INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:43 UTC

# Conduent Third-Party Data Breach Impacts Elevance Health / Anthem Members

DATA BREACH | HIGH

| | |
|---|---|
| SCC Item ID | SCC-DBR-2026-0005 |
| Type | Data Breach |
| Severity | HIGH |
| Affected Products | Elevance Health (Anthem) member data; Conduent Business Services third-party print, mail, and back-office systems |
| Published | 2 weeks ago |

## Executive Summary

Conduent Business Services, a third-party vendor handling print, mail, and back-office operations for Elevance Health (Anthem), suffered a data breach that exposed personal information belonging to Elevance Health plan members. The breach originated at the vendor layer, meaning Elevance Health's own infrastructure was not directly compromised, but member data processed by Conduent was exposed. Business risk centers on potential HIPAA liability, member notification obligations, and reputational harm tied to a downstream vendor the organization does not directly control.

## Technical Analysis

This incident reflects a third-party supply chain exposure pattern. Conduent, operating as a business associate under HIPAA definitions, processed PHI and PII on behalf of Elevance Health subsidiaries including Anthem. The attack surface resided outside Elevance Health's direct security perimeter, within Conduent's print, mail, and back-office systems. Relevant CWE mapping: CWE-359 (Exposure of Private Personal Information to an Unauthorized Actor). MITRE ATT&CK techniques associated with this pattern include T1199 (Trusted Relationship, exploitation of third-party access), T1078 (Valid Accounts, likely used for lateral movement or initial access within the vendor environment), and T1530 (Data from Cloud Storage, possible exfiltration vector depending on Conduent's infrastructure). No CVE identifier is assigned; this is a data exposure incident rather than a software vulnerability. Specific data elements exposed and total affected population have not been confirmed in available source material. CVSS scoring is not applicable. Note: Source URLs provided in the item data reference the 2015 Anthem breach, not this Conduent third-party incident specifically. Content above is based on the incident description and established third-party breach patterns; direct source verification for this specific Conduent event was not possible from the supplied URLs.

## Action Checklist

1. Step 1, Immediate: Confirm your organization's contractual and data-sharing relationship with Conduent; determine whether your member or patient data flows through Conduent's print, mail, or back-office systems.
2. Step 2, Detection: Review data transfer and access logs at integration points between your environment and Conduent; flag any anomalous outbound transfers from business associate connections in the relevant timeframe.
3. Step 3, Assessment: Inventory all PHI and PII categories transmitted to or processed by Conduent on your behalf; estimate affected population size to support HIPAA breach notification threshold analysis.
4. Step 4, Communication: Engage legal and compliance to assess HIPAA breach notification obligations (60-day window to HHS, individual notification requirements); prepare member-facing communication if notification threshold is met; notify your cyber insurer.
5. Step 5, Long-term: Conduct a formal third-party risk review of all business associates handling PHI or PII; verify Business Associate Agreements (BAAs) include security incident notification SLAs; assess whether vendor security controls meet NIST SP 800-66r2 or equivalent standards.

## IR / Forensic Enrichment

| | |
|---|---|
| **Triage Priority** | IMMEDIATE |
| **Escalation Criteria** | Escalate to executive leadership and external forensic IR firm immediately if: (1) affected population exceeds 500 members (mandatory HHS notification triggers state AG notification requirements in most jurisdictions); (2) legal/compliance cannot rule out unauthorized access to SSNs or financial account data; (3) Conduent breach notification is incomplete or does not provide timeline/scope details within 48 hours. |
| **Recovery Notes** | Post-containment recovery focuses on three actions: (1) amend all BAAs with mandatory incident notification SLAs (24-hour discovery notice) and annual security assessment rights; (2) implement compensating controls for any vendor lacking encryption or robust access controls (e.g., redact SSNs from print-ready files, use encrypted file transfer instead of unencrypted SFTP); (3) establish quarterly third-party risk review cadence to monitor vendor security posture and contract compliance. Document all remediation actions in your Vendor Risk Register for audit evidence. |
| **Forensic Artifacts** | Firewall/proxy egress logs covering suspected breach window ±90 days (network indicators of data exfiltration) \| Database audit/transaction logs showing data exports to Conduent accounts or SFTP endpoints (data access patterns and volumes) \| Email gateway logs for large file transfers or encrypted attachments sent to Conduent addresses (lateral data movement detection) \| IAM/access control logs showing permission grants, role assignments, and service account activity for Conduent-related integrations (privilege escalation or over-provisioning) \| Conduent incident response report or breach notification letter (external source of truth for scope, timeline, and forensic findings) |

### Per-Action IR Details

**Step 1, Immediate: Confirm your organization's contractual and data-sharing relationship with Conduent; determine whether your member or patient data flows through Conduent's print, mail, or back-office systems.**

**NIST Phase:** Preparation

**Reference:** NIST 800-61r3 §2.1 (Organization Preparation)

**Controls:** NIST 800-53 SA-9 (Third-Party System Services), CIS 6.6 (Manage Access to Assets)

**Compensating:** Pull a Business Associate list from procurement or legal files; cross-reference against your system architecture diagrams. Query your CMDB (or maintain a spreadsheet) for each vendor's ingestion points. If no CMDB exists, interview data stewards for each business unit (claims, enrollment, mail production) to identify Conduent touchpoints. Document in a simple table: vendor name, data types, ingestion method, owner, contract date.

**Evidence:** Capture contractual metadata (BA agreement signature dates, amendment dates, scope of services, data retention clauses) before analysis begins; preserve email threads between your procurement and Conduent contacts that reference data types, volumes, or transmission methods. Document current system access privileges granted to Conduent staff in your identity management system. Screenshot or export any vendor system access logs showing Conduent logins or API calls within the past 12 months.

**Step 2, Detection: Review data transfer and access logs at integration points between your environment and Conduent; flag any anomalous outbound transfers from business associate connections in the relevant timeframe.**

**NIST Phase:** Detection Analysis

**Reference:** NIST 800-61r3 §3.1 (Detection and Analysis)

**Controls:** NIST 800-53 SI-4 (System Monitoring), NIST 800-53 AU-12 (Audit Generation), CIS 8.2 (Collect Audit Logs)

**Compensating:** Without a SIEM, export firewall or proxy logs for outbound connections to Conduent's IP ranges (obtain their IP CIDR blocks from their security team or Whois); parse with grep or awk for anomalous volumes or timestamps outside business hours. Example: `grep 'conduent.ip.range' firewall.log | awk '{print $1, $5, $7}' | sort | uniq -c | sort -rn`. For database transfers, enable query logging on production databases (if not already enabled) and search for exports to Conduent accounts or SFTP locations: `grep 'conduent\|sftp\.conduent' database_audit.log`. Check email gateway logs for large attachments or encrypted files sent to Conduent addresses. Document baseline transfer volumes (size, frequency, time-of-day) for the 30 days pre-breach to establish anomaly thresholds.

**Evidence:** Preserve firewall or proxy logs covering the suspected breach window plus 90 days prior (for baseline anomaly detection). Capture database transaction logs or query audit tables showing data exports. Export email gateway logs for large file transfers or encrypted content sent to Conduent addresses. Preserve VPN or API gateway access logs showing session timing, data volume, and source IP for any authenticated Conduent connections. Screenshot or export IAM logs showing permission grants to Conduent accounts or service principals.

**Step 3, Assessment: Inventory all PHI and PII categories transmitted to or processed by Conduent on your behalf; estimate affected population size to support HIPAA breach notification threshold analysis.**

**NIST Phase:** Detection Analysis

**Reference:** NIST 800-61r3 §3.2.2 (Determine Scope of Compromise)

**Controls:** NIST 800-53 SI-4(24) (Information System Monitoring — Automated Alerts), NIST 800-53 PM-30 (Supply Chain Risk Management), CIS 1.2 (Establish and Maintain a Data Inventory)

**Compensating:** Query your data dictionary or data governance tool (or build a manual spreadsheet if neither exists) to list all PHI/PII data elements sent to Conduent: member IDs, names, DOBs, SSNs, addresses, email, phone, plan type, claim history, etc. Query production databases for record counts by data category using SQL; example: `SELECT COUNT(DISTINCT member_id) FROM claims WHERE vendor_id='CONDUENT' AND extract_date >= '2024-01-01';`. For print/mail operations, review batch job logs to count letters, EOBs, or statements printed. Cross-reference with Conduent's retention schedules (from your BA agreement) to determine what data should still exist on their systems. Document assumptions and data quality issues (e.g., 'member count is an estimate due to duplicate records').

**Evidence:** Preserve database backups or export snapshots from the month before suspected breach date (for later forensic comparison). Capture data dictionary entries and ETL/integration mappings showing what fields flow to Conduent. Export batch job logs and print queue records showing job IDs, timestamps, record counts, and destination for Conduent jobs. Preserve email approvals or change requests authorizing data transfers to Conduent. Screenshot or export contractual schedules of services (SOW) listing data retention periods and purge procedures.

**Step 4, Communication: Engage legal and compliance to assess HIPAA breach notification obligations (60-day window to HHS, individual notification requirements); prepare member-facing communication if notification threshold is met; notify your cyber insurer.**

**NIST Phase:** Containment

**Reference:** NIST 800-61r3 §3.3 (Containment, Eradication, and Recovery) — communication component; NIST 800-66r2 §4.2 (Breach Notification Rule)

**Controls:** NIST 800-53 IR-4 (Incident Handling), NIST 800-53 IR-6 (Incident Reporting), CIS 17.1 (Designate Personnel to Manage Incident Handling)

**Compensating:** Create a breach notification timeline template (spreadsheet or document) with hard dates: suspected breach date, confirmation date, 60-day HHS notification deadline, 30-day individual notification deadline (notification deadline is the later of these). Assign a cross-functional incident response lead to coordinate legal, compliance, communications, and claims teams. Document all communications in a centralized log (email thread or incident ticket) with timestamps. Draft a member notification letter template using CMS/HHS guidance; include what data was exposed, steps Conduent is taking, and member protection resources (credit monitoring offer, fraud alert info). Notify your cyber liability insurer within 24 hours with a written summary (email is acceptable initially) containing: breach discovery date, population at risk, data types exposed, and preliminary legal/compliance assessment.

**Evidence:** Preserve all legal analysis memos on HIPAA breach notification thresholds, legal risk, and recommended actions. Document all incident communications (emails, meeting notes, Slack messages) showing when leadership, legal, compliance, marketing, and insurance were notified and what actions they decided on. Capture the member notification letter (final approved version) and distribution method (mail tracking, email delivery logs). Preserve the cyber insurance notice letter and insurer's acknowledgment. Document any state attorney general notifications (some states require separate notice in addition to HHS).

**Step 5, Long-term: Conduct a formal third-party risk review of all business associates handling PHI or PII; verify Business Associate Agreements (BAAs) include security incident notification SLAs; assess whether vendor security controls meet NIST SP 800-66r2 or equivalent standards.**

**NIST Phase:** Post Incident

**Reference:** NIST 800-61r3 §3.4 (Post-Incident Activities); NIST 800-53 SA-9 (Third-Party System Services)

**Controls:** NIST 800-53 SA-9 (Third-Party System Services), NIST 800-53 SA-3 (System Development Life Cycle), NIST 800-53 PM-30 (Supply Chain Risk Management), CIS 6.6 (Manage Access to Assets)

**Compensating:** Audit all BAAs for three missing provisions: (1) a specific incident notification SLA (target: 24-hour notice of suspected breach to your org); (2) a requirement for the vendor to demonstrate compliance with NIST SP 800-66r2 security safeguards or HIPAA Technical Safeguards Rule; (3) a right for your organization to conduct annual security assessments (on-site or via questionnaire). Create a vendor security assessment template (spreadsheet) covering: encryption in transit and at rest, access controls, audit logging, vulnerability management, incident response plan, and proof of cyber liability insurance. Send the assessment to all BAAs; flag those that do not respond within 30 days or score below your baseline (e.g., 'no encryption at rest' = fail). Document remediation timelines for each vendor: immediate fixes (encryption enablement, SLA amendment), 90-day fixes (access control improvements), and quarterly re-assessments. Update your Vendor Risk Register with post-assessment ratings.

**Evidence:** Preserve original and amended BAAs (scan signatures if paper). Document all security assessment questionnaire responses from vendors (email, portal exports). Capture evidence of vendor security control implementation (SOC 2 reports, ISO 27001 certs, vulnerability scan results, penetration test summaries if available). Preserve email communications regarding SLA negotiations or remediation timelines. Document any vendor assessments that resulted in contract termination or data transfer restrictions (keep in file for audit trail).

## Detection Guidance

Direct detection within your environment is limited because the breach occurred at the vendor layer. Focus detection efforts on: (1) Business associate connection logs, review SFTP, API, or EDI transfer logs to and from

Conduent endpoints for anomalous data volumes or off-hours transfers; (2) Identity and access logs, cross-reference T1078 (Valid Accounts) by auditing any shared or service accounts used in Conduent integrations for unauthorized access patterns; (3) Data loss prevention (DLP) alerts, review historical DLP events on outbound transfers to Conduent IP ranges or domains; (4) SIEM queries, search for connection events to known Conduent infrastructure addresses in the 90-day window preceding public disclosure; (5) Vendor notification channel, primary detection path is direct notification from Conduent per your BAA incident notification clause. No public IOCs specific to this incident are available at time of content generation.

## Framework Mappings

### MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1530** — Data from Cloud Storage
- **T1199** — Trusted Relationship

### NIST-800-53R5

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

### HIPAA-SECURITY

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

### SOC2-TSC

- **CC7.4** — Responds to identified security incidents
- **CC9.2** — Manages risks associated with vendors and business partners

### ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information
- **A.5.21** — Managing information security in the ICT supply chain

### NIST-CSF-2

- **RS.CO-03** — Recovery activities and progress communicated
- **GV.SC-01** — Cybersecurity supply chain risk management program

### CIS-V8

- **15.1** — Establish and Maintain an Inventory of Service Providers

## MITRE ATT&CK Mapping

| Technique ID | Technique Name | Tactic |
|---|---|---|
| T1078 | Valid Accounts | Defense-Evasion |
| T1530 | Data from Cloud Storage | Collection |
| T1199 | Trusted Relationship | Initial-Access |

## Sources

| Source | URL | Tier |
|---|---|---|
| **Today** | https://today.iu.edu/live/news/49092-data-breach-impacts-some-anthe... | T1 |
| **Consumer information on Anthem Blue Cross data breach** | https://www.insurance.ca.gov/0400-news/0100-press-releases/anthemcy... | T1 |
| **Anthem Data Breach and How This Affects You - People & Culture** | https://hr.berkeley.edu/news/anthem-data-breach-and-how-affects-you | T1 |
| **Anthem Data Breach: What Happened, Impact, and Lessons** | https://www.huntress.com/threat-library/data-breach/anthem-data-breach | T3 |
| **Cyber Case Study: Anthem Data Breach - CoverLink Insurance** | https://coverlink.com/case-study/anthem-data-breach/ | T3 |



Generated 2026-03-29 18:43 UTC by TJS Security Command Center