INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-12 07:02 UTC

Ransomware Claims Target Advanced Family Surgery Center, Orem Eye Clinic, and Belmont Aesthetic & Reconstructive Plastic Surgery

DATA BREACH | HIGH | CVSS 8.1

SCC Item ID	SCC-DBR-2026-0162
Type	Data Breach
Severity	HIGH
CVSS Base Score	8.1
Affected Products	Advanced Family Surgery Center, Orem Eye Clinic, Belmont Aesthetic & Reconstructive Plastic Surgery, healthcare provider networks and patient data systems
Published	2026-06-11
Discovery Source	Gemini

Executive Summary

Ransomware threat actors have claimed attacks against three U.S. healthcare providers, Advanced Family Surgery Center, Orem Eye Clinic, and Belmont Aesthetic & Reconstructive Plastic Surgery, with double-extortion tactics alleged at Advanced Family Surgery Center, including exfiltration of patient insurance records, diagnoses, and Social Security numbers before encryption. All three organizations face potential HIPAA breach notification obligations and significant reputational exposure given the sensitivity of the data involved. Attribution remains unconfirmed, no specific exploited vulnerability has been publicly identified, and source reporting is based on threat actor claims that have not been independently verified by the affected organizations as of available data.

Technical Analysis

Three U.S. healthcare providers have been named in ransomware group claims. The Advanced Family Surgery Center incident exhibits double-extortion characteristics: data exfiltration of PHI and PII (insurance records, diagnoses, Social Security numbers) alleged prior to encryption, consistent with MITRE T1083 (File and Directory Discovery), T1041 (Exfiltration Over C2 Channel), and T1486 (Data Encrypted for Impact). Initial access vector is unconfirmed but aligns with common ransomware entry patterns: phishing (T1566), valid account abuse (T1078), and service disruption via T1489. Exfiltration for leverage maps to T1657. No CVE has been identified in available source data. Relevant CWEs: CWE-693 (Protection Mechanism Failure), CWE-311 (Missing Encryption of Sensitive Data), CWE-284 (Improper Access Control). No patch is applicable because no

specific vulnerability has been identified. Threat actor attribution is unconfirmed. Source quality score is 0.56; primary sourcing is HIPAA Journal (T3), retrieved via discovery and not directly verified by this analysis.

Action Checklist

1. Step 1: Containment. Isolate any systems showing anomalous encryption activity, unexpected process termination (T1489), or large outbound data transfers. Segment clinical and administrative networks if flat architecture exists. Reference NIST AC-4 (Information Flow Enforcement) to enforce network segmentation boundaries.
2. Step 2: Detection. Review endpoint and SIEM logs for indicators of double-extortion staging: bulk file enumeration (T1083), outbound transfers to unknown destinations (T1041), and encryption process spawning (T1486). Check for dormant or compromised accounts used for lateral movement (T1078); audit privileged account activity against NIST AC-2 (Account Management) baseline. Enable local account anomaly monitoring for anomalous account behavior.
3. Step 3: Eradication. No specific patch or CVE remediation applies; focus on credential rotation for all accounts with access to PHI systems per NIST IA-4 (Identifier Management). Enforce MFA on all remote access and administrative interfaces per CIS 6.3, CIS 6.4, and CIS 6.5. Harden authentication posture through NIST IA-5 (Authentication) enforcement. Review and restrict user account permissions per NIST AC-6 (Least Privilege).
4. Step 4: Recovery. Before restoring from backup, verify backup integrity and confirm backups were not accessed or encrypted during the intrusion window. Validate restored systems against known-good configuration baselines per CIS 4.6. Monitor for re-infection or secondary persistence mechanisms using NIST SC-7 (Boundary Protection) and system initialization analysis. Maintain enhanced logging per NIST AU-6 and CIS 8.2 during the recovery period.
5. Step 5: Post-Incident. Conduct a gap assessment against NIST AC-6 (Least Privilege) and NIST AC-5 (Separation of Duties) to identify over-permissioned accounts that enabled lateral movement. Review audit log coverage and retention adequacy per NIST AU-11 (Audit Record Retention) and NIST AU-4 (Audit Storage Capacity). Evaluate whether phishing-resistant MFA and email filtering controls were in place; map gaps to CIS 7.1 and CIS 7.2 for remediation prioritization. Initiate HIPAA breach risk assessment immediately.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to executive leadership, legal counsel, and external DFIR retainer immediately upon confirmation of PHI exfiltration or encryption affecting any of the three named organizations, as double-extortion ransomware involving patient SSNs, insurance records, and diagnoses triggers mandatory HIPAA breach notification to HHS OCR within 60 days (45 CFR §164.400–414) and may trigger state attorney general notification; involve FBI Cyber Division (IC3) and HHS OCR concurrently if exfiltration is confirmed.

Recovery Notes	Restore PHI systems only from backups with a verified timestamp predating the earliest evidence of threat actor presence — not merely the encryption event — given that double-extortion actors typically dwell for days to weeks during the exfiltration phase before triggering encryption. Maintain enhanced logging (Sysmon, Windows Security Auditing at Success+Failure for logon, object access, and process creation) on all restored EHR, billing, and patient records systems for a minimum of 30 days post-restoration, with daily log review, to detect re-infection via any persistence mechanism or credential not identified during eradication. Verify that all restored systems' VSS/backup agents are functional and producing clean snapshots before declaring recovery complete, as ransomware groups frequently return to organizations that paid or failed to fully eradicate the initial access vector.
Forensic Artifacts	Windows Security Event Log (Event IDs 4663, 4688, 4624, 4648, 4698, 7045) on EHR servers and billing workstations — captures the file enumeration, privileged logon, scheduled task persistence, and process execution chain specific to double-extortion staging against PHI directories | Network flow logs or firewall egress logs showing sustained large-volume HTTPS/SFTP transfers to non-healthcare IP ranges during the exfiltration window — the specific mechanism by which patient insurance records, diagnoses, and SSNs were moved off-premises before encryption was triggered | Prefetch files (%SystemRoot%\Prefetch) and ShimCache/AmCache registry entries for known data exfiltration binaries (rclone.exe, MEGAsync.exe, WinSCP.exe, FileZilla.exe) executed on clinical or administrative hosts during the intrusion window | Volume Shadow Copy deletion event records (Sysmon Event ID 1 filtered on vssadmin.exe, wmic.exe with 'shadowcopy delete' arguments, or PowerShell 'Get-WmiObject Win32_ShadowCopy | Remove-WmiObject') confirming the ransomware's anti-recovery action sequence on each affected host | EHR application-layer audit logs (e.g., Epic access audit, Meditech audit trail, Athenahealth access logs) documenting which patient records — specifically those containing SSNs, insurance policy numbers, and diagnoses — were accessed or exported during the intrusion window, required for scoping the HIPAA breach notification population under 45 CFR §164.402

Per-Action IR Details

Step 1: Containment — Isolate any systems showing anomalous encryption activity, unexpected process termination (T1489), or large outbound data transfers. Segment clinical and administrative networks if flat architecture exists. Reference NIST AC-4 (Information Flow Enforcement) to enforce network segmentation boundaries.

NIST Phase: Containment

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

Controls: NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: On Windows hosts without EDR, run 'Get-NetTCPConnection | Where-Object {$_.State -eq "Established"} | Sort-Object RemoteAddress' and 'netstat -ano' to identify active outbound connections before isolation. Use Windows Firewall (netsh advfirewall) or a managed switch VLAN to hard-segment clinical (EHR/PACS) VLANs from administrative subnets immediately. On Linux hosts, use 'ss -tulnp' and iptables DROP rules for non-essential egress.

Evidence: BEFORE isolating any host: acquire full RAM image using Magnet RAM Capture or WinPmem; capture 'netstat -ano' and 'Get-NetTCPConnection' output to document active C2 or exfiltration sessions; export Windows Event Log — Security (Event ID 4624/4625/4648 for active sessions, Event ID 7045 for newly installed ransomware services), System (Event ID 7036 for service state changes), and Application logs; capture running process list ('Get-Process | Select-Object Name,Id,Path,StartTime' or 'tasklist /v /fo csv'); snapshot Volume Shadow Copy status ('vssadmin list shadows') before ransomware deletes them; document any open file handles on PHI directories (handle.exe from Sysinternals). These artifacts are destroyed the moment the host is isolated or powered off.

Step 2: Detection — Review endpoint and SIEM logs for indicators of double-extortion staging: bulk file enumeration (T1083), outbound transfers to unknown destinations (T1041), and encryption process spawning (T1486). Check for dormant or compromised accounts used for lateral movement (T1078); audit privileged account activity against NIST AC-2 (Account Management) baseline. Enable D3-LAM (Local Account Monitoring) for anomalous local account behavior.

NIST Phase: Detection Analysis

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

Controls: NIST AC-2 (Account Management), NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-2 (Event Logging), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 8.2 (Collect Audit Logs)

Compensating: Without SIEM, use Sysmon (Event IDs 1, 3, 11, 23) deployed with SwiftOnSecurity config to catch bulk file access and suspicious process spawning. Query Windows Security log for Event ID 4663 (file object access) on PHI directories and Event ID 4688 (process creation) filtering for cmd.exe, powershell.exe, rclone.exe, or MEGAsync.exe spawned by clinical application processes. Use 'Get-WinEvent' PowerShell cmdlet with XPath filters for offline log review. For network exfiltration detection without EDR, run Wireshark or tcpdump capturing traffic on port 443/80 egress and filter for large sustained transfers (>100MB) to non-healthcare IP ranges.

Evidence: Capture before any account lockout or credential rotation: Windows Security Event Log Event ID 4624 (successful logon) and 4648 (explicit credential use) filtered for service accounts and admin accounts accessing EHR/billing systems outside business hours; Event ID 4663 on PHI directories (e.g., C:\PatientRecords, EHR database file paths) showing recursive enumeration patterns; Sysmon Event ID 3 (network connections) for rclone, MEGAsync, or curl/wget processes; prefetch files (%SystemRoot%\Prefetch) for exfiltration tool execution (rclone.exe-XXXXXXXX.pf, winscp.exe-XXXXXXXX.pf); browser history and PowerShell history ($env:APPDATA\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt) for staging commands; Windows Security Event ID 4720/4732 for newly created local accounts added to privileged groups during the intrusion window.

Step 3: Eradication — No specific patch or CVE remediation applies; focus on credential rotation for all accounts with access to PHI systems per D3-CRO (Credential Rotation). Enforce MFA on all remote access and administrative interfaces per CIS 6.3, CIS 6.4, and CIS 6.5, and apply D3-MFA countermeasure. Harden authentication posture per D3-CH (Credential Hardening). Review and restrict user account permissions per D3-UAP.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-2 (Account Management), NIST AC-3 (Access Enforcement), NIST AC-6 (Least Privilege), CIS 5.2 (Use Unique Passwords), CIS 5.3 (Disable Dormant Accounts), 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: Without enterprise IAM tooling, use Active Directory bulk password reset via PowerShell ('Get-ADUser -Filter {Enabled -eq $true} | Set-ADAccountPassword') prioritizing all accounts with ACL access to EHR, billing, and insurance record directories. For MFA without budget, deploy Duo Free tier or Microsoft Authenticator (free for Azure AD) on VPN and RDP gateways immediately. Audit and disable dormant accounts using 'Search-ADAccount -AccountInactive -TimeSpan 45.00:00:00 | Disable-ADAccount'. Remove accounts from Domain Admins and local Administrators groups that have no documented administrative need.

Evidence: BEFORE rotating any credentials: export a full dump of all active sessions on domain controllers ('qwinsta /server:' and 'query session /server:'); capture Windows Security Event ID 4672 (special privileges assigned at logon) and Event ID 4698/4702 (scheduled task created/modified) to document persistence mechanisms installed under compromised credentials; dump LSASS memory (using procdump -ma lsass.exe to a secured analyst workstation, NOT the compromised host) if threat actor tooling such as Mimikatz is suspected — this volatile credential store is gone after credential rotation invalidates cached hashes; document all VPN and RDP session logs from the remote access gateway covering the intrusion window before log rotation.

Step 4: Recovery — Before restoring from backup, verify backup integrity and confirm backups were not accessed or encrypted during the intrusion window. Validate restored systems against known-good configuration baselines per CIS 4.6. Monitor for re-infection or secondary persistence mechanisms using D3-SICA (System Init Config Analysis). Maintain enhanced logging per NIST AU-6 and CIS 8.2 during the recovery period.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-9 (Protection Of Audit Information), CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 8.2 (Collect Audit Logs)

Compensating: Without enterprise backup validation tooling, hash-verify backup archives using CertUtil ('certutil -hashfile SHA256') and compare against stored checksums from before the intrusion window. Use Sysinternals Autoruns (autoruns.exe -a * -c > autoruns_output.csv) on each restored host to enumerate all persistence locations (Run keys, scheduled tasks, services, WMI subscriptions, browser extensions) and diff against a known-clean baseline export. Deploy ClamAV with updated signatures for post-restore malware scanning on restored PHI servers.

Evidence: Before restoring any system from backup, confirm the backup storage target itself was not within the blast radius: check backup server access logs (Windows Security Event ID 4624 on backup server) for unauthorized access during the intrusion window; verify Volume Shadow Copy deletion events (Event ID 524 in System log, or Sysmon Event ID 1 for vssadmin.exe or wmic shadowcopy delete commands) to establish whether backups on the live system were wiped; examine backup solution audit logs (e.g., Veeam job logs, Windows Server Backup event log under Microsoft-Windows-Backup) for job failures or unauthorized access matching the intrusion timeline; document the last known-clean backup timestamp as the recovery point objective anchor before initiating restoration.

Step 5: Post-Incident — Conduct a gap assessment against NIST AC-6 (Least Privilege) and NIST AC-5 (Separation of Duties) to identify over-permissioned accounts that enabled lateral movement. Review audit log coverage and retention adequacy per NIST AU-11 (Audit Record Retention) and NIST AU-4 (Audit Storage Capacity). Evaluate whether phishing-resistant MFA and email filtering controls were in place; map gaps to CIS 7.1 and CIS 7.2 for remediation prioritization. Initiate HIPAA breach risk assessment immediately.

NIST Phase: Post Incident

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

Controls: NIST AC-5 (Separation Of Duties), NIST AC-6 (Least Privilege), NIST AU-4 (Audit Storage Capacity), NIST AU-11 (Audit Record Retention), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Without a GRC platform, conduct the least-privilege gap assessment using AD ACL Scanner (free, GitHub) to export all ACLs on PHI directory trees and cross-reference against job-role authorization lists. Document findings in a structured spreadsheet mapping account → access level → business justification → gap flag. For the HIPAA breach risk assessment, use the HHS Security Risk Assessment Tool (free, provided by ONC/HHS) to score the four-factor breach risk analysis required under 45 CFR §164.402. Log retention gaps can be quantified by querying the oldest event timestamp in each Windows Event Log channel ('Get-WinEvent -LogName Security -Oldest -MaxEvents 1 | Select TimeCreated') to establish actual retention versus policy.

Evidence: Assemble the complete post-incident evidence package before the lessons-learned session: full timeline reconstruction from Security Event Log (4624, 4625, 4648, 4663, 4688, 4698, 7045) correlated with network flow logs covering the period from initial access through encryption trigger; inventory of all PHI data stores confirmed accessible during the intrusion window (EHR database tables, billing system directories, scanned insurance document repositories, SSN-containing flat files) to scope the HIPAA breach notification population under 45 CFR §164.400–414; ransomware note text and any threat actor communication preserving double-extortion claim details for law enforcement referral (FBI IC3) and HHS OCR notification; list of all exfiltration destination IPs/domains identified from network logs for submission to HHS and potential sharing via H-ISAC.

Detection Guidance

No confirmed IOCs are publicly available for these specific incidents. Detection should focus on behavioral patterns consistent with double-extortion ransomware. Monitor for: (1) mass file enumeration events across PHI data stores, high-volume read operations from a single account or process in short time windows; (2) large outbound data transfers to unfamiliar external IPs or cloud storage endpoints, particularly during off-hours; (3) service termination events targeting backup, AV, or database processes (T1489); (4) encryption activity producing high volumes of renamed or modified files in clinical document directories; (5) logins from unusual geolocations or outside business hours using valid credentials (T1078). Log sources: Windows Security Event Log (Event IDs 4624, 4625, 4648, 4672 for account anomalies; 7045 for new service installation), EDR process creation and network telemetry, and firewall/proxy logs for outbound volume spikes. Apply NIST AU-2 (Audit Events) and NIST SC-7 (Boundary Protection) controls. No confirmed file hashes, IPs, or domains are available from current source data.

Framework Mappings

MITRE-ATTACK

- **T1566** — Phishing
- **T1489** — Service Stop
- **T1083** — File and Directory Discovery
- **T1078** — Valid Accounts
- **T1041** — Exfiltration Over C2 Channel
- **T1657** — Financial Theft
- **T1486** — Data Encrypted for Impact

NIST-800-53R5

- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **CM-6** — Configuration Settings
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **AC-3** — Access Enforcement
- **IR-4** — Incident Handling
- **SC-13** — Cryptographic Protection

OWASP-TOP10-2021

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

CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.312(e)(1)** — Transmission Security

NIST-CSF-2

- **RS.MI-01** — Incidents are contained

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.5.34** — Privacy and protection of personal information
- **A.8.24** — Use of cryptography

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1566	Phishing	Initial-Access
T1489	Service Stop	Impact
T1083	File and Directory Discovery	Discovery
T1078	Valid Accounts	Defense-Evasion
T1041	Exfiltration Over C2 Channel	Exfiltration
T1657	Financial Theft	Impact
T1486	Data Encrypted for Impact	Impact

Sources

Source	URL	Tier
Ransomware Groups Claim Responsibility for Attacks on 3 ...	https://www.hipaajournal.com/ransomware-groups-claim-responsibility...	T3
Advanced Eye Surgery Center	https://www.caec.info/advanced-eye-surgery-center	T3
Tennessee Virginia and Utah Clinics Hit by Ransomware - LinkedIn	https://www.linkedin.com/posts/cyber-news-live_ransomware-groups-cl...	T3
East Atlanta Eye Surgery Center	https://eastatlantaeyeasc.com/	T3
Plastic and Reconstructive Surgery - Emory Healthcare	https://www.emoryhealthcare.org/centers-programs/plastic-and-recons...	T3

Generated 2026-06-12 07:02 UTC by TJS Security Command Center