INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-14 06:52 UTC

OpenLoop Health confirms January 2026 Data breach affecting 716,000 individuals

DATA BREACH | HIGH

SCC Item ID	SCC-DBR-2026-0124
Type	Data Breach
Severity	HIGH
Affected Products	OpenLoop Health (telehealth infrastructure platform)
Published	2026-05-13
Discovery Source	Gemini

Executive Summary

OpenLoop Health, a telehealth infrastructure platform serving multiple telehealth operators, confirmed a data breach in January 2026 affecting approximately 716,000 individuals. The exposed data likely includes protected health information (PHI) and personally identifiable information (PII) processed on behalf of telehealth clients, triggering HIPAA breach notification obligations for OpenLoop and potentially its downstream partners. Business risk centers on regulatory enforcement, civil litigation, and third-party liability exposure for healthcare operators whose patient data flows through OpenLoop's infrastructure.

Technical Analysis

OpenLoop Health confirmed unauthorized access to systems containing patient and provider data in January 2026. No CVE has been assigned; this is a breach incident, not a disclosed software vulnerability. Applicable weakness classification is CWE-359 (Exposure of Private Personal Information to an Unauthorized Actor). MITRE ATT&CK techniques associated with the breach pattern include T1213 (Data from Information Repositories), T1078 (Valid Accounts), and T1530 (Data from Cloud Storage Object), suggesting potential credential misuse or misconfigured storage as contributing vectors, though no threat actor or specific attack method has been publicly attributed. Specific data categories compromised (names, dates of birth, SSNs, medical record numbers, insurance details) have not been fully disclosed in available public reporting as of this configuration date. No patch or CVE remediation applies; response focuses on access control review, third-party risk assessment, and HIPAA notification compliance. Reporting is limited to secondary news sources; organizations should monitor for official statements from OpenLoop Health directly or HHS OCR breach portal filings for complete confirmed scope.

Action Checklist

1. Containment: If OpenLoop Health is a third-party vendor or data processor in your environment, immediately review your Business Associate Agreement (BAA) and determine whether PHI or PII your organization holds was routed through OpenLoop systems. Request written confirmation from OpenLoop of which data sets were exposed and whether your patient population is included.
2. Detection: Query your data flow and vendor inventory logs for any integrations, API connections, or data sharing arrangements with OpenLoop Health. Review access logs for OpenLoop-connected systems for anomalous activity in the January 2026 timeframe. If OpenLoop processed data on your behalf, request their breach notification documentation and incident timeline.
3. Eradication: If your organization's data was confirmed in scope, rotate any shared API keys, service account credentials, or OAuth tokens used in OpenLoop integrations. Audit cloud storage buckets and information repositories (aligned with T1530, T1213) shared with or accessible by OpenLoop. Revoke and reissue credentials where shared access existed.
4. Recovery: Validate that PHI/PII data flows to OpenLoop have been suspended or secured pending full breach scope determination. Confirm your own HIPAA breach risk assessment is documented: if OpenLoop is your Business Associate and their breach exposed your patients' PHI, your organization may have independent notification obligations under 45 CFR 164.400-414. Engage legal counsel and your privacy officer.
5. Post-Incident: Review third-party risk management controls for healthcare infrastructure vendors: assess whether BAAs include breach notification SLAs, whether vendor security assessments were current, and whether PHI minimization practices limit future exposure. Map data sharing to the principle of least privilege across all telehealth infrastructure partners.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to executive leadership, legal counsel, and your HIPAA Privacy Officer if OpenLoop's breach notification confirms that your organization's patient PHI was included in the 716,000 affected individuals, triggering mandatory HHS OCR notification under 45 CFR §164.408 and individual notification under §164.404 within 60 days of breach discovery.
Recovery Notes	Before restoring any PHI data flows to OpenLoop or successor systems, obtain independent confirmation from OpenLoop that the breach vector has been fully remediated and that a third-party forensic investigation report is available for your review. Monitor your organization's own HIPAA audit logs and patient complaint channels for 90 days post-incident for signs of downstream misuse of exposed PHI, such as fraudulent telehealth claims or patient identity theft reports. Ensure your breach risk assessment documentation, notification decisions, and all vendor correspondence are archived for a minimum of 6 years per HIPAA §164.530(j) to support any future HHS OCR investigation.

Forensic Artifacts	API gateway and reverse proxy access logs (AWS API Gateway CloudTrail, nginx access.log, or Azure API Management diagnostic logs) covering October 2025–January 2026, filtered for outbound requests to OpenLoop Health domains and IP ranges — establishes data transfer volume and timing relative to the breach window | Identity provider OAuth token issuance logs (Okta System Log, Azure AD Sign-In logs) for the application registration associated with OpenLoop integrations, showing client ID, granted scopes, and token lifetimes — maps exactly which PHI data categories were accessible under each token | Cloud storage access logs (AWS S3 CloudTrail s3:GetObject and s3:ListBucket events, or Azure Blob Storage diagnostic logs) for buckets with OpenLoop IAM roles or cross-account trust policies — identifies what patient record files were retrieved and by which principal | EHR or FHIR server audit logs (Epic audit trail, Redox event logs, or HL7 message logs) capturing patient record queries and responses routed through OpenLoop-connected workflows — provides patient-level granularity needed for HIPAA breach notification scope determination | OpenLoop Health's written breach notification and forensic investigation timeline (requested under BAA obligations) — serves as the authoritative incident chronology for your own risk assessment, regulatory filing, and potential civil litigation defense

Per-Action IR Details

Containment — If OpenLoop Health is a third-party vendor or data processor in your environment, immediately review your Business Associate Agreement (BAA) and determine whether PHI or PII your organization holds was routed through OpenLoop systems. Request written confirmation from OpenLoop of which data sets were exposed and whether your patient population is included.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST IR-6 (Incident Reporting), NIST SA-9 (External System Services) — enforces contractual requirements on third-party providers including breach notification obligations, CIS 15.1 (Establish and Maintain an Inventory of Service Providers) — verify OpenLoop is inventoried with BAA linkage and data classification

Compensating: Maintain a vendor register in a spreadsheet with BAA file paths, data categories shared (PHI, PII), and a contact column for breach notification. Use grep or PowerShell (Select-String) against your integration config files and CI/CD environment variables to locate any references to OpenLoop endpoints (e.g., 'openloophealth.com', 'openloop-api') and flag those systems for immediate access suspension pending scope determination.

Evidence: Before suspending integrations, capture point-in-time snapshots of: (1) API gateway access logs showing all outbound requests to OpenLoop Health endpoints in the October 2025–January 2026 window; (2) your data mapping documentation or HL7/FHIR transaction logs showing which patient record sets were transmitted to OpenLoop; (3) BAA execution date and data processing addendum to establish scope of PHI categories covered; (4) any OpenLoop-issued confirmation emails, incident notices, or breach notification letters timestamped in January 2026.

Detection — Query your data flow and vendor inventory logs for any integrations, API connections, or data sharing arrangements with OpenLoop Health. Review access logs for OpenLoop-connected systems for anomalous activity in the January 2026 timeframe. If OpenLoop processed data on your behalf, request their breach notification documentation and incident timeline.

NIST Phase: Detection Analysis

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

Controls: NIST IR-5 (Incident Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs) — confirm logging was enabled on all systems with OpenLoop integrations during the January 2026 breach window

Compensating: Run the following PowerShell command against IIS or application logs to identify OpenLoop-bound traffic: Select-String -Path 'C:\inetpub\logs\LogFiles*' -Pattern 'openloophealth\.com' | Select-Object Filename,

LineNumber, Line. For Linux-based API servers: grep -rn 'openloophealth' /var/log/nginx/ --include='*.log'. Cross-reference your /etc/hosts, application config files, and .env files for OpenLoop API base URLs. Use osquery's 'process_open_sockets' and 'system_info' tables on integration hosts to confirm current or recent connectivity.

Evidence: Collect before analysis: (1) API gateway or reverse proxy logs (nginx, Apache, AWS API Gateway CloudTrail events) for all requests to OpenLoop-owned domains/IPs in the September 2025–January 2026 window; (2) OAuth 2.0 token issuance and refresh logs from your identity provider showing tokens scoped to OpenLoop integrations; (3) FHIR server or EHR audit logs (e.g., Epic MyChart, Redox event logs) capturing which patient records were pushed or pulled via OpenLoop-connected workflows; (4) DNS query logs from your resolver showing resolution frequency of OpenLoop Health domains, which can help establish the data transfer volume and timeline.

Eradication — If your organization's data was confirmed in scope, rotate any shared API keys, service account credentials, or OAuth tokens used in OpenLoop integrations. Audit cloud storage buckets and information repositories (aligned with T1530, T1213) shared with or accessible by OpenLoop. Revoke and reissue credentials where shared access existed.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management) — revoke OpenLoop-associated service accounts and shared credentials, NIST IA-5 (Authenticator Management) — enforce credential rotation for all API keys and OAuth tokens issued to OpenLoop integrations, NIST SI-7 (Software, Firmware, and Information Integrity) — verify integrity of data repositories accessible by OpenLoop after credential revocation, CIS 5.2 (Use Unique Passwords) — confirm API keys were not reused across other vendor integrations, MITRE ATT&CK T1530 (Data from Cloud Storage) — audit S3 buckets, Azure Blob containers, or GCS buckets with OpenLoop IAM roles or cross-account access policies, MITRE ATT&CK T1213 (Data from Information Repositories) — review shared SharePoint sites, Confluence spaces, or sFTP directories provisioned for OpenLoop data exchange

Compensating: Use AWS CLI to enumerate bucket policies and cross-account access: aws s3api get-bucket-policy --bucket and aws iam list-roles | grep -i openloop. For Azure: az role assignment list --all | grep -i openloop. Rotate API keys immediately via your secrets manager (HashiCorp Vault, AWS Secrets Manager, or manually in your developer portal) and document rotation timestamps as evidence. For OAuth tokens, query your IdP (Okta, Azure AD) to list and revoke all active tokens issued to the OpenLoop application registration: az ad app list --display-name 'OpenLoop' followed by az ad app credential reset.

Evidence: Before rotating credentials, capture: (1) a full export of all IAM roles, policies, and cross-account trust relationships referencing OpenLoop or their AWS/Azure account IDs — this establishes the blast radius; (2) cloud storage access logs (AWS S3 server access logs or CloudTrail s3:GetObject events) showing what data OpenLoop accounts retrieved from your buckets and when; (3) OAuth token issuance logs from your IdP showing all tokens granted to the OpenLoop application client ID, including scopes requested — this maps exactly what PHI data types were accessible; (4) any shared sFTP or SFTP audit logs showing file transfer names and sizes, which can help quantify the volume of patient records potentially exposed.

Recovery — Validate that PHI/PII data flows to OpenLoop have been suspended or secured pending full breach scope determination. Confirm your own HIPAA breach risk assessment is documented: if OpenLoop is your Business Associate and their breach exposed your patients' PHI, your organization may have independent notification obligations under 45 CFR 164.400-414. Engage legal counsel and your privacy officer.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan) — verify your IR plan addresses Business Associate breach scenarios and HIPAA notification timelines, NIST IR-6 (Incident Reporting) — document breach risk assessment findings and notification decisions with timestamps, NIST AU-11 (Audit Record Retention) — retain all breach investigation records for a minimum of 6 years per HIPAA §164.530(j), CIS 3.4 (Enforce Data Retention) — ensure PHI records relevant to the breach are preserved and not purged during recovery, CIS 7.2 (Establish and Maintain a Remediation Process) — track breach risk assessment completion and notification decisions

as formal remediation milestones

Compensating: Document your HIPAA breach risk assessment using the HHS four-factor test (nature of PHI, unauthorized persons involved, whether PHI was acquired/viewed, mitigation extent) in a structured spreadsheet. Track notification deadlines: HIPAA requires individual notification within 60 days of breach discovery (45 CFR §164.404), and HHS notification within the same window for breaches affecting 500+ individuals. Use a shared document with version history (Google Docs, SharePoint) to maintain a defensible audit trail without a GRC platform. Assign a named owner for each open item with a due date.

Evidence: Before resuming any OpenLoop data flows: (1) obtain and retain OpenLoop's written breach notification and incident timeline — this is both regulatory evidence and establishes when your 60-day HIPAA clock started; (2) document your breach risk assessment conclusion (reportable or not reportable) with the date, analyst name, and four-factor analysis — HHS OCR expects this to be producible on demand; (3) capture the current state of your PHI data flow diagrams showing the OpenLoop integration path, marked as suspended, to demonstrate containment; (4) retain any legal hold notices issued internally covering communications about the OpenLoop breach, as these will be discoverable in any OCR investigation or civil litigation.

Post-Incident — Review third-party risk management controls for healthcare infrastructure vendors: assess whether BAAs include breach notification SLAs, whether vendor security assessments were current, and whether PHI minimization practices limit future exposure. Map data sharing to the principle of least privilege across all telehealth infrastructure partners.

NIST Phase: Post Incident

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

Controls: NIST IR-4 (Incident Handling) — incorporate lessons learned from OpenLoop breach into updated IR playbooks for Business Associate breach scenarios, NIST SA-9 (External System Services) — strengthen contractual requirements for telehealth infrastructure vendors to include breach notification SLAs of 72 hours or less, NIST RA-3 (Risk Assessment) — conduct updated vendor risk assessments for all telehealth infrastructure partners using OpenLoop breach as a trigger event, NIST AC-6 (Least Privilege) — enforce PHI minimization and least-privilege access across all telehealth data sharing integrations, NIST SI-12 (Information Management and Retention) — implement data minimization controls so that only the minimum necessary PHI is shared with telehealth infrastructure vendors, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — extend vulnerability management scope to include third-party SaaS and API-connected telehealth platforms, CIS 15.2 (Establish and Maintain a Service Provider Management Policy) — update policy to require annual security assessments and breach notification SLAs for all Business Associates handling PHI

Compensating: Conduct a tabletop exercise specifically simulating a repeat Business Associate breach at another telehealth infrastructure vendor — document gaps discovered. Build a vendor risk tier list in a spreadsheet ranking all BAAs by PHI volume and integration depth, then prioritize security questionnaire outreach (use the SIG Lite or CAIQ as a free baseline). Update BAA templates to require: (1) breach notification within 24–72 hours of discovery, (2) annual SOC 2 Type II or HITRUST report sharing, and (3) PHI data deletion certification upon contract termination. These are legal and administrative controls achievable by a 2-person privacy/security team without additional tooling.

Evidence: For lessons-learned documentation: (1) compile a complete vendor inventory audit showing all current Business Associates with PHI access, their data categories, integration type, and last security assessment date — the OpenLoop incident likely revealed gaps in this inventory; (2) collect BAA documents for all telehealth infrastructure partners and compare breach notification SLA language — document which BAAs lack notification timelines as a remediation finding; (3) produce a data flow map showing PHI minimization status for each integration (what fields are shared, whether de-identification or tokenization is applied) — this becomes the baseline for least-privilege remediation tracking.

Detection Guidance

No IOCs have been publicly disclosed for this incident. Detection focus should center on third-party exposure assessment rather than network-based indicators. Steps: (1) Audit vendor inventory and data flow

documentation for any OpenLoop Health integration. (2) Review API gateway and data transfer logs for connections to OpenLoop endpoints in the January 2026 window. (3) If your organization uses a SIEM, search for outbound data transfers to OpenLoop IP ranges or domains during Q4 2025 through January 2026. (4) For cloud environments, review CloudTrail, GCP Audit Logs, or Azure Monitor for access events on shared storage objects or repositories connected to OpenLoop. (5) Monitor HHS Office for Civil Rights (OCR) breach portal for the official OpenLoop filing, which will contain confirmed data categories and affected population details. Refer to HHS.gov/HIPAA for current breach notification portal information.

Framework Mappings

MITRE-ATTACK

- **T1213** — Data from Information Repositories
- **T1078** — Valid Accounts
- **T1530** — Data from Cloud Storage

NIST-800-53R5

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

ISO-27001-2022

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

HIPAA-SECURITY

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

SOC2-TSC

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

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1213	Data from Information Repositories	Collection
T1078	Valid Accounts	Defense-Evasion
T1530	Data from Cloud Storage	Collection

Sources

Source	URL	Tier
716000 Impacted by OpenLoop Health Data Breach	https://www.securityweek.com/716000-impacted-by-openloop-health-dat...	T3
OpenLoop Health Data Breach Affects 716000 Individuals	https://www.hipaajournal.com/openloop-health-data-breach/	T3
OpenLoop Health Faces Major Data Breach Affecting ...	https://www.reddit.com/r/pwnhub/comments/1s32gd5/openloop_health_fa.. .	T3
OpenLoop Health Data Breach	https://www.almeidalawgroup.com/data-breach-news/openloop-health-da...	T3
Gil Vidals' Post	https://www.linkedin.com/posts/gil-vidals_telehealth-platform-provi...	T3

Generated 2026-05-14 06:52 UTC by TJS Security Command Center