INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-22 18:53 UTC

May 2026 Healthcare Data Breach Roundup: 9 HIPAA-Regulated Entities Affected Including TridentLocker Ransomware Incident

DATA BREACH | HIGH

SCC Item ID	SCC-DBR-2026-0137
Type	Data Breach
Severity	HIGH
Affected Products	University of Nebraska Medical Center (REDCap software), Singing River Health System, Tampa Bay Dental Implants & Prosthetics, Aligned Orthopedic Partners (AWS environment), Pivot Health (AWS environment), LHC Group, Mays Housecall Home Health, World Trade Center Health Program (TridentLocker ransomware)
Discovery Source	Gemini

Executive Summary

Nine HIPAA-regulated healthcare organizations reported data breaches in May 2026, exposing protected health information (PHI) across multiple attack surfaces including ransomware, cloud environment compromises, and a research data platform. The World Trade Center Health Program was struck by TridentLocker ransomware, which combines encryption with likely data exfiltration; Aligned Orthopedic Partners and Pivot Health suffered breaches within AWS-hosted environments. Regulatory exposure under HIPAA is certain for all nine entities, with breach notification obligations, OCR investigation risk, and potential civil monetary penalties across a broad set of covered entities and business associates.

Technical Analysis

This roundup covers nine separate breach events reported to HHS/OCR in May 2026. Attack surfaces span three distinct categories: (1) Research platform compromise, University of Nebraska Medical Center's REDCap instance was involved; REDCap is a web-based clinical data management system widely deployed in academic medical centers, often handling de-identified or limited-dataset PHI. No CVE was assigned to this incident; root cause is unconfirmed in available source data. (2) Cloud environment breaches, Aligned Orthopedic Partners and Pivot Health both reported breaches occurring within AWS environments. MITRE T1530 (Data from Cloud Storage Object) and T1078 (Valid Accounts) are mapped techniques, consistent with misconfigured S3 buckets, overly permissive IAM policies, or credential compromise. CWE-732 (Incorrect Permission Assignment for Critical Resource) and CWE-306 (Missing Authentication for Critical Function) are relevant weakness classifications. (3) Ransomware, World Trade Center Health Program was impacted by TridentLocker, a

ransomware variant. T1486 (Data Encrypted for Impact) and T1567 (Exfiltration Over Web Service) are mapped techniques, indicating potential double-extortion capability. CWE-284 (Improper Access Control) and CWE-312 (Cleartext Storage of Sensitive Information) are flagged weaknesses. Attribution confidence is medium per source metadata. Singing River Health System, Tampa Bay Dental Implants & Prosthetics, LHC Group, and Mays Housecall Home Health round out the nine entities; specific attack vectors for these four are not detailed in available source data. No CVSS scores are assigned; no CVE identifiers are associated with these incidents. Source quality score: 0.72 (T2 primary source, HIPAA Journal roundup format). Per-entity technical detail is limited; claims about specific attack vectors for the four undisclosed entities should not be inferred.

Action Checklist

1. Step 1: Containment, If you operate REDCap, isolate the instance from external access immediately and revoke all active API tokens and user sessions; audit who has accessed the system in the past 90 days. If PHI is stored in AWS S3 buckets or RDS instances, block public access at the bucket and VPC level now and rotate all IAM access keys and service account credentials (supports NIST AC-2, AC-3; CIS 6.2).
2. Step 2: Detection, For AWS environments, query CloudTrail for anomalous GetObject, ListBuckets, and AssumeRole events, especially from unfamiliar IP ranges or outside business hours; check S3 Access Analyzer for publicly accessible buckets containing PHI (MITRE T1530). For ransomware indicators: search endpoint logs for TridentLocker file extension patterns, unusual Volume Shadow Copy deletion commands (vssadmin delete shadows), and outbound HTTPS traffic to non-standard destinations consistent with T1567 exfiltration. For REDCap: review application and web server access logs for bulk data export events or API calls not associated with known research accounts (supports NIST AU-6, AU-12; CIS 8.2).
3. Step 3: Eradication, For cloud breaches: enforce least-privilege IAM policies across all AWS roles and users (NIST AC-6; CIS 5.4); remove all overly permissive S3 bucket policies; enable AWS Config rules for s3-bucket-public-read-prohibited and iam-no-inline-policy. For REDCap: apply all pending software updates from Vanderbilt's REDCap release channel; enforce MFA for all REDCap user accounts (NIST IA-2; CIS 6.3). For TridentLocker ransomware: reimage affected systems from verified clean backups; do not restore from snapshots taken after initial access; engage forensics before reconnecting to production network.
4. Step 4: Recovery, Validate PHI data integrity against pre-incident backups before restoring clinical or research operations. Re-enable AWS services incrementally with CloudTrail and GuardDuty fully active; confirm no persistence mechanisms remain via forensic persistence checks (startup folder analysis, registry audits, scheduled task verification). For ransomware recovery: restore from offline or immutable backups only; verify backup integrity with hash comparison before use. Conduct tabletop review of restored environment before returning to production (supports NIST CP-10, IR-4).
5. Step 5: Post-Incident, These incidents expose control gaps in cloud access governance (CWE-732, CWE-306), credential management (T1078), and backup/recovery for ransomware scenarios. Implement continuous monitoring per NIST AC-2 (Account Management) and IA-2 (Authentication) across all PHI-handling systems. Review and enforce NIST AC-2 (Account Management) and AC-6 (Least Privilege) for all cloud IAM roles. Conduct a HIPAA Security Rule risk analysis update covering cloud-hosted PHI per 45 CFR §164.308(a)(1), and document findings before OCR inquiry arrives.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to senior IR leadership, legal counsel, and HIPAA Privacy Officer immediately if TridentLocker exfiltration is confirmed (data leak site monitoring or C2 contact), if any AWS S3 bucket containing PHI was publicly accessible for a determinable period, or if the number of affected individuals at any single entity exceeds 500 (triggering HHS OCR notification within 60 days under 45 CFR §164.408).
Recovery Notes	Restore WTCHP clinical systems only from backups whose SHA-256 hash is verified against pre-incident manifests and whose snapshot timestamp predates the earliest confirmed TridentLocker indicator; monitor Windows Event ID 4688 and 7045 for 30 days post-restoration to detect any reinfection or residual persistence. For AWS-hosted PHI at Aligned Orthopedic and Pivot Health, maintain CloudTrail and GuardDuty in active monitoring mode for a minimum of 90 days post-recovery and review GuardDuty findings daily for credential reuse (T1078) or renewed enumeration activity. REDCap at UNMC should remain in restricted-access mode (no external API access) until Vanderbilt's REDCap security advisory is confirmed resolved and all user MFA enrollment is verified complete.
Forensic Artifacts	REDCap MySQL database table `redcap_log_event` at UNMC — contains timestamped records of every data export, API call, and user session; primary source for determining PHI scope and identifying unauthorized bulk exports tied to this breach. | AWS CloudTrail logs for S3 GetObject, ListBuckets, AssumeRole, and CreatePresignedUrl API events in the Aligned Orthopedic Partners and Pivot Health accounts — the definitive record of which IAM principals accessed PHI buckets, from which IPs, and at what volume, supporting both forensic scope determination and HIPAA breach notification. | Windows Volume Shadow Copy service logs and Security Event Log (Event ID 4688 filtered on vssadmin.exe and wmic.exe with shadow deletion arguments) on WTCHP endpoints — TridentLocker's VSS deletion is typically one of the last pre-encryption actions and timestamps this event to narrow the encryption start window. | TridentLocker ransom note files dropped in encrypted directories on WTCHP systems (typically named `README_TRIDENT.txt` or variant) and any recovered binary samples — ransom notes often contain variant-specific C2 onion addresses or victim IDs that enable threat intelligence cross-referencing and exfiltration confirmation via dark web leak site monitoring. | AWS IAM credential report (`aws iam get-credential-report`) and access key last-used metadata for all IAM users and roles in affected AWS accounts — establishes which credentials were active during the breach window and whether any keys were used from attacker-controlled IPs, which is required evidence for both eradication completeness and HIPAA risk analysis documentation.

Per-Action IR Details

Step 1: Containment — If you operate REDCap, isolate the instance from external access immediately and revoke all active API tokens and user sessions; audit who has accessed the system in the past 90 days. If PHI is stored in AWS S3 buckets or RDS instances, block public access at the bucket and VPC level now and rotate all IAM access keys and service account credentials (supports NIST AC-17, AC-3; CIS 6.2).

NIST Phase: Containment

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

Controls: NIST AC-3 (Access Enforcement), NIST AC-17 (Remote Access), NIST AC-2 (Account Management), CIS 6.2 (Establish an Access Revoking Process)

Compensating: For REDCap without enterprise tooling: disable external-facing Apache/nginx vhost immediately via `systemctl stop apache2` or equivalent, then dump active sessions from REDCap's `redcap_log_event` table filtering on `ts >= NOW() - INTERVAL 90 DAY` to enumerate recent user and API activity. For AWS without CSPM: run `aws s3api put-public-access-block --bucket --public-access-block-configuration BlockPublicAcls=true,IgnorePublicAcls=true,BlockPublicPolicy=true,RestrictPublicBuckets=true` for each PHI-holding bucket, then `aws iam list-access-keys --user-name ` and `aws iam delete-access-key` for all active keys on affected IAM principals. Use AWS CLI in a read-only audit role first to preserve pre-containment state.

Evidence: Before revoking REDCap tokens, export the full `redcap_log_event` table (MySQL) filtered to the past 90 days — this is your only record of which user accounts or API tokens accessed or exported PHI records at UNMC. Capture REDCap's `redcap_user_information` table to document all active accounts and last-login timestamps. For AWS: snapshot CloudTrail S3 bucket contents and export current IAM credential report via `aws iam generate-credential-report` and `aws iam get-credential-report` before any key rotation — rotation destroys the evidentiary link between the compromised key and its actions. Capture VPC Flow Logs for the 90-day window before changing security groups or NACLs at Aligned Orthopedic Partners and Pivot Health AWS environments.

Step 2: Detection — For AWS environments, query CloudTrail for anomalous GetObject, ListBuckets, and AssumeRole events, especially from unfamiliar IP ranges or outside business hours; check S3 Access Analyzer for publicly accessible buckets containing PHI (MITRE T1530). For ransomware indicators: search endpoint logs for TridentLocker file extension patterns, unusual Volume Shadow Copy deletion commands (vssadmin delete shadows), and outbound HTTPS traffic to non-standard destinations consistent with T1567 exfiltration. For REDCap: review application and web server access logs for bulk data export events or API calls not associated with known research accounts (supports NIST AU-6, AU-12; CIS 8.2).

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-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs), MITRE ATT&CK T1530 (Data from Cloud Storage), MITRE ATT&CK T1567 (Exfiltration Over Web Service), MITRE ATT&CK T1490 (Inhibit System Recovery)

Compensating: For AWS without a SIEM: use AWS CloudTrail Insights (free tier) to detect unusual API call volume, then run targeted Athena queries against CloudTrail logs — query: `SELECT userIdentity.arn, sourceIPAddress, eventName, eventTime FROM cloudtrail_logs WHERE eventName IN ('GetObject','ListBuckets','AssumeRole') AND eventTime > '2026-03-04' ORDER BY eventTime DESC`. For TridentLocker on Windows without EDR: deploy Sysmon with SwiftOnSecurity config and query Event ID 4688 (Process Creation) filtering on `vssadmin.exe` with `/delete` arguments and `wmic shadowcopy delete` via PowerShell: `Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4688 -and $_.Message -like '*vssadmin*delete*'}`. For REDCap bulk export detection: parse Apache access logs with `grep -E 'POST.*redcap.*export|GET.*redcap.*data' /var/log/apache2/access.log | awk '{print $1,$7,$NF}' | sort | uniq -c | sort -rn` to surface high-volume data access by IP.

Evidence: AWS CloudTrail logs showing S3 GetObject and ListBuckets API calls against PHI buckets at Aligned Orthopedic Partners and Pivot Health — specifically look for calls from EC2 instance metadata service (IMDS) credential abuse indicating T1552.005. REDCap application log at `/edocs/redcap_v*/logs/` and MySQL `redcap_log_event` table rows where `object_type = 'record'` and `action LIKE '%export%'` at UNMC. For TridentLocker at WTCHP: Windows Security Event Log Event ID 4688 showing `vssadmin.exe delete shadows /all /quiet` and Event ID 7045 (new service installed) which is a common TridentLocker persistence precursor. Windows Event ID 4663 (file access) on shares showing mass file rename events with TridentLocker-specific extension appended to filenames.

Step 3: Eradication — For cloud breaches: enforce least-privilege IAM policies across all AWS roles and users (NIST AC-6; CIS 5.4); remove all overly permissive S3 bucket policies; enable AWS Config rules for s3-bucket-public-read-prohibited and iam-no-inline-policy. For REDCap: apply all pending software updates from Vanderbilt's REDCap release channel; enforce MFA for all REDCap user accounts (NIST IA-2; CIS 6.3). For TridentLocker ransomware: reimage affected systems from verified clean backups; do not restore from snapshots taken after initial access; engage forensics before reconnecting to production network.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-6 (Least Privilege), NIST IA-2 (Identification and Authentication — Organizational Users), NIST SI-2 (Flaw Remediation), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: For REDCap MFA without enterprise IAM: enable REDCap's native two-factor authentication module (Settings > Security > Two-Factor Authentication) and enforce via `$enable_twofactor = 1` in `database.php`; enforce for all accounts with PHI data access permissions. For AWS least-privilege without CSPM: run `aws iam get-account-authorization-details > iam_baseline.json` to capture current state, then use the open-source tool `parliament` (pip install parliament) to lint all inline and managed policies and flag overly permissive actions. For TridentLocker eradication without enterprise EDR: before reimaging, run Volatility3 against a memory image (`vol.py -f memory.raw windows.pstree`) to identify injected processes and confirm ransomware process lineage; preserve this image as forensic evidence before wiping.

Evidence: Before reimaging TridentLocker-affected WTCHP systems: acquire full disk images using `dc3dd` or FTK Imager and capture RAM with WinPMEM — TridentLocker likely leaves decryption key material in memory during active encryption. Preserve the ransom note file (typically dropped in every encrypted directory) as it may contain TridentLocker variant identifiers and C2 contact information. For REDCap patching: document the currently installed REDCap version from `redcap_config` table (`SELECT value FROM redcap_config WHERE field_name = 'redcap_version'`) before applying updates to establish a vulnerability window. For AWS eradication: capture `aws iam get-account-authorization-details` output and all S3 bucket policy JSON (`aws s3api get-bucket-policy`) before modification to document the misconfiguration state for HIPAA breach documentation.

Step 4: Recovery — Validate PHI data integrity against pre-incident backups before restoring clinical or research operations. Re-enable AWS services incrementally with CloudTrail and GuardDuty fully active; confirm no persistence mechanisms remain via D3-SICA (System Init Config Analysis) and D3-SFA (System File Analysis). For ransomware recovery: restore from offline or immutable backups only; verify backup integrity with hash comparison before use. Conduct tabletop review of restored environment before returning to production (supports NIST CP-10, IR-4).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST CP-10 (System Recovery and Reconstitution), NIST IR-4 (Incident Handling), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: For backup integrity verification without enterprise backup tooling: generate SHA-256 hashes of backup archives before and after transfer using `sha256sum > backup.sha256` and compare against pre-incident hash manifests; reject any backup whose hash cannot be verified against a pre-incident record. For WTCHP ransomware recovery without immutable backup infrastructure: restore from offline tape or air-gapped media only — S3 versioning-enabled buckets with Object Lock (WORM) are acceptable if lock was enabled before TridentLocker initial access date. For AWS persistence checking without commercial tooling: use `aws lambda list-functions`, `aws events list-rules`, and `aws iam list-roles` to enumerate all potential persistence points re-established by an attacker; cross-reference against a known-good IaC baseline (Terraform state or CloudFormation templates) if available.

Evidence: Before restoring WTCHP clinical systems: verify that backup timestamps predate the earliest TridentLocker indicator of compromise — check Windows Event Log ID 4698 (scheduled task created) and registry key `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks` for attacker-created persistence tasks that may have been active before encryption began. For REDCap recovery at UNMC: run a row-count and checksum comparison between restored MySQL database and the last clean backup using `CHECKSUM TABLE redcap_data` to detect PHI record tampering or deletion. For AWS recovery at Aligned Orthopedic and Pivot Health: enable AWS Config conformance pack for HIPAA and run `aws configservice describe-compliance-by-config-rule` to validate that restored environment meets baseline before re-enabling clinical data flows.

Step 5: Post-Incident — These incidents expose control gaps in cloud access governance (CWE-732, CWE-306), credential management (T1078), and backup/recovery for ransomware scenarios. Implement continuous D3-LAM (Local Account Monitoring) and D3-MFA (Multi-factor Authentication) across all PHI-handling systems. Review and enforce NIST AC-2 (Account Management) and AC-6 (Least Privilege) for all cloud IAM roles. Conduct a HIPAA Security Rule risk analysis update covering cloud-hosted PHI per 45 CFR §164.308(a)(1), and document findings before OCR inquiry arrives.

NIST Phase: Post Incident

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

Controls: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), NIST IR-4 (Incident Handling), NIST RA-3 (Risk Assessment), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.5 (Require MFA for Administrative Access), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For continuous local account monitoring without SIEM: deploy osquery with the `users` and `last` tables on a 15-minute scheduled query (`SELECT username, uid, gid, directory, shell FROM users WHERE uid >= 1000`) on all PHI-handling Linux hosts; on Windows, use Sysmon Event ID 4720 (account created) and 4732 (account added to privileged group) forwarded to a central syslog server via Windows Event Forwarding at zero cost. For the HIPAA 45 CFR §164.308(a)(1) risk analysis update: use the free HHS Security Risk Assessment (SRA) Tool (available from healthit.gov) to document cloud-specific PHI risks introduced by AWS-hosted environments at Aligned Orthopedic and Pivot Health — this produces OCR-acceptable documentation. Schedule a 30-day post-incident review meeting with specific agenda items: TridentLocker initial access vector confirmation, REDCap patch cadence SLA, and AWS IAM policy review cycle.

Evidence: Compile a post-incident evidence package for HIPAA Breach Notification Rule (45 CFR §164.400-414) compliance: (1) CloudTrail export showing the full timeline of S3 access events for Aligned Orthopedic and Pivot Health environments, (2) REDCap `redcap_log_event` export showing which PHI records were accessed or exported at UNMC, (3) TridentLocker ransom note and any recovered C2 network IOCs from WTCHP memory forensics, (4) IAM credential report showing key age and last-used timestamps for all compromised AWS principals, (5) documented backup hash verification results confirming which restored systems can be certified as returning to a known-good state. All nine entities face a 60-day breach notification window to HHS OCR; this evidence package forms the factual basis for the required breach notification letters.

Detection Guidance

Three detection priorities for this incident cluster: (1) AWS cloud PHI exposure, Enable and review AWS S3 Access Analyzer findings for any bucket storing PHI. Query CloudTrail for s3:GetObject, s3:ListBucket, and iam:CreateAccessKey events originating from IPs outside your known infrastructure. Alert on AssumeRole events for roles with S3 read permissions to PHI buckets. NIST AU-6 and CIS 8.2 require this logging to be active. (2) TridentLocker ransomware, Hunt for: mass file rename events with unfamiliar extensions across file servers or clinical workstations; execution of cmd.exe or powershell.exe spawning vssadmin.exe with delete arguments; outbound encrypted traffic to non-categorized or newly registered domains, consistent with T1567 exfiltration prior to encryption. Check EDR telemetry for process injection or lateral movement via T1078 (valid account reuse). (3) REDCap anomalies, Review REDCap application logs for bulk record exports, API token generation outside normal researcher activity, or logins from IP addresses not associated with your institution's research network. Cross-reference with NIST AU-3 (audit record content) to confirm logs capture user identity, timestamp, and data accessed. Monitor CISA threat alerts, vendor threat intelligence (Malwarebytes Labs, CrowdStrike, Kaspersky), and ransomware-tracking forums for TridentLocker IOCs and file extension patterns as they are disclosed.

Framework Mappings

MITRE-ATTACK

- **T1190** — Exploit Public-Facing Application
- **T1530** — Data from Cloud Storage
- **T1078** — Valid Accounts
- **T1486** — Data Encrypted for Impact
- **T1567** — Exfiltration Over Web Service

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
- **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
- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **3.3** — Configure Data Access Control Lists
- **6.3** — Require MFA for Externally-Exposed Applications

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
- **CC6.3** — Authorizes, modifies, or removes access

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(6)(ii)** — Response and Reporting
- **164.312(e)(1)** — Transmission Security

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.8.24** — Use of cryptography
- **A.5.23** — Information security for use of cloud services

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1190	Exploit Public-Facing Application	Initial-Access
T1530	Data from Cloud Storage	Collection
T1078	Valid Accounts	Defense-Evasion
T1486	Data Encrypted for Impact	Impact
T1567	Exfiltration Over Web Service	Exfiltration

Sources

Source	URL	Tier
May 2026 Data Breach Round Up - The HIPAA Journal	https://www.hipaajournal.com/may-2026-data-breach-round-up/	T3
REDCap | Research Resources	https://www.unmc.edu/vcr/rito/software/redcap/index.html	T1
The REDCap Consortium: Building an International Community of ...	https://pmc.ncbi.nlm.nih.gov/articles/PMC7254481/	T1

Source	URL	Tier
Our Company | REDCap Cloud	https://www.redcapcloud.com/company/	T3
CodaMetrix — Code For Better, Contextual Coding Automation	https://www.codametrix.com/resources/codametrix-announces-40m-serie...	T3

Generated 2026-05-22 18:53 UTC by TJS Security Command Center