INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:44 UTC

Nebraska AG's Lawsuit Against Change Healthcare Survives Motion to Dismiss

GOVERNANCE | CRITICAL

SCC Item ID	SCC-GOV-2026-0001
Type	Governance
Severity	CRITICAL
Affected Products	Change Healthcare (UnitedHealth Group subsidiary), healthcare data exchange and payment processing platform
Published	2025-11-17

Executive Summary

A Nebraska court has allowed the state AG's lawsuit against Change Healthcare to proceed, stemming from the February 2024 ALPHV/BlackCat ransomware attack that exposed health and personal data of an estimated 100 million individuals. The ruling signals that state attorneys general are prepared to pursue healthcare entities for inadequate cybersecurity controls, independent of federal enforcement. Organizations handling protected health information face escalating legal exposure at the state level, with executive accountability now a documented judicial concern.

Technical Analysis

The February 2024 breach of Change Healthcare (UnitedHealth Group subsidiary) was attributed to ALPHV/BlackCat ransomware operators. Initial access is assessed via valid account abuse (T1078) and exploitation of public-facing applications (T1190), followed by data exfiltration (T1041) and ransomware deployment (T1486). The breach affected Change Healthcare's claims processing and payment exchange infrastructure, a platform processing roughly one-third of U.S. healthcare transactions. Relevant weaknesses include CWE-359 (exposure of private information), CWE-693 (protection mechanism failure), and CWE-284 (improper access control). No CVE is assigned to this incident. The lawsuit centers on alleged failures to implement HIPAA-aligned administrative, physical, and technical safeguards, as well as violations of Nebraska consumer protection statutes. No patch applies; the compliance and legal risk is architectural and procedural.

Action Checklist

1. Step 1 (Immediate): Audit MFA enforcement across all remote access points, VPN gateways, and privileged accounts, T1078 (valid account abuse) was the assessed initial access vector in this breach.

2. Step 2 (Detection): Review authentication logs for anomalous credential use, off-hours access, and lateral movement patterns consistent with pre-ransomware staging; cross-reference against ALPHV/BlackCat TTPs in CISA Advisory AA23-353A and updated Change Healthcare-specific threat guidance from CISA or HHS OCR.

3. Step 3 (Assessment): Inventory all third-party health data processors and clearinghouses in your environment; map data flows involving PHI and PII to identify CWE-284 and CWE-359 exposure points.

4. Step 4 (Compliance): Engage legal and compliance teams to assess state AG enforcement exposure across jurisdictions where your organization holds resident data; document current HIPAA Security Rule control implementation against NIST SP 800-66r2.

5. Step 5 (Long-term): Conduct a tabletop exercise simulating ransomware-driven data exfiltration targeting a critical third-party dependency; update incident response playbooks to include state AG notification thresholds alongside HHS breach notification requirements.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO and General Counsel immediately if any privileged account lacks MFA, if forensic analysis reveals unauthorized lateral movement, or if inventory identifies unassessed third-party data flows — state AG litigation exposure makes any control gap a material risk.
Recovery Notes	Post-containment: Implement MFA across all identified gaps within 30 days (prioritize remote access and privileged accounts). Revoke any compromised credentials and rotate all service account passwords used in third-party integrations. Conduct a full forensic timeline to establish initial access vector and dwell time (critical for state AG discovery). Update third-party vendor contracts to require annual penetration testing and SOC 2 Type II reports. Schedule state AG notifications (and HHS breach reporting if threshold met) in consultation with legal — document all notification dates and recipients for regulatory compliance.
Forensic Artifacts	Windows Event Log 4624 (successful logon) and 4625 (failed logon) — identifies anomalous authentication patterns and credential abuse | Windows Event Log 4688 (process creation with command line) — reveals lateral movement and post-compromise staging activity | /var/log/auth.log and /var/log/wtmp (Unix authentication and login records) — authenticates SSH access and privilege escalation | Firewall/proxy logs with source IP, destination IP, port, protocol, and timestamp — establishes data exfiltration path and volume | VPN gateway connection logs (username, source IP, timestamp, duration, bytes) — identifies remote access abuse and off-hours logons | Active Directory/Entra ID sign-in logs with MFA failure/success status — confirms MFA enforcement and suspicious authentication methods | DNS query logs and NetFlow data — reveals command-and-control communication and data staging activity | Change Healthcare breach advisories and CISA AA23-353A technical details — establishes TTPs for ALPHV/BlackCat targeting this sector

Per-Action IR Details

Step 1 (Immediate): Audit MFA enforcement across all remote access points, VPN gateways, and privileged accounts, T1078 (valid account abuse) was the assessed initial access vector in this breach.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (preparation phase); §3.2.1 (detection and analysis for credential compromise)

Controls: NIST 800-53r5 IA-2 (Authentication), NIST 800-53r5 IA-4 (Identifier Management), NIST 800-53r5 AC-2 (Account Management), CIS v8 5.3 (MFA for all users), CIS v8 5.4 (MFA for remote access)

Compensating: Use native OS auditing: Windows (Get-MsolUser -All | Where {$_.StrongAuthenticationMethods.Count -eq 0}) for Microsoft Entra; Linux (awk -F: '$2!="!" && $2!="*" {print $1}' /etc/shadow | while read user; do getent passwd $user; done). For VPN, enable verbose logging in OpenVPN config (verb 4) or check Cisco ASA (show aaa authentication login) output. Document each account's MFA status in a spreadsheet by gateway/application.

Evidence: Capture before audit: VPN gateway authentication logs (last 90 days minimum), Active Directory/Entra sign-in logs (Azure portal > Sign-in logs), Windows Event Log 4624 (successful logons) and 4625 (failed logons) from domain controllers, SSH auth.log entries from Unix systems (/var/log/auth.log or /var/log/secure). Preserve syslog exports if centralized logging exists.

Step 2 (Detection): Review authentication logs for anomalous credential use, off-hours access, and lateral movement patterns consistent with pre-ransomware staging; cross-reference against ALPHV/BlackCat TTPs in CISA Advisory AA23-353A and updated Change Healthcare-specific threat guidance from CISA or HHS OCR.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 (detection and analysis); §3.2.4 (incident handling steps specific to credential abuse)

Controls: NIST 800-53r5 AU-2 (Audit Events), NIST 800-53r5 AU-6 (Audit Review, Analysis, and Reporting), NIST 800-53r5 SI-4 (Information System Monitoring), CIS v8 8.2 (Log all access and changes), CIS v8 8.5 (Alert on anomalous activity)

Compensating: Parse authentication logs with grep, awk, and Python scripts. Search for: (1) logon times outside business hours (grep for 22:00-06:00 timestamps in Windows Event 4624); (2) impossible travel (same user logging in from geographically distant IPs within seconds — extract Source IP from 4624, cross-reference with MaxMind GeoIP free database); (3) repeated failed logons followed by success (Event 4625 then 4624 from same source); (4) lateral movement via 4688 (Process Creation) for suspicious outbound connections (netstat, Get-NetTCPConnection). Create a manual timeline spreadsheet with User, Timestamp, Source IP, Destination Host, and Event Type columns. Reference MITRE ATT&CK T1078 (Valid Accounts), T1021.001 (RDP), T1021.006 (SSH) for behavioral patterns.

Evidence: Capture Windows Event Logs: 4624 (successful logon), 4625 (failed logon), 4688 (process creation with command line), 4720-4722 (account creation/changes), 4779 (RDP session disconnect). For Unix: /var/log/auth.log (authentication attempts), /var/log/syslog (system activity), /var/log/wtmp (binary login records — use 'last' command to parse). Network: firewall/proxy logs showing outbound connections from privileged accounts (source IP, dest IP, port, timestamp). VPN: connection logs with username, source IP, timestamp, duration. Preserve all logs in read-only format (e.g., tar.gz with hash).

Step 3 (Assessment): Inventory all third-party health data processors and clearinghouses in your environment; map data flows involving PHI and PII to identify CWE-284 and CWE-359 exposure points.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (preparation; asset inventory); NIST 800-66r2 (HIPAA Security Rule implementation guidance for PHI protection)

Controls: NIST 800-53r5 CM-8 (Information System Component Inventory), NIST 800-53r5 SA-9 (External Information System Services), NIST 800-53r5 CA-6 (Security Assessment and Authorization), CIS v8 2.1 (Authorized software inventory), CIS v8 2.2 (Address unauthorized software)

Compensating: Manual discovery: (1) Query DNS and firewall logs for external IPs/domains contacted by healthcare systems (grep outbound traffic for common clearinghouse domains: hl7.org, x12.org, clearinghouses like Emdeon, Experian, Optum, Change Healthcare); (2) Review Active Directory group policies and application documentation for integrated third-party services; (3) Interview application owners and systems administrators for data flow diagrams (draw manually if needed); (4) Check routing tables, firewall ACLs, and NAT rules for external data flows. Create a simple spreadsheet: Vendor Name | Data Type (PHI/PII) | Connection Method (API/SFTP/VPN) | Frequency | Last Security Assessment. CWE-284 (Improper Access Control) and CWE-359 (Exposure of Private Information) map to insufficient encryption in transit and storage — document which vendors use TLS 1.2+, encryption at rest, and have signed BAAs (Business Associate Agreements).

Evidence: Capture: Firewall/proxy logs (last 90 days) showing all outbound connections to third-party IPs (source, dest, port, protocol, bytes transferred). DNS query logs showing external domain resolutions. Network flow data (NetFlow, sFlow exports). Active Directory group memberships and service accounts with external access. VPN logs showing which accounts access third-party systems. Configuration management database (CMDB) or IT asset inventory exports. BAAs and vendor security questionnaires (store hashes of documents for integrity verification).

Step 4 (Compliance): Engage legal and compliance teams to assess state AG enforcement exposure across jurisdictions where your organization holds resident data; document current HIPAA Security Rule control implementation against NIST SP 800-66r2.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §3.4 (post-incident activities); NIST 800-66r2 (HIPAA Security Rule guidance for compliance documentation)

Controls: NIST 800-53r5 CA-7 (Continuous Monitoring), NIST 800-53r5 SA-3 (System Development Life Cycle), NIST 800-53r5 RA-3 (Risk Assessment), CIS v8 1.1 (Establish policies and procedures)

Compensating: Create a control implementation matrix: Map each HIPAA Security Rule requirement (Administrative, Physical, Technical Safeguards from 45 CFR 164.304-318) to corresponding NIST 800-53r5 control and current organizational implementation status (Implemented / Partial / Not Implemented). Use NIST 800-66r2 Appendix A for direct mapping. For jurisdictional AG exposure: Identify all states where your organization has patients/members (review patient residence data from EHR/claims). Cross-reference with state AG enforcement histories (search NAAG database, HHS OCR enforcement actions). Document in a table: State | Resident Count | Recent AG Actions | HIPAA Violation Risk. Provide this documentation to legal/compliance for liability assessment. CRITICAL: This step requires legal counsel — do not make liability determinations without attorney review.

Evidence: Capture: Current security policies and procedures (signed and dated). Control assessment worksheets (manual or automated from any GRC tools). Audit reports from internal/external assessments (SOC 2, HIPAA risk assessments). Breach notification logs (if any prior incidents). Evidence of security training completion and attendance records. Risk assessments documenting threat modeling and mitigation strategies. Encryption and data loss prevention (DLP) configuration exports. Access control matrices showing privileged account assignments. Change management logs for security-relevant changes (last 12 months).

Step 5 (Long-term): Conduct a tabletop exercise simulating ransomware-driven data exfiltration targeting a critical third-party dependency; update incident response playbooks to include state AG notification thresholds alongside HHS breach notification requirements.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §2.3.9 (tabletop exercises); §3.4.1 (lessons learned); NIST 800-66r2 §2.6 (breach response planning for HIPAA)

Controls: NIST 800-53r5 CP-3 (Contingency Planning and Training), NIST 800-53r5 IR-3 (Incident Response Testing), NIST 800-53r5 IR-4 (Incident Handling), CIS v8 17.1 (Establish an incident response program)

Compensating: Tabletop design: (1) Scenario — ransomware attacks third-party clearinghouse; exfiltrates 50K patient records (names, DOBs, SSNs, diagnoses); attacker threatens sale. (2) Inject decision points: detect time (+X hours), containment decision (contact vendor?), data quantification (how do we count affected residents?), notification decision (HHS + state AG? which states?). (3) Walk through roles: Incident Commander, Privacy Officer, Legal, Vendor Relations, Communications. (4) Document gaps and update playbooks. Update playbooks with: (A) State AG notification matrix — list all states where patients reside, each state's notification law thresholds (most trigger at 500+ residents; verify your state's threshold via NIST 800-66r2 Appendix C); (B) Notification language template for state AGs (must acknowledge inadequate vendor controls per Nebraska AG complaint); (C) Decision tree: Has breach affected residents of State X? → Check resident count → If ≥ threshold, notify AG within required timeframe (typically 30-60 days). (D) Evidence preservation — before notifying, freeze forensic evidence and chain of custody logs.

Evidence: Capture: Tabletop exercise notes (attendees, decisions made, gaps identified). Updated incident response playbook (version controlled, signed by leadership). Notification templates and approval workflows (for HHS, state AGs). Vendor communication templates and escalation contacts. Forensic preservation procedures (who collects, how, chain of custody form). Legal review of notification language (attorney signature on playbook approval). Prior breach

notifications or HHS OCR breach log extracts (to understand precedents). Test case data for notification system (ensure system can identify and quantify affected residents by state).

Detection Guidance

This is a governance and compliance intelligence item, not an active exploitation alert. Detection focus should be retrospective and preventive. Review SIEM logs for T1078 indicators: successful authentications from new geolocations, credential use outside business hours, and service account logins to interactive sessions. For T1190, audit vulnerability scan history for public-facing application findings that were unpatched at the time of the original breach window (January-February 2024). For organizations that used Change Healthcare services, confirm whether you received breach notification and whether your own PHI inventory reflects the scope of data shared with Change Healthcare. ALPHV/BlackCat behavioral indicators are documented in CISA Advisory AA23-353A; use these to validate existing detection rule coverage in your EDR and SIEM. No new IOCs are associated with this ruling event; however, IOCs from the original February 2024 breach remain valid for retrospective log review.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`No confirmed live IOCs associated with this ruling`	ALPHV/BlackCat infrastructure from the February 2024 breach has been documented by CISA and FBI; refer to CISA Advisory AA23-353A for historical indicators. No new IOCs are associated with the court ruling itself.	LOW

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1190** — Exploit Public-Facing Application
- **T1041** — Exfiltration Over C2 Channel
- **T1486** — Data Encrypted for Impact

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection

- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **CA-7** — Continuous Monitoring
- **SI-4** — System Monitoring
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **AC-3** — Access Enforcement
- **IR-4** — Incident Handling

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

CIS-V8

- **6.1**
- **6.2**

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC7.4** — Responds to identified security incidents

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.308(a)(6)(ii)** — Response and Reporting

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **RS.CO-03** — Recovery activities and progress communicated

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.5.34** — Privacy and protection of personal information
- **A.5.23** — Information security for use of cloud services

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1190	Exploit Public-Facing Application	Initial-Access
T1041	Exfiltration Over C2 Channel	Exfiltration

Technique ID	Technique Name	Tactic
T1486	Data Encrypted for Impact	Impact

Sources

Source	URL	Tier
Hipaajournal	https://www.hipaajournal.com/change-healthcare-responding-to-cybera...	T3
Nebraska AG's lawsuit against Change Healthcare survives motion ...	https://hipaatimes.com/nebraska-ags-lawsuit-against-change-healthca...	T3
Court Allows Attorney General Hilgers' Case Against Change ...	https://ago.nebraska.gov/news/court-allows-attorney-general-hilgers...	T1
Lawsuit Against Change Healthcare Over Massive Data Breach Will ...	https://todaysgeneralcounsel.com/lawsuit-against-change-healthcare-...	T3
Nebraska Court Allows Data Privacy Lawsuit Against Change ...	https://www.insurancejournal.com/news/midwest/2025/11/17/847698.htm	T3

Generated 2026-03-29 18:44 UTC by TJS Security Command Center