INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-05 13:57 UTC

ShinyHunters Leaks 234 GB of DentaQuest Data Exposing 2.6M Accounts Including Government IDs and Health Records

DATA BREACH | HIGH | CVSS 7.5

SCC Item ID	SCC-DBR-2026-0150
Type	Data Breach
Severity	HIGH
CVSS Base Score	7.5
Affected Products	DentaQuest (Sun Life subsidiary), dental benefits administration platform serving U.S. Medicaid and Medicare programs
Published	2026-06-04T14:36:27
Discovery Source	Rss

Executive Summary

ShinyHunters publicly released 234 GB of data exfiltrated from DentaQuest, a Sun Life subsidiary administering dental benefits for U.S. Medicaid and Medicare programs, exposing approximately 2.6 million accounts containing government-issued IDs, health insurance records, and dates of birth. The data is actively circulating and available for download, meaning downstream exploitation for identity fraud, benefits fraud, and targeted phishing is immediate rather than theoretical. Organizations that process, exchange, or rely on DentaQuest eligibility data should treat this as an active incident requiring immediate third-party risk assessment and beneficiary notification review.

Technical Analysis

ShinyHunters exfiltrated and publicly leaked 234 GB from DentaQuest's systems following failed extortion negotiations. No CVE has been assigned; this is an organizational breach rather than a discrete software vulnerability. Contributing weaknesses identified are CWE-284 (Improper Access Control), CWE-522 (Insufficiently Protected Credentials), and CWE-200 (Exposure of Sensitive Information to an Unauthorized Actor). MITRE ATT&CK techniques observed or inferred include T1078 (Valid Accounts) for initial access, T1530 (Data from Cloud Storage Object) for collection, T1567 (Exfiltration Over Web Service) for exfiltration, T1657 (Financial Theft) as a likely objective, and T1486 (Data Encrypted for Impact) as a secondary extortion lever. The exposed dataset includes government-issued identification documents, health insurance data, and dates of birth, data categories that cannot be revoked or rotated. Patch status is not applicable; remediation

requires access control remediation, credential rotation, and breach notification at the organizational level. CVSS base score is reported at 7.5 (High) by the source; given the public availability of the full dataset, sensitivity of exposed data categories, and vulnerability of the affected population (Medicaid and Medicare beneficiaries), a qualitative Critical assessment is warranted.

Action Checklist

1. Containment, Determine immediately whether your organization exchanges eligibility, enrollment, or claims data with DentaQuest via EDI feeds, API integrations, or shared portals; suspend automated data flows pending DentaQuest's formal breach notification and until the access vector is confirmed contained. Reference NIST AC-20 (Use of External Systems) for third-party connection controls.
2. Detection, Query your SIEM and identity logs for any accounts or service principals used in DentaQuest integrations over the past 90 days; review for anomalous authentication patterns (T1078, Valid Accounts) and unusual outbound data transfers to web services (T1567). Enable local account monitoring on accounts with DentaQuest portal access. Per NIST AU-6, review audit records for indicators of unauthorized access to stored beneficiary data.
3. Eradication, Rotate all credentials used for DentaQuest API connections, portal logins, and EDI interchange accounts. Enforce MFA on any remaining external-facing access points tied to DentaQuest or benefits administration workflows per CIS 6.3 (Require MFA for Externally-Exposed Applications). Apply NIST AC-3 (Access Enforcement) and AC-6 (Least Privilege) reviews to any shared data repositories containing beneficiary records.
4. Recovery, Validate that all DentaQuest-connected service accounts have been re-provisioned with new credentials and reduced permissions. Confirm audit logging is active and forwarding per NIST AU-2 (Event Logging) and CIS 8.2 (Collect Audit Logs). Monitor for beneficiary-targeted phishing campaigns and benefits fraud attempts, alert your fraud operations team to elevated risk for the affected population. Verify data access control lists on any locally stored beneficiary data per CIS 3.3 (Configure Data Access Control Lists).
5. Post-Incident, Conduct a formal third-party risk review of all vendors handling Medicaid and Medicare beneficiary data; map controls against NIST AC-20 (Use of External Systems) and NIST AC-4 (Information Flow Enforcement). Document control gaps exposed by this breach, specifically, the absence of credential hardening and insufficient access segmentation (NIST AC-5, Separation of Duties), and incorporate findings into your next GRC review cycle. Confirm HIPAA breach notification obligations have been assessed by your privacy and legal teams.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to legal, privacy officer, and executive leadership if your organization holds or received any of the approximately 2.6 million affected records containing government-issued IDs or health insurance data, as HIPAA breach notification obligations under 45 CFR §164.400 and potential CMS reporting requirements for Medicaid/Medicare program data may be triggered regardless of whether your organization was the direct breach victim.

Recovery Notes	Restoration of EDI and API data flows to DentaQuest should not resume until DentaQuest provides written confirmation that the access vector has been identified and remediated, and until your organization has independently verified that new credentials are in place and MFA is enforced on all portal access points. Given that ShinyHunters' leaked data is actively circulating and downloadable, elevated fraud monitoring for the affected beneficiary population — specifically anomalous claims submissions matching leaked member IDs and dates of birth — should remain active for a minimum of 12 months. Conduct a full review of all other Sun Life subsidiary integrations as lateral exposure within the parent organization's environment cannot be ruled out without DentaQuest's forensic findings.
Forensic Artifacts	EDI transaction logs (270/271 eligibility, 834 enrollment files) transmitted to/from DentaQuest SFTP endpoints — file transfer timestamps, sender/receiver ISA header identifiers, and record counts per transmission establish the data exposure window and volume | Firewall and proxy egress logs showing outbound data transfer volume to DentaQuest portal domains and IP ranges over the 90 days preceding breach disclosure — a sustained or spiked outbound byte count is consistent with ShinyHunters' 234 GB exfiltration pattern | Identity provider sign-in logs (Azure AD, Okta, or on-prem AD Event ID 4624/4648) for service accounts and portal user accounts tied to DentaQuest access — unusual authentication times, source IPs, or access from unfamiliar geographic locations indicate potential credential compromise upstream at DentaQuest | Local beneficiary data extract files stored on integration servers (common paths: /data/eligibility/, C:\EDI\Outbound\, or mapped network shares) — file last-accessed timestamps and ACL audit logs (Windows Event ID 4663) reveal whether locally cached copies of PHI were accessed beyond normal processing workflows | Browser and application session logs on workstations used to access the DentaQuest benefits administration portal — specifically saved session cookies, browser history, and any downloaded reports containing member records, which would represent locally held copies of the leaked dataset subject to independent HIPAA scoping

Per-Action IR Details

Containment — Determine immediately whether your organization exchanges eligibility, enrollment, or claims data with DentaQuest via EDI feeds, API integrations, or shared portals; suspend automated data flows pending DentaQuest's formal breach notification and until the access vector is confirmed contained. Reference NIST AC-20 (Use of External Systems) for third-party connection controls.

NIST Phase: Containment

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

Controls: NIST AC-20 (Use Of External Systems), NIST AC-4 (Information Flow Enforcement)

Compensating: Run `netstat -anb` or `ss -tulnp` on systems hosting EDI translation software (e.g., OpenEDI, TrueCommerce) to enumerate active outbound connections to DentaQuest endpoints. Block DentaQuest IP ranges and SFTP hostnames at the perimeter firewall using an ACL rule — document with timestamp. For API connections, revoke or null-route the OAuth token or API key immediately by setting it to an invalid value in the local config file and restarting the integration service.

Evidence: Before suspending feeds, capture: (1) EDI transaction logs showing 270/271 eligibility and 834 enrollment file transmissions to/from DentaQuest SFTP endpoints for the past 90 days — preserve originals in a read-only archive; (2) firewall/proxy logs showing outbound connections to DentaQuest portal domains and IP ranges; (3) API gateway access logs recording all requests/responses exchanged with DentaQuest REST or SOAP endpoints, including HTTP status codes, payload sizes, and timestamps; (4) a snapshot of the current integration configuration files (connection strings, credential stores, scheduled task definitions) before any changes are made.

Detection — Query your SIEM and identity logs for any accounts or service principals used in DentaQuest integrations over the past 90 days; review for anomalous authentication patterns (T1078 — Valid Accounts)

and unusual outbound data transfers to web services (T1567). Enable D3-LAM (Local Account Monitoring) on accounts with DentaQuest portal access. Per NIST AU-6, review audit records for indicators of unauthorized access to stored beneficiary data.

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-2 (Event Logging), NIST AU-12 (Audit Record Generation), NIST AC-2 (Account Management)

Compensating: Without a SIEM, use PowerShell to extract relevant Windows Security Event Log entries: `Get-WinEvent -LogName Security | Where-Object {$_.Id -in @(4624,4625,4648,4768,4769,4776) -and $_.TimeCreated -gt (Get-Date).AddDays(-90)} | Export-Csv dentaquest_auth_review.csv`. Cross-reference service account names against the DentaQuest integration config. For Linux-based EDI or API servers, run `grep -E '(dentaquest|sftp|api\.sun)' /var/log/auth.log /var/log/syslog` and review cron job history with `grep CRON /var/log/syslog`. Deploy Sysmon (config: SwiftOnSecurity baseline) on integration hosts and filter Event ID 3 (Network Connection) for outbound connections to DentaQuest IP ranges.

Evidence: Collect before analysis: (1) Windows Security Event Log — Event ID 4624 (successful logon) and 4648 (explicit credential logon) for service accounts tied to DentaQuest SFTP or portal sessions; (2) Event ID 4663 (object access) on directories storing local copies of 834/270/271 EDI files or beneficiary extracts; (3) Linux auth.log entries for SSH sessions from integration servers to DentaQuest SFTP hosts; (4) Proxy or DNS logs showing volume and frequency of outbound HTTP/HTTPS requests to DentaQuest portal domains — a spike in data volume transferred outbound is a key indicator of T1567 exfiltration; (5) Azure AD or Okta sign-in logs for service principals or federated accounts used to authenticate to DentaQuest's web portal.

Eradication — Rotate all credentials used for DentaQuest API connections, portal logins, and EDI interchange accounts (D3-CRO — Credential Rotation). Enforce MFA on any remaining external-facing access points tied to DentaQuest or benefits administration workflows per CIS 6.3 (Require MFA for Externally-Exposed Applications) and D3-MFA. Apply NIST AC-3 (Access Enforcement) and AC-6 (Least Privilege) reviews to any shared data repositories containing beneficiary records.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-3 (Access Enforcement), NIST AC-6 (Least Privilege), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), CIS 5.2 (Use Unique Passwords), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Generate new unique SFTP keypairs using `ssh-keygen -t ed25519 -C 'dentaquest-integration-[date]'` and submit the new public key to DentaQuest for registration before removing the old one. For API keys stored in config files or environment variables, update in-place and restart the integration service — then verify the old key is rejected by DentaQuest's API with a test call. For portal accounts, use the browser's built-in password manager audit or KeePass to confirm no credential reuse across other benefits portals. Enable TOTP-based MFA (e.g., Google Authenticator or Authy) on any portal accounts that support it.

Evidence: Before rotating credentials, document: (1) the full list of service accounts, API keys, SFTP keypairs, and portal usernames used in DentaQuest integrations — extracted from password vaults, config files, and scheduled task definitions; (2) the last-used timestamps for each credential from identity provider logs (Azure AD sign-in logs, local /etc/passwd last login, or Windows Event ID 4624 filtered by account name); (3) a before-snapshot of ACLs on file shares or databases storing local beneficiary data extracts — use `icacls /save acl_before.txt` on Windows or `getfacl -R > acl_before.txt` on Linux — to confirm over-permissioned access that will be tightened.

Recovery — Validate that all DentaQuest-connected service accounts have been re-provisioned with new credentials and reduced permissions. Confirm audit logging is active and forwarding per NIST AU-2 (Event Logging) and CIS 8.2 (Collect Audit Logs). Monitor for beneficiary-targeted phishing campaigns and benefits fraud attempts — alert your fraud operations team to elevated risk for the affected population. Verify data access control lists on any locally stored beneficiary data per CIS 3.3 (Configure Data Access Control Lists).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 8.2 (Collect Audit Logs), CIS 3.3 (Configure Data Access Control Lists), NIST AC-2 (Account Management)

Compensating: Validate re-provisioned accounts using `net user /domain` or `id ` to confirm group membership is limited to required access only. Verify Sysmon and Windows Event Forwarding are active on integration hosts by checking the Sysmon service status with `Get-Service Sysmon64` and confirming events are appearing in the forwarding subscription. For phishing monitoring, configure a free Canary Token (canarytokens.org) embedded in a local beneficiary data file — any unauthorized open will generate an alert. Brief fraud operations with a specific indicator list: claims submitted for the approximately 2.6 million affected members using credentials matching the leaked government IDs and dates of birth.

Evidence: Before restoring automated data flows: (1) confirm new SFTP key fingerprints match what DentaQuest has on record — request written confirmation from their technical contact; (2) run a test 270 eligibility transaction and verify only the new credentials authenticate successfully, with the old key/password rejected; (3) pull a current ACL report on beneficiary data repositories and compare against the pre-rotation snapshot to confirm permissions were actually reduced; (4) verify audit log forwarding by injecting a test event (e.g., intentional failed login) and confirming it appears in the central log store within the expected latency window.

Post-Incident — Conduct a formal third-party risk review of all vendors handling Medicaid and Medicare beneficiary data; map controls against NIST AC-20 (Use of External Systems) and NIST AC-4 (Information Flow Enforcement). Document control gaps exposed by this breach — specifically, the absence of credential hardening (D3-CH) and insufficient access segmentation (NIST AC-5, Separation of Duties) — and incorporate findings into your next GRC review cycle. Confirm HIPAA breach notification obligations have been assessed by your privacy and legal teams.

NIST Phase: Post Incident

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

Controls: NIST AC-20 (Use Of External Systems), NIST AC-4 (Information Flow Enforcement), NIST AC-5 (Separation Of Duties), 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), CIS 3.2 (Establish and Maintain a Data Inventory)

Compensating: Build a vendor data flow inventory using a simple spreadsheet: list every third-party benefits administrator (like DentaQuest) with columns for data elements exchanged (PHI, government IDs, enrollment data), transmission method (EDI/SFTP/API), authentication mechanism, MFA status, and last credential rotation date. Use this as your standing third-party risk register reviewed quarterly. For HIPAA breach notification assessment, use HHS's free Breach Risk Assessment Tool guidance at hhs.gov/hipaa/for-professionals to document whether the exposure of the 2.6M records triggers the 60-day notification clock under 45 CFR §164.412 — flag this immediately for your privacy officer even if your organization was not the breached party but received or holds the affected data.

Evidence: Preserve for post-incident documentation and potential regulatory inquiry: (1) full 90-day audit log archive from all DentaQuest integration points — retain per NIST AU-11 for a minimum period consistent with HIPAA's 6-year retention requirement for PHI-related records; (2) the complete inventory of data elements your organization received from or transmitted to DentaQuest, with record counts and date ranges, to scope any secondary HIPAA breach notification obligation; (3) written confirmation from DentaQuest's breach notification (once issued) of the confirmed attack vector and timeline, to close the gap in your own incident timeline; (4) the before/after ACL snapshots and credential rotation records as evidence of remediation actions taken, timestamped, for potential HHS Office for Civil Rights inquiry.

Detection Guidance

No public IOCs (IPs, domains, hashes) have been confirmed for the DentaQuest breach at this time. Detection focus should be on behavioral and data exposure indicators. Query identity and access logs for service

accounts or user accounts with DentaQuest portal or API access, look for off-hours authentication, logins from unfamiliar IP ranges, or bulk data queries in the 30-90 days preceding disclosure. In data loss prevention (DLP) tools, search for outbound transfers of health insurance identifiers, government ID numbers, or date-of-birth fields in large volumes. Cross-reference with T1530 (Data from Cloud Storage Object) hunting hypotheses if DentaQuest data was stored in cloud object storage accessible via your integration. Apply system file analysis to any local systems storing replicated beneficiary records, look for unauthorized modification or access to files containing PII. For organizations receiving DentaQuest eligibility feeds, audit all inbound data handling pipelines for signs of data tampering or unexpected record counts, which could indicate downstream manipulation of the leaked dataset. No CISA KEV entry exists for this incident.

Framework Mappings

MITRE-ATTACK

- **T1585** — Establish Accounts
- **T1078** — Valid Accounts
- **T1586** — Compromise Accounts
- **T1657** — Financial Theft
- **T1530** — Data from Cloud Storage
- **T1486** — Data Encrypted for Impact
- **T1566** — Phishing
- **T1567** — Exfiltration Over Web Service

NIST-800-53R5

- **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
- **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
- **AC-3** — Access Enforcement
- **SC-28** — Protection of Information at Rest

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control
- **A04:2021** — Insecure Design

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

CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **5.2** — Use Unique Passwords
- **6.3** — Require MFA for Externally-Exposed Applications
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

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

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.308(a)(5)(ii)(D)** — Password Management
- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(5)(i)** — Security Awareness and Training
- **164.308(a)(6)(ii)** — Response and Reporting

ISO-27001-2022

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1585	Establish Accounts	Resource-Development
T1078	Valid Accounts	Defense-Evasion
T1586	Compromise Accounts	Resource-Development
T1657	Financial Theft	Impact
T1530	Data from Cloud Storage	Collection
T1486	Data Encrypted for Impact	Impact
T1566	Phishing	Initial-Access
T1567	Exfiltration Over Web Service	Exfiltration

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/dentaquest-data-brea...	T3
	https://www.bleepingcomputer.com/news/security/data-breach-at-frenc...	T3
Sun Life Completes Acquisition of DentaQuest	https://www.dentaquest.com/en/news-and-resources/news-events/news-r...	T3
Sun Life to acquire DentaQuest, a leader in dental benefits in the ...	https://www.sunlife.com/en/newsroom/news-releases/announcement/sun-.. .	T3
Sun Life completes acquisition of DentaQuest - PR Newswire	https://www.prnewswire.com/news-releases/sun-life-completes-acquisi...	T3

Generated 2026-06-05 13:57 UTC by TJS Security Command Center