INTELLIGENCE BRIEFING
Security Command Center

TLP:CLEAR
2026-06-04 06:49 UTC

ViaQuest Psychiatric & Behavioral Solutions Data Breach Exposes PII and PHI of 6,420 Individuals

DATA BREACH | HIGH

SCC Item ID	SCC-DBR-2026-0147
Type	Data Breach
Severity	HIGH
Affected Products	ViaQuest Psychiatric & Behavioral Solutions (Ohio-based mental health provider), patients and staff
Published	2026-06-02
Discovery Source	Gemini

Executive Summary

ViaQuest Psychiatric & Behavioral Solutions, an Ohio-based behavioral health provider, disclosed a network server hacking incident affecting 6,420 current and former patients and staff. The breach exposed both PII and PHI, with heightened sensitivity given the psychiatric and behavioral health context of the compromised records. Business risk includes HIPAA regulatory exposure, reputational harm tied to the nature of the data, and active lawsuit investigation initiated in 2026.

Technical Analysis

The breach is classified as a hacking/network server incident per HHS OCR breach portal data (reporting date May 8, 2026). No CVE has been assigned; this is an organizational breach disclosure. CWE-359 (Exposure of Private Personal Information to an Unauthorized Actor) applies. MITRE ATT&CK techniques associated with this incident type include T1530 (Data from Cloud Storage) and T1078 (Valid Accounts). The specific intrusion method, initial access vector, and whether ransomware or exfiltration tooling was deployed have not been publicly confirmed. No patch or vendor advisory is applicable; remediation is organizational. Note: Technical details are sourced from HHS OCR breach portal registry; ViaQuest has not published independent official technical disclosure as of report date. Readers should cross-reference with primary HHS OCR filing for authoritative incident classification.

Action Checklist

1. Step 1: Containment, If your organization shares vendor relationships, data exchange agreements, or network connectivity with ViaQuest, immediately audit those connections for anomalous traffic. Isolate any shared data pipelines pending review. Reference NIST SP 800-61 Rev. 2 (Computer Security Incident Handling Guide) and notify relevant internal stakeholders.
2. Step 2: Detection, Review access logs for your EHR and PHI data stores for indicators matching T1078 (Valid Accounts abuse): off-hours logins, accounts accessing unusual data volumes, or logins from unfamiliar IP ranges. Enable or verify AU-2 (Event Logging) and AU-6 (Audit Record Review) are active across systems handling PHI. Apply local account monitoring per NIST AC-2 (Account Management) to identify unauthorized local account activity.
3. Step 3: Eradication, If any credential overlap exists with ViaQuest systems (shared service accounts, third-party vendor credentials), rotate those credentials immediately per NIST IA-4 (Identifier Management). Audit privileged account usage per NIST AC-6 (Least Privilege) and CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts).
4. Step 4: Recovery, Validate that MFA is enforced on all externally exposed applications and remote access per CIS 6.3 and CIS 6.4. Confirm audit logging integrity per NIST AU-9 (Protection of Audit Information). Review retention settings to ensure audit records meet AU-11 requirements for post-incident forensic support.
5. Step 5: Post-Incident, This incident highlights gaps in network server security and account management for healthcare environments. Assess your own controls against NIST SI-4 (System Monitoring) and CIS 8.2 (Collect Audit Logs). Evaluate whether PHI data flows are fully inventoried per CIS 3.2 (Establish and Maintain a Data Inventory) and whether access control lists are enforced per CIS 3.3.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to legal counsel, privacy officer, and executive leadership if forensic review of third-party connection logs, EHR access logs, or credential overlap analysis reveals any indicators of unauthorized access to your organization's PHI systems — given the active lawsuit investigation against ViaQuest disclosed in 2026, discovery of any related exposure triggers HIPAA Breach Notification Rule obligations (45 CFR §164.404) with a 60-day notification deadline and mandatory HHS OCR reporting.
Recovery Notes	Before resuming any data exchange with ViaQuest or affiliated vendors, obtain written attestation from ViaQuest that their network server compromise has been fully remediated and that a third-party forensic investigation has confirmed eradication — do not rely solely on their public disclosure. Monitor EHR access logs and PHI database query logs for a minimum of 90 days post-containment for anomalous account behavior, given that threat actors who compromise healthcare networks frequently maintain dormant persistence and return after initial response activity subsides. Given the psychiatric and behavioral health nature of the exposed records, coordinate with your HIPAA Privacy Officer to assess whether the heightened sensitivity of this PHI category requires notification to affected individuals beyond the standard breach notification threshold, as state mental health privacy laws (including Ohio Rev. Code §5122.31) may impose obligations independent of federal HIPAA requirements.

Forensic Artifacts	EHR application-layer audit logs showing user account, source IP, session duration, and record access count — bulk queries pulling psychiatric diagnosis codes (ICD-10 F-chapter codes), treatment notes, or insurance identifiers in a single session are the primary exfiltration signature for this breach type affecting 6,420 patient and staff records | Network firewall and proxy logs for all egress traffic from EHR and PHI database servers over the 90 days preceding ViaQuest's breach disclosure, specifically looking for large data transfers (>10MB sessions) to external IPs not in your authorized data exchange partner list — consistent with the network server hacking method disclosed | Windows Security Event Log Event IDs 4624 (Successful Logon), 4648 (Explicit Credential Use), and 4672 (Special Privileges Assigned) from domain controllers and EHR application servers, filtered to accounts with any naming convention or group membership associated with ViaQuest vendor access or third-party EHR integration service accounts | Database transaction logs (SQL Server LDF files, MySQL binary logs, or Oracle redo logs) from PHI data stores covering the breach window — these capture the specific tables queried and row counts returned, which is required to accurately scope whether your organization's data was accessed via any compromised shared connection | VPN and remote access gateway authentication logs (Cisco ASA, Palo Alto GlobalProtect, or Windows RRAS event logs) showing all successful authentications from IP ranges associated with ViaQuest's Ohio-based network infrastructure, which would indicate an adversary who compromised ViaQuest credentials subsequently used them to authenticate into connected partner environments

Per-Action IR Details

Step 1: Containment — If your organization shares vendor relationships, data exchange agreements, or network connectivity with ViaQuest, immediately audit those connections for anomalous traffic. Isolate any shared data pipelines pending review. Reference NIST IR-6 (Incident Reporting) and notify relevant internal stakeholders.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: isolate affected systems and third-party connections to prevent lateral spread while preserving evidence

Controls: NIST IR-4 (Incident Handling), NIST IR-6 (Incident Reporting), NIST AC-4 (Information Flow Enforcement), NIST SC-7 (Boundary Protection), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: Run 'netstat -ano' on servers with ViaQuest-connected interfaces to enumerate active connections; cross-reference with known ViaQuest IP ranges obtained from your data exchange agreement. Use Wireshark or tcpdump on the boundary interface ('tcpdump -i eth0 host -w viaquest_capture.pcap') to capture a 15-minute baseline before isolating. Block ViaQuest IP ranges at the host firewall using 'netsh advfirewall firewall add rule' (Windows) or 'iptables -I INPUT -s -j DROP' (Linux) pending review.

Evidence: Before isolating, capture: (1) full netflow or firewall session logs showing all traffic between your network and ViaQuest IP ranges for the prior 90 days — this establishes the normal communication baseline and will reveal anomalous data volumes consistent with exfiltration; (2) firewall deny/allow logs for ports associated with your EHR data exchange protocol (commonly HL7 over TCP 2575 or SFTP over TCP 22); (3) DNS query logs for any ViaQuest-associated domains queried by internal hosts, which may indicate beaconing if the attacker pivoted through ViaQuest infrastructure; (4) a packet capture snapshot of the active connection state before termination to document whether any sessions were mid-transfer at time of isolation.

Step 2: Detection — Review access logs for your EHR and PHI data stores for indicators matching T1078 (Valid Accounts abuse): off-hours logins, accounts accessing unusual data volumes, or logins from unfamiliar IP ranges. Enable or verify AU-2 (Event Logging) and AU-6 (Audit Record Review) are active across systems handling PHI. Apply D3-LAM (Local Account Monitoring) to identify unauthorized local account activity.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlate logs across PHI-handling systems to identify T1078 (Valid Accounts) abuse consistent with the network server hacking method used against ViaQuest

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-3 (Content of Audit Records), NIST SI-4 (System Monitoring), NIST AC-7 (Unsuccessful Logon Attempts), CIS 8.2 (Collect Audit Logs)

Compensating: On Windows EHR servers, query Security Event Log for Event ID 4624 (Successful Logon) filtered by Logon Type 3 (Network) and 10 (RemoteInteractive) outside business hours: 'Get-WinEvent -FilterHashtable @{LogName="Security"; Id=4624} | Where-Object {$_.TimeCreated.Hour -lt 7 -or $_.TimeCreated.Hour -gt 19}'. Also query Event ID 4648 (Explicit Credential Logon) and 4672 (Special Privileges Assigned) to surface privilege escalation. For Linux-based EHR or database servers, parse '/var/log/auth.log' and '/var/log/secure' for successful SSH authentications from non-standard source IPs. Deploy Sysmon with the SwiftOnSecurity config to capture process creation (Event ID 1) and network connections (Event ID 3) on PHI-handling hosts.

Evidence: Capture before analysis: (1) EHR application-layer access logs showing user account, timestamp, source IP, and record count per session — bulk PHI record queries (e.g., hundreds of patient records in a single session) are a primary exfiltration indicator for this breach type; (2) Windows Security Event Log Event ID 4624/4625 (logon success/failure) and 4776 (credential validation) from domain controllers and EHR application servers for the 90-day window prior to ViaQuest's disclosed breach discovery date; (3) database audit logs (SQL Server Audit, MySQL general query log, or Oracle Unified Audit) showing SELECT statements against PHI tables — specifically queries pulling name, date of birth, SSN, diagnosis codes, or insurance fields which match the data types ViaQuest confirmed were exposed; (4) VPN or remote access gateway logs showing authentication events tied to any accounts shared with or provisioned for ViaQuest staff or their vendors.

Step 3: Eradication — If any credential overlap exists with ViaQuest systems (shared service accounts, third-party vendor credentials), rotate those credentials immediately per D3-CRO (Credential Rotation). Audit privileged account usage per NIST AC-6 (Least Privilege) and CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: remove threat actor footholds by eliminating compromised credentials and unauthorized access paths before restoring normal operations

Controls: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), NIST IA-4 (Identifier Management), NIST IA-5 (Authenticator Management), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 5.3 (Disable Dormant Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Export a full account inventory from Active Directory using 'Get-ADUser -Filter * -Properties LastLogonDate, PasswordLastSet, MemberOf | Export-Csv accounts.csv'; filter for any accounts whose description, UPN, or group membership references ViaQuest, vendor names, or third-party EHR integration service names. For each identified account, force immediate password reset via 'Set-ADAccountPassword' and revoke active sessions with 'Invoke-Command {klist purge}' on affected hosts. Use osquery ('SELECT * FROM logged_in_users;' and 'SELECT * FROM user_ssh_keys;') on Linux EHR nodes to enumerate currently active sessions and SSH authorized_keys files that may contain vendor-provisioned keys.

Evidence: Before rotating credentials, preserve: (1) a timestamped export of all active sessions on EHR application servers and database hosts — this documents what was live at time of eradication and supports chain-of-custody for any later HIPAA breach investigation; (2) Windows Event ID 4720 (Account Created), 4722 (Account Enabled), 4728/4732/4756 (Member Added to Security Group) logs covering the period since ViaQuest's network server compromise began — threat actors who accessed ViaQuest may have used harvested credentials to create persistence accounts in connected environments; (3) a before-rotation dump of password policy and account privilege assignments (e.g., 'net user /domain') to document the pre-eradication access scope for the HIPAA breach notification record.

Step 4: Recovery — Validate that MFA is enforced on all externally exposed applications and remote access per CIS 6.3 and CIS 6.4. Confirm audit logging integrity per NIST AU-9 (Protection of Audit Information). Review retention settings to ensure audit records meet AU-11 requirements for post-incident forensic

support.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: restore systems to verified-secure operational state with confirmed access controls and logging integrity before resuming PHI data exchanges

Controls: NIST AU-9 (Protection of Audit Information), NIST AU-11 (Audit Record Retention), NIST AC-17 (Remote Access), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.5 (Require MFA for Administrative Access)

Compensating: Verify MFA enrollment coverage by querying your identity provider for accounts with MFA disabled: in Azure AD use 'Get-MsolUser -All | Where-Object {$_.StrongAuthenticationMethods.Count -eq 0}'; for on-prem environments without an IdP, enable Windows RD Gateway with NPS extension as a no-cost MFA enforcement point for remote access. Validate log integrity by comparing current log file hashes against your baseline using 'Get-FileHash -Algorithm SHA256' on Windows log directories or 'sha256sum /var/log/secure' on Linux — discrepancies indicate potential log tampering during the intrusion window. Verify AU-11 retention by checking your SIEM or log management retention policy is set to a minimum of 90 days online and 1 year archived, consistent with HIPAA audit log requirements.

Evidence: Before declaring recovery complete, capture: (1) a signed hash inventory of all audit logs covering the ViaQuest breach disclosure window (2025 through 2026 discovery date) — HIPAA enforcement and the disclosed active lawsuit investigation require demonstrating log integrity and continuity; (2) MFA enrollment audit report showing all accounts with access to PHI systems and their current MFA status, to serve as documentary evidence of post-incident hardening; (3) confirmation screenshots or CLI output showing log forwarding is active from EHR application servers to your centralized log store, ensuring no single-point log deletion risk on individual hosts.

Step 5: Post-Incident — This incident highlights gaps in network server security and account management for healthcare environments. Assess your own controls against NIST SI-4 (System Monitoring) and CIS 8.2 (Collect Audit Logs). Evaluate whether PHI data flows are fully inventoried per CIS 3.2 (Establish and Maintain a Data Inventory) and whether access control lists are enforced per CIS 3.3.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: conduct lessons-learned review focused on PHI data flow visibility, network server hardening gaps, and account management deficiencies revealed by the ViaQuest breach pattern

Controls: NIST SI-4 (System Monitoring), NIST RA-3 (Risk Assessment), NIST CA-7 (Continuous Monitoring), CIS 3.2 (Establish and Maintain a Data Inventory), CIS 3.3 (Configure Data Access Control Lists), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 8.2 (Collect Audit Logs)

Compensating: Conduct a PHI data flow mapping exercise using Wireshark on key network segments to passively identify hosts transmitting HL7, FHIR, or unencrypted health record data — any PHI leaving the EHR application tier to unexpected destinations is a finding. Build a Sigma rule targeting bulk PHI access patterns (high-volume SELECT queries, mass record exports) deployable in your SIEM or parsed against raw logs with 'sigma convert'; the Sigma community maintains healthcare-relevant rules at github.com/SigmaHQ/sigma (verify link before use). Document all PHI data stores, their access control lists, and data retention periods in a simple spreadsheet asset inventory if a formal CMDB is unavailable — this directly addresses the CIS 3.2 gap and provides the data inventory required for future HIPAA breach scope assessments.

Evidence: Preserve as post-incident documentation: (1) the completed PHI data flow diagram showing all systems that store, process, or transmit psychiatric and behavioral health records — this class of data carries heightened HIPAA sensitivity and the ViaQuest breach's lawsuit trajectory suggests regulators will scrutinize whether covered entities had adequate flow visibility; (2) a gap assessment report comparing current SI-4 monitoring coverage against all PHI-handling network segments, noting any unmonitored servers analogous to the ViaQuest network server that was compromised; (3) a formal record of the lessons-learned meeting per NIST 800-61r3 §4 recommendations, documenting what third-party connection audit procedures existed pre-incident and what procedural changes are being implemented — this record supports both HIPAA compliance documentation and defense-in-depth evidence if regulators inquire following the 2026 lawsuit activity.

Detection Guidance

This breach is classified as a network server hacking incident with T1530 (Data from Cloud Storage) and T1078 (Valid Accounts) as mapped techniques, suggesting data exfiltration via credential-based initial access. Detection priorities for organizations in the healthcare sector or with shared vendor exposure: (1) Query authentication logs for accounts accessing PHI repositories outside business hours or from anomalous source IPs. (2) Alert on bulk file access or export events from EHR systems, cloud storage buckets, or network file shares (T1530). (3) Monitor for encryption activity on file servers inconsistent with normal operations. (4) Apply system file analysis per NIST SI-7 (Software, Firmware, and Information Integrity) to detect modification of authentication databases or configuration files. (5) Cross-reference active service accounts against CIS 5.1 (Inventory of Accounts) and flag dormant accounts still in use per CIS 5.3. No confirmed IOCs are publicly available for this incident; detection must rely on behavioral indicators until ViaQuest publishes an official disclosure.

Framework Mappings

MITRE-ATTACK

- **T1486** — Data Encrypted for Impact
- **T1530** — Data from Cloud Storage
- **T1078** — Valid Accounts

NIST-800-53R5

- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **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
- **A.5.23** — Information security for use of cloud services

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
T1486	Data Encrypted for Impact	Impact
T1530	Data from Cloud Storage	Collection
T1078	Valid Accounts	Defense-Evasion

Sources

Source	URL	Tier
ViaQuest Psychiatric & Behavioral Solutions, LLC - May 8, 2026	https://data.rgj.com/health-care-data-breaches/viaquest-psychiatric...	T3
ViaQuest Renames Clinical Services Division to ViaQuest ...	https://viaquestinc.com/viaquest-renames-clinical-services-division...	T3
ViaQuest Data Breach Lawsuit Investigation - Claim Depot	https://www.claimdepot.com/investigations/viaquest-data-breach-2026	T3
Viaquest Behavioral Health Employee Reviews in Akron, OH - Indeed	https://www.indeed.com/cmp/Viaquest-Behavioral-Health/reviews?fcoun...	T3
VIAQUEST BEHAVIORAL HEALTH - Updated May 2026 - Yelp	https://www.yelp.com/biz/viaquest-behavioral-health-cincinnati	T3

Generated 2026-06-04 06:49 UTC by TJS Security Command Center