INTELLIGENCE BRIEFING
Security Command Center

TLP:CLEAR
2026-06-10 07:25 UTC

Senate HELP committee chairman seeks info on NYC Health + Hospital data breach

DATA BREACH | HIGH

SCC Item ID	SCC-DBR-2026-0157
Type	Data Breach
Severity	HIGH
Affected Products	NYC Health + Hospitals, internal systems (specific systems not publicly disclosed)
Published	1 day ago
Discovery Source	Serper

Executive Summary

An unauthorized actor accessed NYC Health + Hospitals systems from late November 2024 through mid-February 2025, a roughly 12-week dwell period before discovery. NYC Health + Hospitals is one of the largest public hospital systems in the United States, and the breach has drawn a formal congressional inquiry from Senate HELP Committee Chairman Bill Cassidy. The full scope of compromised patient data, affected systems, and attack vector has not been publicly confirmed, leaving the organization exposed to regulatory action, reputational harm, and potential class litigation while the investigation continues.

Technical Analysis

Breach window: late November 2024 through mid-February 2025. Public disclosure: March 24, 2025. Affected entity: NYC Health + Hospitals, specific systems not publicly identified. Attack vector: unconfirmed. MITRE ATT&CK techniques associated with this incident type include T1190 (Exploit Public-Facing Application) and T1078 (Valid Accounts), reflecting common initial access patterns in healthcare sector breaches; neither has been officially attributed to this incident. No CVE, CWE, or specific vulnerability has been publicly linked. No CVE base score or EPSS data applies. Compromised data types and patient count remain unconfirmed as of the item date. The approximately 84-day dwell time before detection suggests either delayed alerting, insufficient endpoint or network visibility, or both. Congressional inquiry targets breach scope, affected data categories, and corrective measures, indicating regulators and legislators view the disclosed facts as incomplete.

Action Checklist

1. Step 1: Containment. Audit externally facing applications and authentication systems for signs of unauthorized access consistent with T1190 and T1078. Prioritize systems handling patient data. Enforce session termination for all active privileged sessions pending review (NIST AC-12, Session Termination). Isolate any systems where anomalous access cannot be ruled out.

2. Step 2: Detection. Query authentication logs for dormant or unexpected account activity across the November 2024 to February 2025 window (NIST AU-6, Audit Record Review, Analysis, and Reporting; CIS 8.2, Collect Audit Logs). Look for logins outside business hours, access from unusual geolocations, privilege escalation events, and accounts not used in 45+ days suddenly active (CIS 5.3, Disable Dormant Accounts). Cross-reference against D3-LAM (DEFEND Local Account Monitoring) behavioral baselines.

3. Step 3: Eradication. Rotate credentials for all privileged and service accounts, particularly those with access to clinical or patient data systems (D3-CRO, Credential Rotation; D3-CH, Credential Hardening). Disable or remove any accounts that cannot be positively attributed to a current, authorized user (NIST AC-2, Account Management; CIS 5.3). No vendor-specific patch applies, no CVE has been attributed.

4. Step 4: Recovery. Validate that audit logging is complete and tamper-evident across all patient data systems (NIST AU-9, Protection of Audit Information; NIST AU-11, Audit Record Retention). Confirm MFA is enforced on all remote access paths and administrative accounts (CIS 6.4, Require MFA for Remote Network Access; CIS 6.5, Require MFA for Administrative Access; D3-MFA, Multi-factor Authentication). Verify access control lists restrict patient data access to need-to-know roles (CIS 3.3, Configure Data Access Control Lists; NIST AC-3, Access Enforcement).

5. Step 5: Post-Incident. Conduct a gap assessment against NIST AU-2 (Event Logging) to confirm all relevant event types were captured during the breach window. An 84-day dwell time indicates a detection or alerting failure. Review whether account activity monitoring (D3-LAM) and system file analysis (D3-SFA) were operational. Document findings against NIST AC-6 (Least Privilege) and CIS 5.4 (Restrict Administrator Privileges) to assess whether over-privileged accounts expanded the blast radius. Prepare documentation for potential HHS OCR inquiry and congressional response.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to legal counsel, HHS OCR (HIPAA breach notification required within 60 days of discovery for breaches affecting 500+ individuals), and the Senate HELP Committee liaison if forensic analysis confirms PHI exfiltration, if the attack vector remains unidentified (indicating the threat actor may retain access), or if the credential rotation and containment actions cannot be completed within 24 hours due to system dependencies in clinical operations.
Recovery Notes	Given the 84-day dwell period and unconfirmed attack vector, maintain enhanced monitoring on all patient data systems and authentication infrastructure for a minimum of 90 days post-containment, as re-entry through a second undiscovered persistence mechanism is a realistic risk. Verify integrity of clinical application data (Epic/Cerner audit trails) to confirm patient records were not modified during the dwell period, which carries separate patient safety implications beyond the data breach notification obligation. Do not declare full recovery until an independent forensic firm has confirmed no residual attacker presence, as internal teams may have detection blind spots consistent with the failure that allowed an 84-day dwell time.

Forensic Artifacts	Identity provider authentication logs (Azure AD sign-in logs, Okta system log, or on-prem ADFS event logs) for the full November 23, 2024–February 15, 2025 window — these are the primary source for establishing the initial access timestamp, source IPs, and accounts used, which are the foundation of both the internal timeline and the HHS OCR notification package | Clinical application access audit trails (Epic MyChart/Hyperspace audit logs, Cerner Millennium audit logs, or equivalent EHR platform) showing patient record query counts, data exports, and print/download events per session — this is the primary evidence for quantifying PHI scope and is required for HIPAA breach notification specificity | VPN and remote access gateway session logs (Cisco ASA, Palo Alto GlobalProtect, Citrix ADC, or equivalent) capturing source IP, session duration, bytes transferred, and authentication method for the dwell period — a 12-week dwell time with data exfiltration would show anomalous sustained session volumes or off-hours connection patterns in these logs | Windows Security Event Log EVTX files from domain controllers and patient data application servers, specifically preserving Event IDs 4624/4625/4648/4672/4720/4732/4776 — these establish the lateral movement and privilege escalation chain and must be preserved in original binary format for forensic integrity prior to any log rotation or system changes | Network flow records (NetFlow, IPFIX, or firewall traffic logs) for outbound connections from patient data systems during the dwell period, filtered for large data transfers, connections to non-standard cloud storage endpoints, or sustained beaconing intervals — in a long-dwell breach of this type, exfiltration staging and C2 communication patterns are typically visible in flow data even when endpoint logs are absent

Per-Action IR Details

Step 1: Containment — Audit externally facing applications and authentication systems for signs of unauthorized access consistent with T1190 and T1078. Prioritize systems handling patient data. Enforce session termination for all active privileged sessions pending review (NIST AC-12 — Session Termination). Isolate any systems where anomalous access cannot be ruled out.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST AC-12 — Session Termination, NIST AC-3 — Access Enforcement, NIST AC-17 — Remote Access, CIS 4.4 (IG1/IG2/IG3) — Implement and Manage a Firewall on Servers

Compensating: Without a SIEM, enumerate all active authenticated sessions on externally facing systems using 'netstat -anp' (Linux) or 'Get-NetTCPConnection' (PowerShell) filtered for ESTABLISHED states on ports 443/80/8080. Force-terminate suspect sessions via 'pkill -u ' or Windows 'logoff '. Block inbound access to patient data portals at the firewall/ACL level pending review — a two-person team can execute this with pre-staged deny rules activated via a single firewall CLI command.

Evidence: Before terminating sessions, capture: (1) full output of active session tables from the identity provider (Azure AD sign-in logs, Okta system log, or on-prem AD 'Get-ADUser -Filter * | Get-ADUserResultantPasswordPolicy' combined with last logon timestamps); (2) web server access logs from patient portal endpoints for the November 2024–February 2025 window, specifically filtering for anomalous User-Agent strings, POST requests to authentication endpoints, and IP addresses outside NYC Health + Hospitals' known IP ranges; (3) VPN/remote access gateway authentication logs capturing source IPs, session durations, and data volumes transferred during the dwell period.

Step 2: Detection — Query authentication logs for dormant or unexpected account activity across the November 2024 to February 2025 window (NIST AU-6 — Audit Record Review, Analysis, and Reporting; CIS 8.2 — Collect Audit Logs). Look for logins outside business hours, access from unusual geolocations, privilege escalation events, and accounts not used in 45+ days suddenly active (CIS 5.3 — Disable Dormant Accounts). Cross-reference against D3-LAM (Local Account Monitoring) behavioral baselines.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-6 — Audit Record Review, Analysis, And Reporting, NIST AU-2 — Event Logging, NIST AU-3 — Content Of Audit Records, CIS 8.2 (IG1/IG2/IG3) — Collect Audit Logs, CIS 5.3 (IG1/IG2/IG3) — Disable Dormant Accounts, CIS 5.1 (IG1/IG2/IG3) — Establish and Maintain an Inventory of Accounts

Compensating: Export Active Directory or LDAP authentication logs for the full November 23, 2024–February 15, 2025 window. Use PowerShell: 'Get-EventLog -LogName Security -InstanceId 4624,4625,4648,4672,4720,4732 -After "2024-11-23" -Before "2025-02-15" | Export-Csv auth_review.csv'. Parse with a free tool such as Log Parser Studio or grep/awk on Linux. Filter for Event ID 4624 (successful logon) with Logon Type 3 or 10 (network/remote interactive) outside 0700–1900 local time. Identify accounts with LastLogonDate older than 45 days prior to November 23, 2024 using 'Search-ADAccount -AccountInactive -TimeSpan 45 -UsersOnly'.

Evidence: Preserve before analysis: (1) Windows Security Event Log exports (EVTX format) from all domain controllers and patient data application servers covering the full 84-day dwell window — specifically Event IDs 4624, 4625, 4648, 4672 (privilege use), 4720 (account creation), 4732 (group membership change); (2) identity provider audit logs (Azure AD, Okta, or on-prem ADFS) capturing authentication method used, MFA bypass events, and conditional access policy evaluations; (3) EHR/clinical application access logs (Epic, Cerner, or equivalent) showing which patient records were queried or exported during the dwell period, including user ID, timestamp, and record count per session.

Step 3: Eradication — Rotate credentials for all privileged and service accounts, particularly those with access to clinical or patient data systems (D3-CRO — Credential Rotation; D3-CH — Credential Hardening). Disable or remove any accounts that cannot be positively attributed to a current, authorized user (NIST AC-2 — Account Management; CIS 5.3). No vendor-specific patch applies — no CVE has been attributed.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-2 — Account Management, NIST AC-6 — Least Privilege, NIST AC-1 — Policy And Procedures, CIS 5.3 (IG1/IG2/IG3) — Disable Dormant Accounts, CIS 5.4 (IG1/IG2/IG3) — Restrict Administrator Privileges to Dedicated Administrator Accounts, CIS 6.2 (IG1/IG2/IG3) — Establish an Access Revoking Process

Compensating: Generate a full privileged account inventory using 'Get-ADGroupMember -Identity "Domain Admins","Enterprise Admins","Schema Admins"' and equivalent clinical application admin role exports. For each account, confirm a named current employee with active HR record before resetting. Use 'Set-ADAccountPassword' with '-Reset' flag and force password change at next login for all retained accounts. Disable unattributed accounts via 'Disable-ADAccount' rather than deleting, preserving forensic attribution. Rotate Kerberos KRBTGT account password twice (required to invalidate existing Kerberos tickets and any potential Golden Ticket artifacts).

Evidence: Before rotating credentials, capture: (1) a point-in-time snapshot of all group memberships for privileged AD groups using 'Get-ADGroupMember -Recursive' — this establishes the blast radius of potentially compromised credentials; (2) service account usage logs from clinical systems (Epic/Cerner service account authentication events) to identify any service accounts that authenticated during anomalous hours or from unexpected source hosts; (3) cached credential artifacts from systems identified as potentially accessed — run 'Invoke-Mimikatz' equivalent in a read-only forensic context or collect LSASS memory dump on isolated systems before credential rotation to document what an attacker could have harvested.

Step 4: Recovery — Validate that audit logging is complete and tamper-evident across all patient data systems (NIST AU-9 — Protection of Audit Information; NIST AU-11 — Audit Record Retention). Confirm MFA is enforced on all remote access paths and administrative accounts (CIS 6.4 — Require MFA for Remote Network Access; CIS 6.5 — Require MFA for Administrative Access; D3-MFA — Multi-factor Authentication). Verify access control lists restrict patient data access to need-to-know roles (CIS 3.3 — Configure Data Access Control Lists; NIST AC-3 — Access Enforcement).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-9 — Protection Of Audit Information, NIST AU-11 — Audit Record Retention, NIST AU-4 — Audit Storage Capacity, NIST AC-3 — Access Enforcement, CIS 6.4 (IG1/IG2/IG3) — Require MFA for Remote Network Access, CIS 6.5 (IG1/IG2/IG3) — Require MFA for Administrative Access, CIS 3.3 (IG1/IG2/IG3) — Configure Data

Access Control Lists, CIS 3.4 (IG1/IG2/IG3) — Enforce Data Retention

Compensating: Validate log integrity without a commercial SIEM by enabling Windows Event Log forwarding to a dedicated, network-isolated log server (Windows Event Collector or syslog-ng on Linux) with append-only permissions. Verify no log gaps exist in the 84-day window by checking event sequence numbers for discontinuities. For MFA validation without enterprise tooling, use free Duo MFA (up to 10 users) or enforce certificate-based authentication for VPN via OpenVPN with client cert requirements. Audit ACLs on patient data file shares and database objects using 'Get-Acl' (PowerShell) or 'icacls' and compare against HR-verified role lists.

Evidence: Before declaring recovery complete, capture and retain: (1) log continuity verification reports showing no gaps in audit event sequences during the dwell window — any gaps are themselves evidence of potential log tampering or evasion; (2) MFA enrollment status export for all remote access and administrative accounts showing pre-breach vs. post-remediation enrollment rates — this documents the control gap that existed during the breach; (3) current ACL snapshots for all patient data systems as the post-remediation baseline, enabling future comparison to detect unauthorized permission changes.

Step 5: Post-Incident — Conduct a gap assessment against NIST AU-2 (Event Logging) to confirm all relevant event types were captured during the breach window. An 84-day dwell time indicates a detection or alerting failure. Review whether account activity monitoring (D3-LAM) and system file analysis (D3-SFA) were operational. Document findings against NIST AC-6 (Least Privilege) and CIS 5.4 (Restrict Administrator Privileges) to assess whether over-privileged accounts expanded the blast radius. Prepare documentation for potential HHS OCR inquiry and congressional response.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST AU-2 — Event Logging, NIST AU-6 — Audit Record Review, Analysis, And Reporting, NIST AU-12 — Audit Record Generation, NIST AC-6 — Least Privilege, NIST AC-2 — Account Management, CIS 5.4 (IG1/IG2/IG3) — Restrict Administrator Privileges to Dedicated Administrator Accounts, CIS 7.1 (IG1/IG2/IG3) — Establish and Maintain a Vulnerability Management Process, CIS 7.2 (IG1/IG2/IG3) — Establish and Maintain a Remediation Process

Compensating: Document the AU-2 gap assessment in a structured spreadsheet mapping each event type (authentication, privilege use, data access, remote access, account management) against whether it was logged, where logs resided, and retention period. For HHS OCR response preparation, use the OCR Breach Notification Rule checklist (45 CFR §164.400–414) as a free structural template. A two-person team should assign one analyst to timeline reconstruction (correlating all recovered log fragments into a unified attack timeline) and one to the regulatory documentation package, using the NIST 800-61r3 post-incident report template as the structural basis.

Evidence: For the congressional and HHS OCR response, preserve and organize: (1) the complete reconstructed attack timeline with sourced evidence for each entry — unsupported timeline entries will be challenged in a congressional inquiry; (2) a control gap register documenting specifically which AU-2 event types were not logged, for how long, and on which systems — this is the evidence HHS OCR will scrutinize for willful neglect determination; (3) the pre-breach privileged account inventory showing role assignments and last-access dates, which documents whether AC-6 least privilege and CIS 5.4 admin privilege restrictions were implemented — over-privileged accounts that expanded data access scope are a material finding in both OCR and Senate HELP committee contexts.

Detection Guidance

No confirmed IOCs or attack-specific signatures are publicly available for this incident. Detection should focus on behavioral indicators consistent with T1190 and T1078. Review authentication logs for: (1) logins using valid credentials during off-hours or from anomalous source IPs across the November 2024 to February 2025 window; (2) accounts that were dormant before November 2024 and became active during the breach window; (3) lateral movement indicators, access to systems or data repositories inconsistent with a user's normal role. Per NIST AU-6, audit records should be reviewed for indicators of unauthorized access, privilege escalation, or

data exfiltration. Per CIS 8.2, confirm audit logging was enabled and collecting across all relevant systems before, during, and after the breach window; gaps in log coverage are themselves a finding. Apply D3-LAM (DEFEND Local Account Monitoring) to flag local account behavior deviating from established baselines. If SIEM coverage of clinical systems is incomplete, treat that gap as a priority remediation item.

Framework Mappings

MITRE-ATTACK

- **T1190** — Exploit Public-Facing Application
- **T1078** — Valid Accounts

NIST-800-53R5

- **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
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information

HIPAA-SECURITY

- **164.308(a)(6)(ii)** — Response and Reporting

SOC2-TSC

- **CC7.4** — Responds to identified security incidents

NIST-CSF-2

- **RS.CO-03** — Recovery activities and progress communicated

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1190	Exploit Public-Facing Application	Initial-Access
T1078	Valid Accounts	Defense-Evasion

Sources

Source	URL	Tier
	https://www.fiercehealthcare.com/regulatory/senate-help-committee-s...	T3
Senate Committee Leader Seeks Answers on NYC Health Hack	https://www.govinfosecurity.com/senate-committee-leader-seeks-answe...	T3
NYC Health + Hospitals faces Senate scrutiny after cyber incident	https://www.beckershospitalreview.com/healthcare-information-techno...	T3
Senate HELP committee chairman seeks info on NYC Health + ...	https://x.com/EpicPlain/status/2064157610698268748	T3
Chairman Cassidy Presses Zohran Mamdani, NYC Hospital on ...	https://www.help.senate.gov/rep/newsroom/press/chairman-cassidy-pre...	T1

Generated 2026-06-10 07:25 UTC by TJS Security Command Center