INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-18 18:49 UTC

DragonForce Threat Actor Claims AdvancedHEALTH Data Breach Affecting 2.3M Records

DATA BREACH | HIGH

SCC Item ID	SCC-DBR-2026-0130
Type	Data Breach
Severity	HIGH
Affected Products	AdvancedHEALTH (multi-specialty healthcare group, Tennessee)
Published	2026-05-18
Discovery Source	Gemini

Executive Summary

Ransomware group DragonForce has claimed responsibility for exfiltrating approximately 2.3 million records from AdvancedHEALTH, a Tennessee-based multi-specialty healthcare group, with alleged stolen data including patient names, Social Security numbers, medical records, and financial information. As of May 16, 2026, AdvancedHEALTH has not confirmed the breach or issued a public statement; attribution and scope remain unverified. If confirmed, the organization faces material HIPAA exposure, class-action liability, and significant reputational harm with its patient population.

Technical Analysis

DragonForce, a ransomware-as-a-service (RaaS) group known for double-extortion operations, has claimed exfiltration of approximately 2.3 million lines of data from AdvancedHEALTH. Claimed data types map to Protected Health Information (PHI) and Personally Identifiable Information (PII): patient names, Social Security numbers, medical records, and financial data. No CVE is associated with this incident. Relevant CWEs are CWE-200 (Exposure of Sensitive Information to an Unauthorized Actor) and CWE-359 (Exposure of Private Personal Information to an Unauthorized Actor). MITRE ATT&CK techniques associated with DragonForce operations include T1078 (Valid Accounts, likely initial access vector), T1041 (Exfiltration Over C2 Channel), T1486 (Data Encrypted for Impact), and T1567.002 (Exfiltration to Cloud Storage). No CISA KEV entry exists. No vendor advisory or official patch is applicable at this stage. Breach confirmation and attack vector remain unverified pending official disclosure. Source quality is Tier 3 (legal aggregator and social media); no primary victim or government source has confirmed. Confidence in breach occurrence: medium. Confidence in DragonForce attribution: low-to-medium.

Action Checklist

1. Step 1: Awareness. If your organization partners with, integrates with, or shares data with AdvancedHEALTH, assess whether PHI or PII was transmitted to them and document the data-sharing relationship. Begin scoping immediately; do not delay pending official confirmation.
2. Step 2: Detection. Review outbound data transfer logs, cloud storage upload events, and VPN/remote access authentication logs for anomalies consistent with T1041 and T1567.002. Hunt for T1078 indicators: off-hours logins, logins from unfamiliar geolocations, and accounts with unexpected privilege escalation. If you share a vendor ecosystem with AdvancedHEALTH, treat their breach claim as a third-party risk signal.
3. Step 3: Third-Party Risk. Verify Business Associate Agreements (BAAs) with AdvancedHEALTH if applicable. Under HIPAA, covered entities must assess whether a breach at a business associate triggers their own notification obligations.
4. Step 4: Monitor for Secondary Exploitation. 2.3M records containing SSNs and financial data create a downstream phishing and fraud surface. Brief your SOC on increased likelihood of targeted spear-phishing against patients or staff whose data may have been exposed. No confirmed IOCs are available at this time.
5. Step 5: Post-Incident Controls Review. This incident pattern (RaaS double extortion against a healthcare organization) reflects persistent sector targeting. Audit privileged access management (PAM) controls, MFA enforcement on remote access, and data loss prevention (DLP) policies covering PHI/PII egress. Reference NIST SP 800-53 AC-2, AC-17, and SI-12 for control gaps commonly exploited in this attack pattern.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to legal, compliance, and executive leadership if: (1) your organization has an active BAA with AdvancedHEALTH and can confirm PHI was transmitted to them, triggering HIPAA 45 CFR §164.400-414 breach assessment and the 60-day notification clock; (2) your own telemetry surfaces T1078 or T1041 indicators consistent with DragonForce lateral movement or exfiltration activity in your environment; or (3) AdvancedHEALTH confirms the breach or HHS OCR opens an investigation, as both events materially alter your regulatory exposure timeline.
Recovery Notes	If your organization determines PHI was exposed via AdvancedHEALTH, recovery must include: completing the HIPAA four-factor breach risk assessment to determine notification obligations, notifying affected individuals within 60 days of discovery per 45 CFR §164.410, and reporting to HHS OCR (breaches affecting 500+ individuals require reporting within 60 days to the HHS Breach Portal). Monitor your environment for a minimum of 90 days post-assessment for secondary exploitation activity — DragonForce and its affiliates operationalize stolen healthcare PII for downstream phishing and fraud campaigns that typically surface 30-90 days after exfiltration. Verify that any data-sharing interfaces with AdvancedHEALTH are suspended or placed under enhanced monitoring until AdvancedHEALTH provides a credible remediation attestation.

Forensic Artifacts	HL7/FHIR interface engine transaction logs (e.g., Mirth Connect /logs/ directory or Epic Integration Engine audit trail) showing outbound PHI message volumes and destination endpoints for AdvancedHEALTH — these establish the specific record categories and patient populations potentially within scope of the 2.3M claimed exfiltration | Microsoft 365 Unified Audit Log or on-premises Exchange message tracking logs for file transfers, secure messages, or attachments exchanged with AdvancedHEALTH domains — preserves evidence of PHI categories transmitted and data-sharing volume independent of the BAA documentation | VPN authentication logs (Cisco ASA: %ASA-6-713228, Palo Alto GlobalProtect authentication events) for AdvancedHEALTH-associated accounts or IP ranges in the 90-day window before May 16, 2026 — DragonForce affiliates maintain persistent VPN access using stolen or purchased credentials before deploying ransomware | Windows Security Event ID 4663 (Object Access — File Read) bulk aggregations on file servers or NAS shares containing PHI, filtered for reads of >500 files within a short time window — this artifact pattern is characteristic of DragonForce affiliate staging behavior prior to rclone-based exfiltration matching T1041 and T1567.002 | Dark web and threat actor leak site references: manual or automated checks against DragonForce's known .onion leak site and paste sites for AdvancedHEALTH data samples — if the claimed 2.3M records are partially published as proof, the sample data will indicate which PHI categories and which patient or staff populations are confirmed exposed, directly scoping your notification obligations

Per-Action IR Details

Step 1: Awareness — If your organization partners with, integrates with, or shares data with AdvancedHEALTH, assess whether PHI or PII was transmitted to them and document the data-sharing relationship. Do not wait for official confirmation before scoping exposure.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Establishing IR capability and identifying data-sharing dependencies before an incident is declared

Controls: NIST IR-4 (Incident Handling) — requires preparation that includes identifying third-party data-sharing relationships as a precondition to effective response, NIST IR-8 (Incident Response Plan) — IR plan must account for third-party breach scenarios that trigger the organization's own obligations, NIST RA-3 (Risk Assessment) — assess likelihood and impact of PHI/PII exposure through AdvancedHEALTH as a data-sharing partner, CIS 3.2 (Establish and Maintain a Data Inventory) — data inventory must be current enough to identify what PHI/PII was transmitted to AdvancedHEALTH and under what mechanisms

Compensating: Run a query against your email gateway archive (Exchange PowerShell: Get-MessageTrackingLog -Recipients *advancedhealth* -Start [90-day window]) to identify staff who exchanged data with AdvancedHEALTH. Cross-reference against your data inventory spreadsheet or SharePoint DLP audit log exports. For HL7/FHIR interface engines (e.g., Mirth Connect), check the channel transaction logs at /logs/mirth/ for outbound messages routed to AdvancedHEALTH endpoints. Document findings in a shared incident tracking sheet (even a dated spreadsheet) to establish a defensible scope record.

Evidence: Before scoping, preserve: (1) HL7/FHIR interface engine transaction logs showing outbound PHI transmissions to AdvancedHEALTH IP ranges or SFTP endpoints; (2) email gateway logs for any file transfers or secure messaging to @advancedhealth.com or affiliated domains; (3) VPN/remote access logs showing AdvancedHEALTH staff or systems authenticating to your environment; (4) BAA executed agreements and data flow diagrams on file; (5) API gateway or HTTPS proxy logs for EHR-to-EHR integration calls (e.g., Epic Care Everywhere, CommonWell, Carequality queries) directed at AdvancedHEALTH endpoints.

Step 2: Detection — Review outbound data transfer logs, cloud storage upload events, and VPN/remote access authentication logs for anomalies consistent with T1041 and T1567.002. Hunt for T1078 indicators: off-hours logins, logins from unfamiliar geolocations, and accounts with unexpected privilege escalation. If you share a vendor ecosystem with AdvancedHEALTH, treat their breach claim as a third-party risk signal.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection & Analysis: Correlating third-party breach claims against your own telemetry to determine if the DragonForce campaign extends into your environment

Controls: NIST SI-4 (System Monitoring) — monitor for T1078 (Valid Accounts) and T1041 (Exfiltration Over C2 Channel) indicators in authentication and egress telemetry, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — systematic review of VPN, cloud storage, and outbound transfer logs for DragonForce-consistent exfiltration patterns, NIST IR-5 (Incident Monitoring) — track and document anomalies identified during this hunt as candidate incidents, CIS 8.2 (Collect Audit Logs) — audit logs must be enabled and retained across VPN concentrators, cloud storage services, and authentication systems to support this detection step

Compensating: For T1078 hunting without SIEM: run this PowerShell on your domain controller to surface off-hours logins — Get-EventLog Security -InstanceId 4624 | Where-Object {$_.TimeGenerated.Hour -lt 6 -or $_.TimeGenerated.Hour -gt 20} | Select TimeGenerated,Message | Export-Csv offhours_logins.csv. For T1567.002 (exfiltration to cloud storage): query Windows DNS debug logs or router/firewall syslog for DNS queries to *.onedrive.com, *.dropbox.com, *.mega.nz, *.anonfiles.com, or *.gofile.io from clinical workstations. Deploy the Sigma rule 'proc_creation_win_rclone_exec.yml' via Chainsaw or Hayabusa against collected Windows event logs to detect rclone, which DragonForce affiliates have used for bulk staging. For T1041, filter firewall deny/allow logs for large outbound TCP sessions (>100MB) to non-whitelisted IPs during off-hours.

Evidence: Preserve before hunting: (1) Windows Security Event Log Event ID 4624 (Successful Logon) and 4625 (Failed Logon) from VPN-facing systems and domain controllers, filtered for logon type 3 and 10 (network/remote interactive) from external IPs; (2) Event ID 4672 (Special Privileges Assigned to New Logon) for accounts that received unexpected elevated rights; (3) Cloud storage audit logs — Microsoft 365 Unified Audit Log for FileUploaded/FileSyncUploadedFull operations from clinical endpoints; (4) Firewall/proxy egress logs showing large outbound data volumes to non-EMR cloud destinations in the 30-day window preceding the May 16 claim date; (5) DNS query logs for lookups to known DragonForce or generic RaaS exfiltration infrastructure (MEGA, cloud storage, Tor exit nodes).

Step 3: Third-Party Risk — Verify Business Associate Agreements (BAAs) with AdvancedHEALTH if applicable. Under HIPAA, covered entities must assess whether a breach at a business associate triggers their own notification obligations.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment: Executing IR plan coordination with third parties and assessing whether the DragonForce claim against AdvancedHEALTH triggers your organization's own regulatory containment and notification obligations

Controls: NIST IR-4 (Incident Handling) — incident handling capability must include third-party breach scenarios where a business associate's compromise triggers the covered entity's own HIPAA 45 CFR §164.400-414 breach assessment, NIST IR-6 (Incident Reporting) — personnel must report findings from the BAA review and PHI exposure assessment to organizational IR capability and legal/compliance within defined timeframes consistent with HIPAA's 60-day notification clock, NIST IR-8 (Incident Response Plan) — IR plan should pre-define the HIPAA breach determination workflow, including the four-factor risk assessment (nature of PHI, unauthorized persons, whether PHI was acquired, extent of mitigation) required under 45 CFR §164.402, NIST RA-3 (Risk Assessment) — conduct the HIPAA required risk assessment to determine whether the presumption of breach applies given AdvancedHEALTH's failure to confirm or deny

Compensating: Without a dedicated GRC platform: create a BAA verification checklist in a shared document — fields should include: BAA execution date, data elements covered, PHI transmission mechanism, last data exchange date, and AdvancedHEALTH contact for breach notification. Send a formal written inquiry to AdvancedHEALTH's Privacy Officer via certified mail and email, timestamped, to document your due diligence. Log all contact attempts; under HIPAA the clock runs from when you knew or should have known of the potential breach, not when AdvancedHEALTH confirms it. Use HHS's Breach Risk Assessment Tool guidance (at hhs.gov/hipaa) to document the four-factor analysis. Note: this step requires legal/compliance involvement — see escalation criteria.

Evidence: Preserve before acting: (1) Executed BAA documents with AdvancedHEALTH, including any amendments or addenda specifying PHI categories and permitted uses; (2) Data flow diagrams or interface documentation showing what PHI types (patient names, SSNs, medical records, financial data — the categories DragonForce claimed) were

transmitted to AdvancedHEALTH and in what volume; (3) Last-known data exchange timestamp from interface engine or SFTP logs, establishing the outer boundary of potentially affected records; (4) Any prior breach or security incident notifications received from AdvancedHEALTH; (5) Your organization's HIPAA breach determination documentation from prior incidents, as a template baseline for this assessment.

Step 4: Monitor for Secondary Exploitation — 2.3M records containing SSNs and financial data create a downstream phishing and fraud surface. Brief your SOC on increased likelihood of targeted spear-phishing against patients or staff whose data may have been exposed. No confirmed IOCs are available at this time.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection & Analysis: Expanding detection scope to anticipate T1566 (Phishing) follow-on activity enabled by DragonForce's claimed exfiltration of 2.3M patient and staff records

Controls: NIST SI-3 (Malicious Code Protection) — update email security gateway rules to flag lures referencing AdvancedHEALTH, patient portal resets, or HIPAA breach notification themes consistent with how threat actors operationalize stolen healthcare PII, NIST SI-4 (System Monitoring) — expand monitoring scope to cover inbound phishing lures exploiting the AdvancedHEALTH data set, and outbound credential theft callbacks if staff click on lures, NIST IR-4 (Incident Handling) — the SOC briefing constitutes a preparation update to the active incident handling capability, expanding the incident's threat surface definition, CIS 9.2 (Use DNS Filtering Services) — enable or tune DNS filtering to block newly registered domains mimicking AdvancedHEALTH or patient notification themes (e.g., advancedhealth-breach-notice[.]com patterns)

Compensating: Without enterprise email security: deploy the following in your on-premises email gateway or Microsoft 365 Defender — create a transport rule blocking or quarantining messages with subject lines containing: 'AdvancedHEALTH', 'data breach notification', 'HIPAA notice', 'patient portal reset', combined with external sender origin. Use PhishTank or URLScan.io to manually check suspicious URLs in flagged emails. Brief SOC analysts using a one-page threat context document specifying: DragonForce claimed exfiltration of names, SSNs, medical records, and financial data from a Tennessee healthcare group; downstream phishing lures will likely impersonate patient breach notifications or credit monitoring enrollment. Enable Microsoft 365 Unified Audit Log search for MailItemsAccessed (E3/E5) to detect staff inbox compromise if phishing succeeds.

Evidence: Preserve before and during monitoring: (1) Email gateway/Microsoft 365 Message Trace logs for inbound messages referencing AdvancedHEALTH or healthcare breach notification themes, with sender IP, SPF/DKIM/DMARC pass-fail status; (2) DNS query logs for staff endpoints resolving lookalike domains registered after May 16, 2026 (use WHOIS date filtering); (3) Proxy/web filter logs for GET requests to credential harvesting pages accessed from clinical or administrative workstations; (4) Windows Security Event ID 4768 (Kerberos TGT Request) and 4776 (NTLM Authentication) spikes following any phishing campaign delivery, indicating credential use after compromise; (5) Any dark web or paste site references to the AdvancedHEALTH data set appearing after the DragonForce claim, monitored via free services such as Have I Been Pwned breach feed or manual checks on threat actor leak sites.

Step 5: Post-Incident Controls Review — This incident pattern (RaaS double extortion against a healthcare organization) reflects persistent sector targeting. Audit privileged access management (PAM) controls, MFA enforcement on remote access, and data loss prevention (DLP) policies covering PHI/PII egress. Reference NIST SP 800-53 AC-2, AC-17, and SI-12 for control gaps commonly exploited in this attack pattern.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Applying lessons from the DragonForce-AdvancedHEALTH double-extortion pattern to identify and close PAM, MFA, and DLP control gaps that RaaS affiliates consistently exploit in healthcare environments

Controls: NIST AC-2 (Account Management) — audit service accounts, shared credentials, and dormant privileged accounts that DragonForce affiliates exploit via T1078 (Valid Accounts) for initial access and lateral movement in healthcare environments, NIST AC-17 (Remote Access) — verify MFA is enforced on all remote access pathways (VPN, RDP, Citrix, EMR web portals); DragonForce and its RaaS affiliates frequently gain initial access through MFA-absent remote desktop and VPN endpoints, NIST SI-12 (Information Management and Retention) — review DLP policies governing PHI/PII egress to ensure bulk exfiltration of the type claimed (2.3M records including SSNs, medical

records, financial data) would be detected and blocked at cloud storage and email boundaries, NIST SI-2 (Flaw Remediation) — audit patch currency on internet-facing systems including VPN appliances, EMR web modules, and file transfer services, as RaaS initial access frequently involves unpatched perimeter vulnerabilities, CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts) — enforce separation of privileged and standard accounts; verify no clinical workstation accounts hold local admin or domain admin rights that would facilitate DragonForce-style lateral movement post-initial-access, CIS 6.3 (Require MFA for Externally-Exposed Applications) — verify MFA coverage on all patient portal, EMR, and administrative web applications exposed to the internet, CIS 6.5 (Require MFA for Administrative Access) — MFA must be enforced on all domain admin, local admin, and backup operator accounts — backup infrastructure is a primary DragonForce double-extortion target, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — conduct a vulnerability scan of internet-facing systems and prioritize findings consistent with RaaS initial access vectors (VPN CVEs, unpatched RDP, exposed file transfer services)

Compensating: For a 2-person team with no PAM tooling: run 'net localgroup administrators' on a sample of 10-20 clinical and administrative workstations via PsExec or PowerShell remoting to identify non-compliant local admin memberships. Audit MFA enrollment in your IdP (Azure AD/Entra: Get-MsolUser -All | Where-Object {$_.StrongAuthenticationMethods.Count -eq 0} | Select UserPrincipalName) and produce a gap list for accounts with remote access entitlements. For DLP without enterprise tooling: enable Windows 10/11 built-in Audit Object Access (auditpol /set /subcategory:'File System' /success:enable /failure:enable) on file servers containing PHI, and alert on bulk file reads (>500 files in <10 minutes) using a simple PowerShell Event ID 4663 aggregation script. Review Azure/M365 DLP policy coverage for SSN and medical record number patterns using the built-in sensitive information types at no additional cost.

Evidence: Preserve before the audit: (1) Active Directory privileged group membership exports (Domain Admins, Backup Operators, Remote Desktop Users) timestamped at current state, to establish a baseline for comparison against state at time of any breach; (2) MFA enrollment reports from your IdP covering all accounts with VPN, RDP, or EMR administrative access; (3) DLP policy configuration exports and any DLP alert logs from the 90-day period preceding the May 16 DragonForce claim, to assess whether a bulk exfiltration event would have been detected; (4) VPN concentrator authentication logs showing concurrent session counts and off-hours access patterns, consistent with DragonForce affiliates using stolen credentials for persistent remote access; (5) Backup system access logs and backup job history, as DragonForce double-extortion methodology specifically targets and deletes or encrypts backups to maximize leverage.

Detection Guidance

No confirmed IOCs are available for this incident as of reporting. Detection should focus on behavioral indicators consistent with DragonForce TTPs. For T1078 (Valid Accounts): review authentication logs for off-hours access, impossible travel events, and accounts accessing systems outside their normal baseline. For T1041/T1567.002 (Exfiltration): alert on large outbound data transfers, particularly to cloud storage endpoints (Mega.nz, anonymous S3 buckets, paste sites) that are not part of approved workflows. For T1486 (Ransomware): monitor for mass file rename events, shadow copy deletion (vssadmin delete shadows), and encryption of large file sets in short time windows. SIEM query focus: privileged account anomalies, DLP alerts on PHI field patterns (SSN regex, ICD codes), and unusual process execution on systems hosting patient records. Note: these are pattern-based detections, not IOC-based; no hashes, IPs, or domains have been confirmed for this incident.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`none confirmed`	No IOCs have been publicly attributed to this incident as of May 16, 2026. Monitor threat intelligence feeds for DragonForce infrastructure updates.	LOW

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1041** — Exfiltration Over C2 Channel
- **T1486** — Data Encrypted for Impact
- **T1567.002** — Exfiltration to Cloud Storage

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **AC-3** — Access Enforcement
- **SC-28** — Protection of Information at Rest

OWASP-TOP10-2021

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

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.308(a)(6)(ii)** — Response and Reporting

SOC2-TSC

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

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1041	Exfiltration Over C2 Channel	Exfiltration
T1486	Data Encrypted for Impact	Impact
T1567.002	Exfiltration to Cloud Storage	Exfiltration

Sources

Source	URL	Tier
Possible AdvancedHEALTH Data Breach Reported	https://www.classaction.org/data-breach-lawsuits/advancedhealth-may...	T3
AdvancedHEALTH Data Breach Lawsuit - Class Action U	https://classactionu.org/current-data-breaches/advancedhealth/	T3
Attorneys working with ClassAction.org are looking into whether a ...	https://www.instagram.com/p/DYfXGuuGiZS/	T3
Patient medical records compromised by cyberattack at Columbia ...	https://www.facebook.com/WSMVTV/posts/patient-medical-records-compr...	T3
Advanced Medical Management Experiences Data Breach That ...	https://www.jdsupra.com/legalnews/advanced-medical-management-exper...	T3

Generated 2026-05-18 18:49 UTC by TJS Security Command Center