, source IPs, and MFA success/failure indicators for the past 180 days | Firewall and proxy logs (source IP, destination IP, port, protocol, bytes) for all cross-VLAN and external connections from clinical systems | Backup software logs (Veeam, Bacula, native system backup) covering backup job status, completion timestamps, and restore test results

Per-Action IR Details

Step 1: Assess third-party exposure, audit which vendors have network access to clinical or administrative systems and whether those connections are scoped to least-privilege; prioritize vendors touching billing, pharmacy, and imaging workflows given demonstrated cascade risk from supply chain compromises.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (preparation and prevention), §3.1 (detection analysis for supply chain indicators)

Controls: NIST 800-53 SA-3 (System Development Life Cycle), NIST 800-53 SA-9 (External Information System Services), NIST 800-53 CA-7 (Continuous Monitoring), CIS 6.2 (Third-party Management)

Compensating: Create a manual vendor access matrix (spreadsheet with vendor name, systems accessed, account type, last review date). Query Active Directory with 'dsquery * -filter "(&(objectClass=user)(description=*vendor*))"' to enumerate vendor accounts; cross-reference against vendor contract list. For vendors without AD integration, request network access logs from firewall/proxy covering source IPs and destination ports to billing/pharmacy/imaging subnets over the last 90 days. Document scope of access and request vendor to provide their own least-privilege justification.

Evidence: Capture Active Directory user and group membership exports (dsget user -memberof) before access reviews begin. Export firewall/proxy logs covering vendor egress for the past 180 days (source IP, destination IP, port, bytes, session count); preserve vendor contract agreements and MSAs with stated access scope. Document baseline privileged account inventory for vendor-accessible systems (run 'net localgroup Administrators' and 'Get-ADGroupMember' on critical systems).

Step 2: Validate backup integrity and recovery timelines, confirm that offline or air-gapped backups exist for critical clinical systems, that restoration procedures are documented, and that recovery time objectives have been tested against actual ransomware disruption scenarios, not theoretical ones.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (business continuity and disaster recovery), §3.4 (recovery phase)

Controls: NIST 800-53 CP-9 (Information System Backup), NIST 800-53 CP-10 (Information System Recovery and Reconstitution), NIST 800-53 IR-4 (Incident Handling), CIS 11.3 (Data Recovery Procedures)

Compensating: Document all backup solutions (commercial or open-source) currently in use; for each, record: backup schedule (hourly/daily), retention period, storage location (on-site/off-site/air-gapped), and last successful restore test date. For EHR and medical imaging systems, perform a non-destructive restore test to a isolated test environment monthly, measuring actual wall-clock recovery time and validating data integrity (compare row counts, checksums of key tables). If air-gapped backups do not exist, implement USB-based or external drive backups of EHR database snapshots kept in a physically locked cabinet, updated at least weekly. Document the recovery procedure as a runbook with explicit steps and dependencies.

Evidence: Before any restore test, capture baseline hashes (SHA-256) of critical EHR database files ('certutil -hashfile SHA256'). Preserve backup logs and media integrity reports from backup software (e.g., Veeam logs, Bacula catalogs). Document recovery test results including start time, restore completion time, first user transaction timestamp, and any data anomalies detected. Save screenshots of backup software status dashboards showing last successful backup timestamp.

Step 3: Review network segmentation between clinical OT environments and administrative IT, if electronic health record systems, medical devices, and corporate networks share flat or lightly segmented architecture, prioritize segmentation projects using NIST SP 800-82 guidance for healthcare OT environments.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (network architecture), NIST SP 800-82 (ICS/OT guidance), NIST 800-53 SC-7 (Boundary Protection)

Controls: NIST 800-53 SC-7 (Boundary Protection), NIST 800-53 SC-32 (Information System Partitioning), CIS 13.1 (Network Segmentation)

Compensating: Document current network topology using open-source tools: use 'netstat -an' and 'arp -a' on each clinical system to enumerate active connections; run Nmap from an isolated scanner ('-sV -p 1-65535' on known clinical subnets) to catalog exposed services and versions. Create a manual network diagram showing clinical (EHR, medical devices), administrative (email, finance), and user-facing networks; identify where these currently share routing or switching infrastructure. Implement segmentation using VLAN configuration on existing switches: assign clinical systems to VLAN 100, administrative to VLAN 200, guest/user to VLAN 300; configure ACLs at VLAN boundaries to block unnecessary cross-VLAN traffic. For smaller orgs, configure a software firewall (Windows Defender Firewall Advanced Security or iptables on Linux) on critical systems to block inbound connections from non-clinical subnets.

Evidence: Capture current network traffic baseline using Wireshark (traffic from clinical subnet to administrative systems and vice versa) over 7 days; save pcap files. Document all currently allowed cross-VLAN flows and their business justification. Extract ACL configurations from network devices ('show access-lists' on Cisco, 'show rules-config' on Palo Alto). Baseline firewall rule sets on clinical systems (Get-NetFirewallRule on Windows, 'iptables -L -n' on Linux) before implementing segmentation.

Step 4: Evaluate identity and access management controls, verify MFA enforcement across remote access points, review privileged account inventories, and confirm that third-party vendor accounts are managed through a dedicated access provisioning process with time-limited credentials.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (access controls and authentication), NIST 800-53 IA-2 (Authentication), IA-4 (Identifier Management)

Controls: NIST 800-53 IA-2 (Authentication), NIST 800-53 IA-4 (Identifier Management), NIST 800-53 IA-5 (Authentication Mechanisms), NIST 800-53 AC-2 (Account Management), CIS 5.2 (Ensure MFA is Enforced)

Compensating: Audit Active Directory: run 'Get-ADUser -Filter {Enabled -eq $True} | Select-Object SamAccountName, LastLogonDate, PasswordLastSet' to enumerate active accounts and identify stale accounts (>90 days no logon). For each vendor account, verify MFA by checking if the account is a member of an MFA-enforced security group or confirm MFA enrollment in your authentication logs. For remote access (VPN/RDP), query VPN appliance logs for authentication events and filter for accounts without MFA indicators (look for absence of RADIUS Accept-Challenge or equivalent 2FA log entries). Create a spreadsheet of all vendor accounts with provisioning date, expected expiration, and MFA status; set calendar reminders for credential rotation every 90 days. For accounts

without MFA, configure Windows Hello or install a free TOTP app (Microsoft Authenticator, Google Authenticator) and enforce enrollment before granting remote access.

Evidence: Export Active Directory user accounts with password age, last logon, and group membership (use 'Export-ADUser' PowerShell cmdlet). Capture VPN/RDP access logs covering the past 180 days, filter for authentication events and MFA indicators. Screenshot MFA enrollment status from your authentication management console. Document vendor account provisioning requests and approval chains (email, ticketing system) to establish who authorized each account. Preserve baseline privileged account inventory (Domain Admins, Enterprise Admins groups).

Step 5: Brief leadership on regulatory trajectory; HHS has signaled interest in more prescriptive HIPAA Security Rule updates, though proposed timelines remain under development. Boards should understand that compliance timelines and capital investment needs may increase, and that current defensive posture gaps carry both operational and regulatory risk. Monitor HHS.gov and Federal Register for announcements.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (organizational context for incident response), NIST 800-53 PM-1 (Information Security Program Planning)

Controls: NIST 800-53 PM-1 (Information Security Program Planning), NIST 800-53 AU-1 (Audit and Accountability Policy), CIS 1.1 (Governance and Risk Management)

Compensating: Subscribe to HHS mailing lists (HHS.gov/hipaa) and Federal Register notifications for HIPAA-related notices. Quarterly, review OCR enforcement actions (HHS Office for Civil Rights breach portal, ocrportal.hhs.gov) to identify emerging enforcement trends. Create a simple risk register (spreadsheet) mapping current security gaps (identified in Steps 1-4) to HIPAA Security Rule categories (Administrative, Physical, Technical safeguards) and estimate remediation cost and timeline for each. Present this register to the Board with a narrative: 'Current gaps expose the organization to OCR enforcement and breach liability; regulatory tightening may require accelerated remediation.' Include a slide showing recent settlements (e.g., Ascension, Kaiser Permanente breach settlements from 2023-2024) as precedent.

Evidence: Preserve a copy of the current HIPAA Security Rule (45 CFR Parts 160, 162, 164) and annotate sections with your current compliance gaps. Screenshot HHS mailing list confirmations and Federal Register bookmark/alert settings. Document the risk register with citations to specific HIPAA requirements. Archive OCR enforcement action summaries that are relevant to your organization's threat profile.

Step 6: Engage with Health-ISAC or AHA cyber intelligence channels, smaller and mid-size health systems that are not active threat intelligence consumers should establish membership or liaison relationships to receive sector-specific IOCs and incident notifications before they appear in public reporting.

NIST Phase: Preparation

Reference: NIST 800-61r3 §1.4 (incident response team organization and dependencies), NIST 800-53 SI-4 (Information System Monitoring)

Controls: NIST 800-53 SI-4 (Information System Monitoring), NIST 800-53 SI-5 (Security Alerts, Advisories, and Directives), CIS 4.1 (Secure Configuration Management)

Compensating: If Health-ISAC or AHA membership is cost-prohibitive, join free threat intelligence sharing communities: CISA AIS (Automated Indicator Sharing, free federal service), Reddit r/cybersecurity incident threads, and healthcare-focused OSINT channels (e.g., HealthISAC's free community mailing lists). Designate a threat intelligence liaison (30 minutes/week) to monitor CISA.gov for healthcare-specific advisories, check the MITRE ATT&CK healthcare healthcare-specific articles, and review public breach disclosures (BleepingComputer, Krebs on Security, healthcare-focused blogs). For each ransomware variant or threat actor active in healthcare, document their known TTPs and IOCs (file hashes, C2 domains) in a simple CSV file; cross-reference against your environment using free tools (hash lookups on VirusTotal, domain whois checks). Alert your SOC or IT team when new IOCs are identified.

Evidence: Document your threat intelligence sources and update frequency (e.g., 'CISA advisories, daily check'; 'Health-ISAC alerts, real-time'). Preserve incoming threat intelligence feeds (emails, OSINT summaries) in a dated folder. Maintain an IOC log with date received, source, indicator type (hash/domain/IP), threat actor/malware family,

and action taken (blocked/monitored). Screenshot your CISA AIS account enrollment and mailing list subscriptions.

Detection Guidance

Given the breach patterns AHA's reporting consistently highlights in healthcare, security teams should prioritize the following detection and audit activities:

Authentication anomalies: Review authentication logs for after-hours access to EHR systems, VPN logins from unusual geographies or ASNs, and credential stuffing patterns against patient portals or remote access gateways. Healthcare accounts are frequently targeted via credential markets populated from prior breaches.

Third-party access monitoring: Audit logs for vendor account activity outside contracted maintenance windows. Lateral movement from compromised vendor accounts often begins during off-hours and targets file shares, backup systems, and domain controllers before ransomware deployment.

Backup system access: Monitor for unexpected access to backup infrastructure, particularly deletion or modification of backup catalogs. Ransomware operators targeting healthcare increasingly destroy backups before encryption to maximize leverage.

Clinical system availability baselines: Establish availability baselines for critical clinical applications (EHR, PACS, pharmacy dispensing) and alert on degraded response times or unexpected service restarts, which can indicate early-stage ransomware staging or lateral movement activity before encryption begins.

Policy gap audit: Review whether your organization has completed a HIPAA Security Rule risk analysis within the past 12 months; HHS Office for Civil Rights enforcement data (available at hhs.gov/ocr/privacy/hipaa/enforcement) consistently shows that missing or outdated risk analyses are among the most cited findings in post-breach investigations. Cross-reference controls against the HHS 405(d) Health Industry Cybersecurity Practices (HICP) document as a baseline.

Supply chain contract review: Audit business associate agreements for security baseline requirements; agreements that lack incident notification timelines, audit rights, or minimum control requirements represent both a compliance gap and an unmanaged risk surface.

Sources

Source	URL	Tier
Aha	https://www.aha.org/news/aha-cyber-intel/2025-10-07-2025-cybersecur...	T3
AHA blog: 2025 Cybersecurity Year in Review, Part One	https://www.aha.org/news/headline/2025-10-13-aha-blog-2025-cybersec...	T3
2025 Cybersecurity Year in Review, Part One - MyADS.org	https://www.myads.org/index.php?option=com_content&view=article...	T3
AHA blog: 2025 Cybersecurity Year in Review, Part One	https://ramaonhealthcare.com/aha-blog-2025-cybersecurity-year-in-re...	T3

Source	URL	Tier
2025 Year in Review: Cybersecurity and Data Protection | Paul, Weiss	https://www.paulweiss.com/insights/client-memos/2025-year-in-review...	T3

Generated 2026-03-29 18:34 UTC by TJS Security Command Center