Third-Party Risk Assessment Report

Northwind Analytics, Inc. — Patient Outreach Analytics Platform

Assessing organization	Tidewater Regional Health Partners (Vendor Risk Management)
Assessor	Johnny Vaughan, LLC
Vendor	Northwind Analytics, Inc.
Service assessed	Cloud-hosted patient outreach analytics; processes and stores protected health information
Inherent risk tier	Tier 1 — High (PHI processing, cloud-hosted, no compensating segregation)
Assessment type	Full initial assessment, remote
Fieldwork period	March 3 – March 21, 2026
Report date	March 26, 2026
Methodology	NIST SP 800-53 Rev. 5 control subset mapped to the HIPAA Security Rule

1. Assessment conclusion

Northwind Analytics is approved to process protected health information on a conditional basis, subject to remediation of Finding 01 and Finding 02 within the dates agreed in Section 5. Residual risk after planned remediation is assessed as Moderate, which is within the risk tolerance Tidewater has established for Tier 1 vendors.

The vendor maintains a documented information security program with independent attestation and responded to evidence requests without material delay. Two conditions prevent unconditional approval. Administrative access to the production environment does not consistently enforce multifactor authentication, and the vendor's SOC 2 Type II report carves out its infrastructure subservice organization without documenting the complementary controls Tidewater is expected to rely on. Both conditions affect controls that the Business Associate Agreement makes material.

Two additional findings are rated Low and do not gate approval. They are recorded for tracking and will be revalidated at the next assessment cycle.

Risk rating summary

Domain	Controls tested	Exceptions	Domain rating
Access control (AC)	9	2	High

Domain	Controls tested	Exceptions	Domain rating
Audit and accountability (AU)	5	0	Low
System and communications protection (SC)	7	1	Low
Incident response (IR)	6	1	Moderate
Configuration management (CM)	5	0	Low
Supply chain risk management (SR)	4	1	High
Contingency planning (CP)	4	0	Low
Overall	**40**	**5**	**Moderate**

Overall rating reflects the highest-rated open finding adjusted for the vendor's documented remediation commitment, consistent with Tidewater's vendor rating methodology.

2. Scope and methodology

The assessment covered the Northwind Outreach Cloud production environment, the administrative console used by Tidewater staff, and the data flows between Northwind and Tidewater's electronic health record system. Forty controls were selected from NIST SP 800-53 Rev. 5 based on the inherent risk tier and mapped to the corresponding HIPAA Security Rule standards.

Control evaluation followed a four-step sequence: review of vendor-supplied documentation, inspection of supporting evidence, corroborating interviews with control owners, and comparison of the observed control against the requirement. A control was recorded as an exception only where evidence did not support the vendor's assertion, not where documentation was merely absent from the initial response.

Evidence reviewed

Evidence item	Period covered	Source	Sufficiency
SOC 2 Type II report	Jan 1 – Dec 31, 2025	Vendor, via independent CPA firm	Sufficient with exception noted in Finding 02
Information security policy set (11 documents)	Approved Aug 2025	Vendor	Sufficient
Completed security questionnaire (192 items)	Feb 2026	Vendor	Sufficient after two clarification rounds
Penetration test executive summary	Testing Oct 2025	Third-party testing firm	Partial; technical findings detail withheld
Access control configuration export	Feb 2026 snapshot	Vendor	Sufficient; source of Finding 01
Encryption standard and TLS configuration	Feb 2026	Vendor	Sufficient
Incident response plan and test record	Plan Sep 2025; test Nov 2025	Vendor	Sufficient; source of Finding 03
Business continuity test results	Oct 2025	Vendor	Sufficient
Subservice organization attestation	Requested Mar 2026	Not provided	Not received; basis for Finding 02

Interviews conducted

Director of Information Security (March 6), Cloud Infrastructure Lead (March 11), Privacy Officer (March 13), and Customer Success Manager (March 17). Interviews were used to corroborate documentary evidence and to establish how controls operate in practice, not as a substitute for evidence.

Exclusions

This assessment does not constitute an audit opinion, a certification, or an independent attestation. No penetration testing, vulnerability scanning, or technical testing of vendor systems was performed. Conclusions rest on the evidence the vendor provided during the fieldwork period and on interview corroboration. Where evidence was not

provided, that condition is reported as a finding rather than resolved by assumption. The vendor's fourth parties were assessed only to the extent described in Finding 02.

3. Findings

Five control exceptions were identified across 40 controls tested. Findings are rated on likelihood and impact to Tidewater, not on the vendor's internal severity scale. Findings 01 and 02 are conditions of approval.

F-01 Multifactor authentication not enforced for all administrative access — HIGH

Control reference	AC-2, AC-17, IA-2(1) · HIPAA §164.312(d)
Condition	The February 2026 access configuration export identified 4 of 17 administrative accounts in the production environment configured for password-only authentication. Two of the four are named individual accounts belonging to infrastructure engineers; two are shared break-glass accounts. The vendor's own access control policy requires multifactor authentication for all privileged access.
Cause	The vendor migrated to a new identity provider in September 2025. Accounts created before the migration were transferred without enforcement of the new authentication policy, and no reconciliation was performed after cutover.
Risk	Administrative credentials without a second factor are the most common initial access vector in breaches of hosted health data. These accounts can reach Tidewater's PHI. A credential compromise would be reportable under the Business Associate Agreement and would likely constitute a breach under the HIPAA Breach Notification Rule.
Recommendation	Enforce multifactor authentication on all administrative accounts including break-glass accounts, and provide the post-remediation configuration export as closure evidence. Implement a recurring reconciliation of privileged accounts against the authentication policy following any identity provider change.
Vendor owner	Director of Information Security
Agreed remediation date	April 30, 2026

F-02 Subservice organization carved out of SOC 2 scope without complementary control documentation — HIGH

Control reference	SR-3, SR-6, CA-3 · HIPAA §164.308(b)(1)
Condition	The vendor's SOC 2 Type II report applies the carve-out method to its cloud infrastructure provider. The report identifies complementary subservice organization controls but does not describe how Northwind monitors them. No independent attestation for the subservice organization was provided in response to two requests during fieldwork.
Cause	The vendor treats infrastructure provider assurance as satisfied by the provider's public compliance posture and has not established a documented process for obtaining and reviewing that assurance.
Risk	A material portion of the control environment protecting Tidewater PHI sits outside the scope of the only independent attestation available. Tidewater cannot evidence fourth-party oversight to its own regulators or auditors, and the gap is not visible from the SOC 2 report alone.
Recommendation	Provide the current infrastructure provider attestation and a written description of how Northwind reviews it, including who performs the review and on what frequency. Where reliance is placed on complementary controls, document which controls and how their operation is confirmed.
Vendor owner	Director of Information Security
Agreed remediation date	May 31, 2026

F-03 Incident notification timeline in the incident response plan conflicts with the Business Associate Agreement — MODERATE

Control reference	IR-6, IR-8 · HIPAA §164.410
Condition	The vendor's incident response plan commits to customer notification within 72 hours of incident confirmation. The executed Business Associate Agreement requires notification within 24 hours of discovery. The plan has not been updated since the agreement was signed, and the November 2025 tabletop exercise used the 72-hour figure.
Cause	The incident response plan is maintained by the security team and the Business Associate Agreement was negotiated by legal and customer success. No process routes contractual notification commitments into operational procedures.
Risk	In an actual incident the vendor would execute against the plan its responders have practiced. Tidewater would receive notification outside the contractual window, compressing its own breach assessment and notification timeline.
Recommendation	Update the incident response plan to reflect the shortest notification commitment across customer agreements, and exercise the revised timeline in the next tabletop. Establish a review step that reconciles contractual commitments to operational procedures at agreement execution.
Vendor owner	Director of Information Security
Agreed remediation date	June 30, 2026

F-04 Legacy TLS endpoint remains enabled on a deprecated API — LOW

Control reference	SC-8, SC-13 · HIPAA §164.312(e)(1)
Condition	The v1 reporting API accepts TLS 1.1 connections. The vendor's encryption standard requires TLS 1.2 or higher. Vendor telemetry provided during fieldwork shows no Tidewater traffic on this endpoint in the preceding twelve months.
Cause	The endpoint was retained for two legacy customers and excluded from the 2025 TLS hardening effort.
Risk	Limited direct exposure to Tidewater given no observed traffic, but the endpoint reaches the same data store and represents a deviation from the vendor's own standard.
Recommendation	Disable TLS 1.1 on the v1 endpoint, or confirm in writing that the endpoint cannot access Tidewater tenant data.
Vendor owner	Cloud Infrastructure Lead
Agreed remediation date	August 31, 2026

F-05 Security awareness training completion not evidenced for contractors — LOW

Control reference	AT-2, AT-4 · HIPAA §164.308(a)(5)
Condition	Training completion records were provided for employees at 98 percent completion. Contractors with production access are covered by the training policy but were not included in the completion report.
Cause	The learning management system is provisioned from the human resources system, which does not include contractor records.
Risk	Contractors hold the same access as employees. Unevidenced training for that population is a gap in the vendor's ability to demonstrate compliance with its own policy.
Recommendation	Extend training tracking to contractors with production access and provide a completion report covering that population.
Vendor owner	Director of Information Security
Agreed remediation date	August 31, 2026

4. Control evaluation results

Results for the control families where exceptions were identified. Controls tested without exception are summarized by family in Section 1 and available in full on request.

Control	Requirement tested	Result	Reference
AC-2	Account provisioning, review, and deprovisioning are documented and performed	Effective	—
AC-2(1)	Privileged account inventory maintained and reviewed quarterly	Exception	F-01
AC-6	Least privilege applied to production access	Effective	—
AC-17	Remote access to production is controlled and monitored	Effective	—
IA-2(1)	Multifactor authentication enforced for privileged accounts	Exception	F-01
SC-8	Transmission confidentiality enforced in accordance with policy	Exception	F-04
SC-13	Cryptographic modules meet the vendor's published standard	Effective	—
SC-28	Protected health information encrypted at rest	Effective	—
IR-6	Incident notification performed within committed timelines	Exception	F-03
IR-8	Incident response plan maintained and exercised	Effective with observation	F-03
SR-3	Supply chain controls extend to subservice organizations	Exception	F-02
SR-6	Supplier assessments performed and documented	Exception	F-02
AT-2	Security awareness training delivered to all workforce members	Exception	F-05
AU-6	Audit records reviewed for indications of inappropriate activity	Effective	—
CP-4	Contingency plan tested within the last twelve months	Effective	—

5. Remediation plan and closure criteria

Remediation dates below were agreed with the vendor on March 24, 2026. Findings 01 and 02 are conditions of approval; failure to close either by the agreed date returns the vendor to a pending status and triggers escalation under Tidewater's vendor management procedure.

ID	Rating	Closure evidence required	Agreed date	Condition of approval
F-01	High	Post-remediation privileged account configuration export showing multifactor authentication enforced on all 17 accounts	Apr 30, 2026	Yes
F-02	High	Current subservice organization attestation plus written description of the vendor's review process	May 31, 2026	Yes
F-03	Moderate	Revised incident response plan and record of an exercise using the 24-hour timeline	Jun 30, 2026	No
F-04	Low	Configuration evidence that TLS 1.1 is disabled, or written confirmation of tenant isolation	Aug 31, 2026	No
F-05	Low	Training completion report covering contractors with production access	Aug 31, 2026	No

Reassessment

Full reassessment is scheduled for March 2027 consistent with the Tier 1 annual cycle. Closure evidence for each finding will be validated as received rather than deferred to the next cycle, and the vendor risk rating will be recalculated on closure of Findings 01 and 02.

Basis of the residual risk rating

Pre-remediation inherent risk was rated High on the basis of PHI processing volume, administrative access to Tidewater data, and the two High findings. Residual risk of Moderate assumes closure of Findings 01 and 02 on the agreed dates and no change to the service or data flows. If either finding is not closed, residual risk remains High and continued use of the service requires documented acceptance by the data owner and the Privacy Officer.