INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-12 14:15 UTC

Novo Nordisk Breach Exposes Clinical Trial Data and Healthcare Professional Contact Details

DATA BREACH | HIGH | CVSS 7.5

SCC Item ID	SCC-DBR-2026-0164
Type	Data Breach
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Novo Nordisk internal IT systems (unspecified scope; investigation ongoing)
Published	2026-06-12T06:13:19
Discovery Source	Rss

Executive Summary

Novo Nordisk confirmed unauthorized actors accessed internal IT systems and exfiltrated clinical trial records along with healthcare professional (HCP) contact details including names, registration numbers, phone numbers, and WhatsApp information. Patient data was pseudonymized, reducing direct re-identification risk, but the exposed HCP contact data creates an active social engineering and phishing attack surface targeting medical professionals. The breach vector and full exfiltration scope remain undisclosed; investigation is ongoing, and the regulatory exposure under GDPR and applicable healthcare data protection frameworks is material.

Technical Analysis

Novo Nordisk disclosed unauthorized access to internal IT systems resulting in exfiltration of two data classes: clinical trial records and HCP contact information (names, registration numbers, direct phone numbers, WhatsApp contact details). Patient data was pseudonymized prior to exfiltration, which limits but does not eliminate re-identification risk if attackers possess auxiliary datasets. No CVE is applicable; this is an organizational breach. CWE mapping: CWE-284 (Improper Access Control, enabling unauthorized system entry), CWE-359 (Exposure of Private Personal Information to an Unauthorized Actor, HCP PII and clinical trial records), CWE-668 (Exposure of Resource to Wrong Sphere, internal records accessible to external actors). MITRE ATT&CK techniques consistent with this incident pattern: T1078 (Valid Accounts, possible credential-based initial access), T1213 (Data from Information Repositories), T1530 (Data from Cloud Storage), T1041 (Exfiltration Over C2 Channel), T1567 (Exfiltration Over Web Service), T1589.002 (Gather Victim Identity Information: Email Addresses), T1598 (Phishing for Information), T1566 (Phishing, downstream abuse of exfiltrated HCP contact data). Breach vector, dwell time, affected system scope, and patch or remediation status

have not been publicly disclosed. Attribution is unknown.

Action Checklist

1. Containment: If your organization partners with Novo Nordisk or has shared HCP, clinical, or research data through joint programs, contact Novo Nordisk's security team immediately using their official vulnerability reporting channel (https://www.novonordisk.com/contact-us/report-a-security-vulnerability.html) and request written confirmation of whether your data falls within the affected scope. Suspend data-sharing integrations with Novo Nordisk systems pending clarification of breach boundaries.
2. Detection: Review your SIEM for inbound communications impersonating Novo Nordisk personnel or clinical trial coordinators targeting your HCPs or research staff (AU-2, AU-6, CIS 8.2). Query email gateway logs for domains spoofing novonordisk.com or associated clinical trial program domains. Monitor for WhatsApp-based social engineering attempts targeting medical staff, this is a direct downstream risk from the exfiltrated HCP WhatsApp contact data. No public IOCs have been released as of this report date; check Novo Nordisk's security updates regularly for indicators. Behavioral detection is the primary available method.
3. Eradication: No patch is applicable; this is an organizational breach at Novo Nordisk, not a software vulnerability in your environment. If your organization maintains shared accounts or API integrations with Novo Nordisk systems, rotate those credentials immediately (D3-CRO). Audit third-party access grants to any shared clinical or HCP data repositories and revoke sessions that cannot be verified (AC-2, AC-3, D3-UAP).
4. Recovery: Validate that HCP contact records in your own systems have not been accessed or modified by unauthorized parties. Review access logs for internal clinical trial data stores and HCP directories covering the period since the most recently confirmed clean state (AU-6, AU-9). Re-enable data-sharing integrations with Novo Nordisk only after receiving written confirmation from their security team that affected systems have been remediated and access controls have been hardened (AC-20).
5. Post-Incident: Conduct a tabletop exercise scoping your organization's exposure to third-party data breaches involving shared HCP or clinical trial data. Assess whether your data classification and third-party data sharing agreements require notification obligations triggered by a partner breach (CIS 3.2, NIST AC-20). Evaluate whether MFA is enforced on all externally-exposed systems housing clinical or HCP data, this breach pattern is consistent with credential-based access that MFA would interrupt (CIS 6.3, CIS 6.5, D3-MFA).

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to legal, privacy counsel, and executive leadership if your organization's internal review confirms that HCP contact records or clinical trial data housed in your own systems were accessed or exfiltrated during the period of the Novo Nordisk breach, or if any data sharing agreement with Novo Nordisk triggers mandatory breach notification obligations under GDPR, HIPAA, or applicable national health data regulations.

Recovery Notes	Once data-sharing integrations are re-enabled following written Novo Nordisk remediation confirmation, maintain enhanced audit logging on all HCP directory and clinical trial data access for a minimum of 90 days, alert-thresholding on any bulk export or anomalous after-hours access to those repositories. Monitor for downstream spear-phishing or vishing campaigns targeting your HCPs using Novo Nordisk clinical trial branding for at least 6 months post-breach, as the exfiltrated HCP contact data including WhatsApp details will remain exploitable long after the initial breach window closes. Validate that all third-party data sharing agreements are updated to require reciprocal breach notification within 72 hours, consistent with GDPR Article 33 timelines, as the delayed disclosure timeline in this incident created preventable response lag for partner organizations.
Forensic Artifacts	Email gateway message trace logs: Filter for inbound messages from novonordisk.com lookalike domains (e.g., novo-nordisk.com, novonordsk.com, novonordisk-trials.com) received from the breach disclosure date forward — these represent social engineering attempts leveraging the exfiltrated HCP contact details. | IAM and directory service audit logs (Windows Security Event Log Event IDs 4624, 4634, 4648, 4662, 4672) for all service accounts and integration accounts with access to shared Novo Nordisk data repositories, covering a 90-day lookback window to identify unauthorized access predating the breach disclosure. | API gateway or reverse proxy access logs showing data volume and frequency of requests from Novo Nordisk integration endpoints to your clinical trial data stores and HCP directories — abnormal spikes in data pull volume are the primary forensic indicator for pre-exfiltration reconnaissance against your side of the shared data environment. | HCP directory and clinical trial data store access logs from your internal systems (e.g., Active Directory OU audit trail, REDCap audit log, SharePoint unified audit log) compared against a known-good baseline export — unauthorized read or export events on HCP contact fields (name, phone, registration number) are the specific artifact this breach pattern would produce in downstream partner environments. | Staff-reported social engineering artifacts: Screenshots and metadata (sender phone numbers, WhatsApp account details, message timestamps) from any unsolicited Novo Nordisk-branded contact attempts received by HCPs or research staff via WhatsApp, SMS, or phone — these constitute threat-actor IOCs directly traceable to the exfiltrated HCP WhatsApp contact data and should be preserved and shared with Novo Nordisk's security team and sector ISACs (e.g., H-ISAC) for collective defense.

Per-Action IR Details

Containment — If your organization partners with Novo Nordisk or has shared HCP, clinical, or research data through joint programs, contact Novo Nordisk's security team via their disclosed vulnerability reporting channel and request confirmation of whether your data falls within the affected scope. Suspend data-sharing integrations with Novo Nordisk systems pending clarification of breach boundaries.

NIST Phase: Containment

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

Controls: NIST AC-20 (Use Of External Systems), NIST AC-3 (Access Enforcement), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: If API or SFTP integrations exist with Novo Nordisk systems, immediately disable the relevant service accounts via CLI (e.g., `net user /active:no` on Windows or `usermod -L ` on Linux). Block egress to Novo Nordisk integration endpoints at the perimeter firewall using an explicit deny rule. Document the suspension with a timestamped change ticket before acting.

Evidence: Before suspending integrations, capture: (1) current active sessions to Novo Nordisk endpoints via `netstat -ano` or `Get-NetTCPConnection | Where-Object {$_.RemoteAddress -like ''}` to document live connection state; (2) recent authentication logs for the integration service account from your IAM or directory service (Windows Security Event Log Event ID 4624/4634 for the service account); (3) API gateway or proxy logs showing data volumes

transferred to Novo Nordisk endpoints over the past 90 days to establish a baseline for exfiltration scope assessment.

Detection — Review your SIEM for inbound communications impersonating Novo Nordisk personnel or clinical trial coordinators targeting your HCPs or research staff (AU-2, AU-6, CIS 8.2). Query email gateway logs for domains spoofing novonordisk.com or associated clinical trial program domains. Monitor for WhatsApp-based social engineering attempts targeting medical staff — this is a direct downstream risk from the exfiltrated HCP WhatsApp contact data. No public IOCs have been released; behavioral detection is the primary available method.

NIST Phase: Detection Analysis

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

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, query your email gateway's message trace directly (e.g., Exchange Online: `Get-MessageTrace -SenderAddress '*novonordisk*' -StartDate -EndDate ` or equivalent on-prem transport log search). Use PowerShell to parse mail headers for lookalike domains: filter on From addresses matching regex `novo.?nordisk` but not originating from verified Novo Nordisk MX records. For WhatsApp monitoring, issue a staff advisory to HCPs and research staff asking them to forward and report any unsolicited Novo Nordisk-branded contact attempts — manual human reporting is the only feasible compensating control for encrypted mobile messaging channels.

Evidence: Capture before any blocking action: (1) email gateway logs showing sender domains, DKIM/SPF pass-fail results, and recipient lists for any novonordisk.com lookalike domains received since the breach disclosure date; (2) DNS query logs (if available via Pi-hole or local resolver) for lookups of novonordisk.com lookalike domains from internal hosts; (3) any reported WhatsApp messages from staff, preserved with screenshots and metadata (sender number, timestamp) — these constitute social engineering IOCs specific to the exfiltrated HCP WhatsApp contact data.

Eradication — No patch is applicable; this is an organizational breach at Novo Nordisk, not a software vulnerability in your environment. If your organization maintains shared accounts or API integrations with Novo Nordisk systems, rotate those credentials immediately (D3-CRO). Audit third-party access grants to any shared clinical or HCP data repositories and revoke sessions that cannot be verified (AC-2, AC-3, D3-UAP).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-2 (Account Management), NIST AC-3 (Access Enforcement), NIST AC-12 (Session Termination)

Compensating: Enumerate all third-party accounts with access to your clinical or HCP data repositories: on Windows, run `Get-ADUser -Filter {Description -like '*NovNordisk*' -or Description -like '*integration*'} -Properties *` and cross-reference with any OAuth token grants in your identity provider. For web-hosted repositories, use the provider's token management console to enumerate and revoke active refresh tokens for integration accounts. Document every revoked credential with timestamp and approver before rotation to preserve the audit trail.

Evidence: Before revoking any sessions or rotating credentials, capture: (1) active session tokens and last-activity timestamps for all Novo Nordisk integration accounts from your IAM platform or LDAP (Windows Security Event Log Event ID 4648 — explicit credential use — and 4672 — special privilege logon — for the integration accounts); (2) authorization logs from any shared clinical data repository (e.g., SharePoint audit logs, REDCap access logs, or SFTP server auth logs) for the integration accounts covering the 90-day window preceding the breach disclosure; (3) a full export of current OAuth/API token grants from your identity provider prior to revocation, to document what access existed at time of containment.

Recovery — Validate that HCP contact records in your own systems have not been accessed or modified by unauthorized parties. Review access logs for internal clinical trial data stores and HCP directories covering the period since the most recently confirmed clean state (AU-6, AU-9). Re-enable data-sharing integrations with Novo Nordisk only after receiving written confirmation from their security team that affected systems have been remediated and access controls have been hardened (AC-20).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-9 (Protection Of Audit Information), NIST AC-20 (Use Of External Systems)

Compensating: Without enterprise DLP, use PowerShell or bash to diff current HCP directory exports against a known-good backup snapshot: `Compare-Object (Import-Csv .\hcp_baseline.csv) (Import-Csv .\hcp_current.csv) -Property Name,Phone,Email` to surface unauthorized modifications. For audit log integrity, verify log file hashes against stored checksums if your logging system supports it (e.g., Windows Event Log: export and hash with `Get-FileHash`). For re-enablement gates, require written confirmation from Novo Nordisk's CISO or designated security contact — email is acceptable, but retain as a dated artifact in your incident record.

Evidence: Before re-enabling integrations, confirm and document: (1) access logs from your HCP directory and clinical trial data stores (e.g., Active Directory audit logs for OU containing HCP records — Event ID 4662 — object access on directory objects; or equivalent LDAP audit trail) covering the period from the last known-clean state to present; (2) file integrity hashes or change-detection output for HCP contact record exports stored in file shares or databases — compare against pre-breach baseline snapshots; (3) written remediation confirmation from Novo Nordisk security team, retained as a dated artifact to support any regulatory notification decisions.

Post-Incident — Conduct a tabletop exercise scoping your organization's exposure to third-party data breaches involving shared HCP or clinical trial data. Assess whether your data classification and third-party data sharing agreements require notification obligations triggered by a partner breach (CIS 3.2, NIST AC-20). Evaluate whether MFA is enforced on all externally-exposed systems housing clinical or HCP data — this breach pattern is consistent with credential-based access that MFA would interrupt (CIS 6.3, CIS 6.5, D3-MFA).

NIST Phase: Post Incident

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

Controls: CIS 3.2 (Establish and Maintain a Data Inventory), NIST AC-20 (Use Of External Systems), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

Compensating: For teams without a GRC platform, conduct the tabletop using a structured scenario document: seed the exercise with the actual Novo Nordisk breach parameters (HCP contact exfiltration, clinical trial records, unknown vector) and walk through your organization's third-party data sharing agreements manually. Use a spreadsheet to inventory all third parties with access to HCP or clinical data, mapped against data classification and contractual notification triggers. For MFA gap assessment, use a free TOTP solution (e.g., Google Authenticator with Authelia as a reverse proxy MFA layer) if enterprise MFA licensing is unavailable for external-facing clinical data portals.

Evidence: For the lessons-learned record, preserve and review: (1) the complete incident timeline documenting when your organization first learned of the Novo Nordisk breach, what actions were taken, and elapsed time between notification and containment — this feeds the tabletop scenario and regulatory notification gap analysis; (2) the inventory of third-party data sharing agreements referencing Novo Nordisk or similar pharma/clinical partners, with notation of which agreements contain breach notification obligations and applicable regulatory frameworks (e.g., GDPR Article 28 processor obligations, HIPAA Business Associate Agreement provisions if US-based HCPs are involved); (3) MFA coverage audit results for all externally-exposed systems housing HCP or clinical trial data, documented as a baseline for post-incident hardening verification.

Detection Guidance

No IOCs have been publicly released as of this report date; check Novo Nordisk's security updates regularly for indicators. Detection relies on behavioral and communication-pattern monitoring. In your email gateway and messaging security tools, create detection rules for inbound messages referencing Novo Nordisk clinical trial programs, HCP registration numbers, or WhatsApp contact requests from unverified Novo Nordisk sender identities, consistent with T1566 and T1598 downstream abuse of exfiltrated HCP data. In your SIEM, alert on unusual access to internal HCP directories or clinical trial data repositories, particularly after-hours access, bulk

record queries, or access from unfamiliar source IPs or user agents (AU-6, AU-12, CIS 8.2). If your organization uses shared data integrations with Novo Nordisk, review authentication logs on those integration accounts for anomalous session activity consistent with T1078 (Valid Accounts). Monitor endpoint and DLP telemetry for large outbound transfers from clinical data stores (T1041, T1567). Because pseudonymization does not prevent re-identification when combined with auxiliary data, treat exfiltrated clinical trial record fields as potentially re-identifiable and flag any external queries attempting to correlate pseudonymized records against other datasets. No specific log event IDs are available without knowledge of the affected system vendors.

Framework Mappings

MITRE-ATTACK

- **T1598** — Phishing for Information
- **T1589.002** — Email Addresses
- **T1566** — Phishing
- **T1530** — Data from Cloud Storage
- **T1567** — Exfiltration Over Web Service
- **T1213** — Data from Information Repositories
- **T1041** — Exfiltration Over C2 Channel
- **T1078** — Valid Accounts

NIST-800-53R5

- **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-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AC-3** — Access Enforcement

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **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

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.308(a)(5)(i)** — Security Awareness and Training

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
T1598	Phishing for Information	Reconnaissance
T1589.002	Email Addresses	Reconnaissance
T1566	Phishing	Initial-Access
T1530	Data from Cloud Storage	Collection
T1567	Exfiltration Over Web Service	Exfiltration
T1213	Data from Information Repositories	Collection
T1041	Exfiltration Over C2 Channel	Exfiltration
T1078	Valid Accounts	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/pharmaceutical-giant...	T3
Novo Nordisk flags IT security incident - PharmaLive	https://www.pharmalive.com/novo-nordisk-flags-it-security-incident/	T3
Patient information exposed in breach, says Novo Nordisk	https://pharmaphorum.com/news/patient-information-exposed-breach-sa...	T3
Novo Nordisk Cybersecurity Breach Puts Data Controls And Investor ...	https://finance.yahoo.com/sectors/healthcare/articles/novo-nordisk-...	T3

Source	URL	Tier
Report a security vulnerability - Novo Nordisk	https://www.novonordisk.com/contact-us/report-a-security-vulnerabil...	T3

Generated 2026-06-12 14:15 UTC by TJS Security Command Center