INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-31 06:18 UTC

CareCloud EHR Breach Exposes Patient Records Across One of Six SaaS Environments

DATA BREACH | HIGH | CVSS 7.5

SCC Item ID	SCC-DBR-2026-0071
Type	Data Breach
Severity	HIGH
CVSS Base Score	7.5
Affected Products	CareCloud Health EHR platform (one of six SaaS environments); CareCloud revenue cycle management, practice management, and patient experience management solutions
Published	2026-03-30T17:44:31
Discovery Source	Rss

Executive Summary

On March 16, 2026, CareCloud, a New Jersey-based healthcare SaaS provider, confirmed unauthorized access to one of its six EHR environments, resulting in confirmed patient data exposure and an eight-hour network disruption. The breach affects downstream medical practices using CareCloud's revenue cycle management, practice management, and patient experience platforms, with full patient impact scope still undetermined. SEC disclosure has been filed; organizations relying on CareCloud as a third-party SaaS vendor face both direct data exposure risk and regulatory notification obligations under HIPAA.

Technical Analysis

CareCloud confirmed unauthorized access to one of six multi-tenant SaaS EHR environments on March 16, 2026. No CVE has been assigned; no ransomware group has claimed responsibility; the initial access vector has not been publicly disclosed. Applicable weakness classes based on available reporting: CWE-284 (Improper Access Control), CWE-200 (Exposure of Sensitive Information to an Unauthorized Actor), and CWE-522 (Insufficiently Protected Credentials), suggesting access control failure, credential compromise, or both as plausible initial access paths. MITRE ATT&CK techniques consistent with the reported indicators include T1078 (Valid Accounts), T1190 (Exploit Public-Facing Application), T1530 (Data from Cloud Storage), T1213 (Data from Information Repositories), T1041 (Exfiltration Over C2 Channel), and T1486 (Data Encrypted for Impact, noted as a mapped technique; no ransomware deployment confirmed). The breach is contained to one of six SaaS environments; lateral movement across remaining environments has not been confirmed but has not been ruled out publicly. A Big Four-affiliated cyber response team has been engaged. Patch status and remediated vector: not disclosed as of 2026-03-30. No CVSS vector or EPSS data available; qualitative severity

rated High given PHI exposure in a regulated environment.

Action Checklist

1. Step 1: Containment, If your organization uses CareCloud EHR, revenue cycle, practice management, or patient experience products, contact your CareCloud account representative immediately to confirm whether your tenant resides in the affected environment. Request written confirmation of environment isolation status and whether your data partition was accessed. Do not assume non-impact based on CareCloud's multi-environment architecture until confirmed in writing.
2. Step 2: Detection, Review your CareCloud-integrated identity and access logs for anomalous authentication events between March 1-16, 2026 (pre-disclosure window). Check SSO, SAML assertion logs, and any API gateway logs connecting your systems to CareCloud endpoints. Look for authentication from unfamiliar IPs, off-hours access to patient record queries, and bulk data export events. If CareCloud provides tenant-level audit logs, request the full export for this window immediately.
3. Step 3: Eradication, Rotate all credentials used to authenticate to CareCloud services, including service accounts, API keys, and any shared credentials used by integrated systems (billing, EHR, scheduling). Audit and revoke third-party integrations connecting to CareCloud that may share credential scope. If SSO is in use, force token invalidation for the affected integration. Confirm with CareCloud when the affected environment was fully isolated and what remediation was applied before resuming normal operations.
4. Step 4: Recovery, Validate that PHI accessed via CareCloud APIs or portals has not been staged elsewhere in your environment. Confirm integrity of patient records synced from CareCloud to internal systems. Monitor for anomalous outbound data transfers from any system with a CareCloud integration. Re-enable integrations only after CareCloud provides a formal incident report confirming scope and remediation.
5. Step 5: Post-Incident, Conduct a third-party vendor risk review of CareCloud's current security posture, including requesting their updated SOC 2 Type II report and any incident-specific attestation. Assess whether your organization's HIPAA Business Associate Agreement (BAA) with CareCloud requires breach notification to patients on your behalf or assigns that obligation to CareCloud. Document this incident in your risk register and evaluate whether SaaS vendor contractual requirements for breach notification timelines and audit rights are adequate. Review your multi-tenant SaaS inventory for similar access control and credential exposure risks across other healthcare vendors.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to legal counsel, HIPAA Privacy Officer, and executive leadership if CareCloud confirms your tenant resided in the affected environment, if any PHI export or bulk query event is identified in your audit logs for the March 1–16 window, or if your BAA review indicates your organization (as a Covered Entity) holds primary breach notification obligation to affected patients — HIPAA mandates notification to HHS and affected individuals within 60 days of discovery (45 CFR §164.410, §164.412).

Recovery Notes	Re-enable CareCloud integrations only after receiving CareCloud's formal written incident report confirming root cause, full isolation of the affected environment, and remediation validation — do not accept verbal assurances. After re-enabling, maintain elevated monitoring on all CareCloud API gateway logs and outbound data transfer volumes for a minimum of 30 days, baselining against pre-March-1 traffic patterns to detect any residual unauthorized access or re-compromise. Validate patient record integrity in all internally synced data stores by comparing record counts, modification timestamps, and a sample of PHI field values against your most recent pre-breach backup to confirm no data manipulation occurred during the eight-hour network disruption window.
Forensic Artifacts	IdP/SSO SAML assertion logs (Okta System Log, Azure AD Sign-In Logs, or AD FS Security Event Log) for the March 1–16, 2026 window — specifically targeting assertions issued to CareCloud service provider entity IDs, flagging any with unexpected source IPs, unusual AuthnContextClassRef values, or sessions initiated outside business hours | API gateway access logs (NGINX, Kong, AWS API Gateway, or equivalent) for all outbound requests to CareCloud API endpoints — filter for unusually large response payloads (potential bulk PHI export), HTTP 200 responses to patient record query endpoints, and any API calls authenticated with service account credentials outside normal integration schedules | CareCloud tenant-level audit log export (if available via CareCloud admin portal) covering March 1–16, 2026 — this is the primary artifact confirming whether your data partition was accessed; request immediately and preserve with integrity hash upon receipt | Outbound firewall and proxy session logs from integration servers hosting CareCloud billing, EHR sync, or scheduling connectors — filter for large data transfers (>10MB sessions) to non-CareCloud external IPs during the breach window, which would indicate data staging or exfiltration from your environment post-unauthorized access | Windows Security Event Log Event ID 4663 (Object Access) and Event ID 4688 (Process Creation) from any on-premises servers running CareCloud integration middleware or storing CareCloud-synced PHI exports — Event ID 4663 identifies which files were read during the window; Event ID 4688 identifies any anomalous processes (e.g., archiving or compression tools) that could indicate local data staging prior to exfiltration

Per-Action IR Details

Step 1: Containment — If your organization uses CareCloud EHR, revenue cycle, practice management, or patient experience products, contact your CareCloud account representative immediately to confirm whether your tenant resides in the affected environment. Request written confirmation of environment isolation status and whether your data partition was accessed. Do not assume non-impact based on CareCloud's multi-environment architecture until written confirmation is received.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy; CSF [RS] — Execute IR plan, categorize, contain, communicate, mitigate

Controls: NIST IR-4 (Incident Handling), NIST IR-6 (Incident Reporting), NIST SA-9 (External System Services), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without an enterprise vendor risk portal, use a structured email template to CareCloud support with specific written questions: (1) Is tenant ID [your-org-ID] hosted in the compromised environment? (2) Were any API calls, data exports, or authentication events recorded against our partition between March 1–16, 2026? (3) Provide signed written attestation of isolation status. Log the timestamp and reference number of every communication. A two-person team can manage this via a shared mailbox with a tracking spreadsheet (date, contact name, response status, assertion type). If CareCloud does not respond within 24 hours, treat impact as confirmed and escalate to HIPAA Breach Notification procedures.

Evidence: Before contacting CareCloud, snapshot your current CareCloud integration configuration: record all tenant IDs, environment URLs (e.g., *.carecloud.com subdomains your org connects to), and any environment labels visible in your CareCloud admin portal. Screenshot or export the environment assignment page. This establishes your pre-communication baseline and prevents CareCloud from retroactively reassigning your tenant designation. Preserve any prior CareCloud communications referencing your environment assignment (onboarding docs, BAA schedules, support tickets).

Step 2: Detection — Review your CareCloud-integrated identity and access logs for anomalous authentication events between March 1–16, 2026 (pre-disclosure window). Check SSO, SAML assertion logs, and any API gateway logs connecting your systems to CareCloud endpoints. Look for authentication from unfamiliar IPs, off-hours access to patient record queries, and bulk data export events. If CareCloud provides tenant-level audit logs, request the full export for this window immediately.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis; CSF [DE] — Monitor, detect, analyze, correlate, triage adverse events

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST IR-5 (Incident Monitoring), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: For teams without a SIEM, execute the following manual log review sequence: (1) Pull your IdP logs (Okta, Azure AD, or on-prem AD FS) and filter SAML assertion events targeting CareCloud audience URIs — export to CSV and sort by source IP, then flag any IP not in your known corporate egress range. (2) Query your firewall or proxy logs for outbound connections to CareCloud API endpoints (api.carecloud.com, app.carecloud.com) between 2026-03-01 00:00 UTC and 2026-03-16 23:59 UTC — use grep or PowerShell 'Select-String' against exported logs. (3) If you use an API gateway (Kong, AWS API Gateway, NGINX), pull access logs and filter for HTTP 200 responses to CareCloud-bound requests with response body sizes exceeding your baseline (bulk export indicator). A two-person team should divide: one analyst owns IdP/SSO log review, the other owns network/API gateway log review, then cross-reference findings.

Evidence: Capture and preserve before analysis: (1) Full IdP authentication logs for the March 1–16 window, exported as immutable files with hash verification (sha256sum on export). (2) SAML assertion logs showing NameID, SessionIndex, and AuthnContextClassRef values — anomalous assertions may show unexpected AuthnContextClassRef values (e.g., 'PasswordProtectedTransport' where MFA is normally enforced). (3) API gateway access logs showing CareCloud-bound requests, particularly any with HTTP methods GET/POST to patient record or report endpoints with atypically large response payloads. (4) DNS query logs for your resolver showing lookups to CareCloud domains — lateral movement or data staging sometimes reveals itself through unexpected DNS resolution patterns from non-standard internal hosts. Preserve all logs in write-once storage before analysis begins per NIST AU-9 (Protection of Audit Information).

Step 3: Eradication — Rotate all credentials used to authenticate to CareCloud services, including service accounts, API keys, and any shared credentials used by integrated systems (billing, EHR, scheduling). Audit and revoke third-party integrations connecting to CareCloud that may share credential scope. If SSO is in use, force token invalidation for the affected integration. Confirm with CareCloud when the affected environment was fully isolated and what remediation was applied before resuming normal operations.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication; CSF [RS] — Remove threat from environment, verify eradication

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), NIST IA-5 (Authenticator Management), NIST CM-2 (Baseline Configuration), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: For teams without a PAM solution: (1) Run 'Get-ADServiceAccount -Filter *' (PowerShell) or 'net user /domain' to enumerate all service accounts with CareCloud authentication scope — cross-reference against your CareCloud integration documentation. (2) For each API key issued by CareCloud, revoke via the CareCloud admin portal and document the revocation timestamp — if portal access is unavailable, submit written revocation request to CareCloud with explicit key IDs. (3) Force SSO session invalidation by revoking the CareCloud application assignment

in your IdP (Okta: Deactivate application; Azure AD: Revoke all refresh tokens via 'Revoke-AzureADUserAllRefreshToken' cmdlet for service principals). (4) For shared credentials used by billing or scheduling integrations (common in small practice EHR deployments), change passwords immediately and update all downstream config files or secrets stores. Document every rotated credential with a before/after timestamp.

Evidence: Before rotating credentials, document the full current state: (1) Export a list of all CareCloud-integrated service accounts and API keys with their last-used timestamps — this establishes whether any credential was used during the breach window. (2) If your IdP provides it, export the OAuth token issuance log for the CareCloud application integration to identify all tokens issued between March 1–16, 2026 — tokens issued during this window should be treated as potentially compromised regardless of source IP. (3) Check for any hardcoded credentials in integration scripts or configuration files connecting to CareCloud (common in smaller practice management setups) — run grep -r 'carecloud' on integration server config directories and capture findings before rotation. This evidence establishes the credential exposure scope and supports HIPAA breach notification scope determination.

Step 4: Recovery — Validate that PHI accessed via CareCloud APIs or portals has not been staged elsewhere in your environment. Confirm integrity of patient records synced from CareCloud to internal systems. Monitor for anomalous outbound data transfers from any system with a CareCloud integration. Re-enable integrations only after CareCloud provides a formal incident report confirming scope and remediation.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery; CSF [RC] — Execute recovery plan, restore systems, verify integrity, communicate

Controls: NIST IR-4 (Incident Handling), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AU-11 (Audit Record Retention), NIST CP-9 (System Backup), CIS 3.2 (Establish and Maintain a Data Inventory), CIS 3.3 (Configure Data Access Control Lists)

Compensating: For teams without DLP or UEBA: (1) Use Wireshark or tcpdump on integration server network interfaces to capture outbound traffic for 72 hours post-credential rotation — filter for large payload transfers (>1MB) to non-CareCloud external IPs from systems that hold CareCloud-synced PHI. Save captures with sha256 integrity hashes. (2) On Windows integration servers, query the Security Event Log for Event ID 4663 (Object Access — file read) on directories holding CareCloud-synced patient data exports — filter for the March 1–16 window. (3) Compare current patient record counts and last-modified timestamps in any local database or file store synced from CareCloud against your most recent pre-March-1 backup — statistical anomalies (unexpected bulk modifications, new records, deletions) indicate possible data manipulation or staging. (4) Deploy osquery on integration servers with a query targeting large file creation events: 'SELECT * FROM file WHERE directory='/path/to/sync/' AND size > 10000000 AND ctime > 1740787200;' (Unix timestamp for March 1, 2026).

Evidence: Before re-enabling CareCloud integrations, collect and preserve: (1) A point-in-time snapshot of all PHI data stores synced from CareCloud (row counts, schema checksums, last-modified timestamps per table) — this establishes integrity baseline for post-recovery comparison. (2) Outbound firewall session logs from integration servers for the March 1–16 window, specifically filtering for large data transfers to non-CareCloud external IPs. (3) Windows Event ID 4688 (Process Creation) logs from integration servers showing any new processes — particularly scripting interpreters (powershell.exe, python.exe, cmd.exe) — executed in the breach window that are not part of the normal integration process baseline. This evidence supports both internal integrity validation and any downstream HIPAA breach notification impact quantification.

Step 5: Post-Incident — Conduct a third-party vendor risk review of CareCloud's current security posture, including requesting their updated SOC 2 Type II report and any incident-specific attestation. Assess whether your organization's HIPAA Business Associate Agreement (BAA) with CareCloud requires breach notification to patients on your behalf or assigns that obligation to CareCloud. Document this incident in your risk register and evaluate whether SaaS vendor contractual requirements for breach notification timelines and audit rights are adequate. Review your multi-tenant SaaS inventory for similar access control and credential exposure risks across other healthcare vendors.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity; CSF [GV, ID] — Lessons learned, update policies, improve detection, share intelligence

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST RA-3 (Risk Assessment), NIST SA-9 (External System Services), 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: For teams without a GRC platform: (1) Create a structured vendor risk record in a spreadsheet (or Jira/ServiceNow ticket) capturing: BAA clause reference for breach notification obligations, CareCloud's stated notification timeline vs. actual March 16 disclosure date, SOC 2 Type II last audit date and coverage period, and open remediation commitments from CareCloud. (2) Draft a formal lessons-learned document within 30 days per NIST 800-61r3 §4 — include timeline reconstruction, detection gap identification (why did you learn of this via SEC disclosure rather than direct CareCloud notification?), and specific control improvements. (3) For the multi-tenant SaaS inventory review, build a one-page matrix of all healthcare SaaS vendors listing: environment isolation architecture (shared vs. dedicated), credential type (API key, OAuth, SSO), PHI data categories accessible, and BAA status — prioritize any vendor using a shared multi-tenant architecture similar to CareCloud's six-environment model.

Evidence: Preserve for post-incident documentation and potential regulatory inquiry: (1) All written communications with CareCloud from March 16 onward, timestamped and stored in write-protected archive — HIPAA breach notification regulations (45 CFR §164.410) require Business Associates to notify Covered Entities without unreasonable delay and no later than 60 days. (2) Your organization's internal incident timeline log documenting when you first learned of the breach, from what source, and what actions were taken — this is a required element of HIPAA breach response documentation. (3) A copy of the current BAA with CareCloud, with the breach notification and audit rights clauses highlighted — this document determines your regulatory obligations and legal remedies. (4) CareCloud's SEC disclosure filing (8-K or equivalent) — preserve as evidence of the breach's confirmed scope and timing, which anchors your notification obligation timeline. Retain all incident documentation for a minimum of six years per HIPAA recordkeeping requirements (45 CFR §164.530(j)).

Detection Guidance

No IOCs (IPs, domains, hashes) have been publicly released as of 2026-03-30. Detection must rely on behavioral and access pattern analysis. Focus areas: (1) Authentication logs, review SIEM for CareCloud-related authentication events from March 1-16, 2026; flag logins from IPs outside known CareCloud infrastructure ranges, impossible travel events, or credential use outside business hours. (2) Data access telemetry, if CareCloud exposes audit logs per tenant, query for bulk record retrievals, mass export events, or queries against patient demographics and PHI fields at unusual volume or cadence. (3) API gateway logs, look for high-volume GET requests against CareCloud API endpoints, particularly those returning patient record payloads. (4) Outbound data transfer, check DLP and firewall logs for large outbound transfers to non-CareCloud destinations originating from integrated systems. (5) Credential reuse, if CareCloud credentials share password patterns with internal systems, run a credential audit against your identity provider for matching patterns. Detection confidence is low given no public IOCs; behavioral indicators are the primary signal available.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`carecloud.com`	CareCloud primary domain — include in outbound monitoring to distinguish legitimate tenant traffic from anomalous exfiltration patterns. Not malicious; reference for traffic baseline.	LOW

Framework Mappings

MITRE-ATTACK

- **T1530** — Data from Cloud Storage
- **T1213** — Data from Information Repositories
- **T1486** — Data Encrypted for Impact
- **T1190** — Exploit Public-Facing Application
- **T1041** — Exfiltration Over C2 Channel
- **T1657** — Financial Theft
- **T1078** — Valid Accounts

NIST-800-53R5

- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **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
- **CA-7** — Continuous Monitoring
- **SI-4** — System Monitoring
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AC-3** — Access Enforcement
- **SC-28** — Protection of Information at Rest
- **IR-4** — Incident Handling

OWASP-TOP10-2021

- **A04:2021** — Insecure Design
- **A07:2021** — Identification and Authentication Failures
- **A01:2021** — Broken Access Control

CIS-V8

- **5.2** — Use Unique Passwords
- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **6.3** — Require MFA for Externally-Exposed Applications

HIPAA-SECURITY

- **164.308(a)(5)(ii)(D)** — Password Management
- **164.312(a)(1)** — Access Control
- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.312(d)** — Person or Entity Authentication

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC6.3** — Authorizes, modifies, or removes access

NIST-CSF-2

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

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.5.23** — Information security for use of cloud services

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1530	Data from Cloud Storage	Collection
T1213	Data from Information Repositories	Collection
T1486	Data Encrypted for Impact	Impact
T1190	Exploit Public-Facing Application	Initial-Access
T1041	Exfiltration Over C2 Channel	Exfiltration
T1657	Financial Theft	Impact
T1078	Valid Accounts	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/healthcare-tech-firm...	T3
Healthcare IT Platform CareCloud Probing Potential Data Breach	https://www.securityweek.com/healthcare-it-platform-carecloud-probi...	T3
CareCloud Data Breach: The Supply Chain Threat to Healthcare ...	https://cmitsolutions.com/lasvegas-nv-1206/blog/carecloud-data-brea...	T3
Security Risk Analysis Essentials - CareCloud	https://carecloud.com/continuum/essentials-security-risk-analysis/	T3
CareCloud: Cloud-Based and AI-Powered Healthcare Solutions	https://carecloud.com/	T3

Generated 2026-03-31 06:18 UTC by TJS Security Command Center