ÄNDERUNGSANTRAG

ÄNDERUNGSANTRAG

Sicherheitsbewertung & Bereitschaftsvertrag

VON

NULLWIRE SECURITY

500 Yale Ave N, Seattle, WA 98109, United States

AN

MERIDIAN HEALTH SYSTEMS

4400 Forbes Blvd, Columbus, OH 43219, United States

Dieser Änderungsantrag ändert die unten genannte Leistungsbeschreibung. Er wird erst wirksam, sobald beide Parteien ihn unterzeichnet haben.

ÄNDERUNGSANTRAG NR.	DATUM DES INKRAFTTRETENS	ÄNDERT	AUSGESTELLT
CR-2026-0225	16. Februar 2026	SOW-2026-0771	22. Januar 2026

Nullwire Security LLC

Vertraulich — erstellt für Meridian Health Systems. Nicht zur Weitergabe über die genannten Parteien hinaus.

AUF EINEN BLICK

ÄNDERUNGSANTRAG

CR-2026-0225

EINGEREICHT

ÄNDERUNGSANTRAG
CR-2026-0225

EINGEREICHT AM
22. Januar 2026

URSPRÜNGLICHER SOW
SOW-2026-0771 · Portal-Penetrationstest

DRINGLICHKEIT
Hoch

STATUS
EINGEREICHT

EINGEREICHT VON
Nullwire Security, Seattle

ANTWORT ERFORDERLICH BIS
6. März 2026

AUF EINEN BLICK

WAS DIESE ÄNDERUNG BETRIFFT

01
ÄNDERT
SOW-2026-0771
Leistungsbeschreibung

02
ZUSÄTZLICHE GEBÜHR
$94,000
$94,000 zzgl. Umsatzsteuer (wa — professionelle Dienstleistungen befreit)

03
ÜBERARBEITETER VERTRAGSWERT
$111,500
Einschließlich dieser Änderung

04
WIRKSAM AB
16. Februar 2026
Nach Genehmigung durch beide Parteien

05
EINGEREICHT VON
Nullwire Security
Genehmigt von Renata Cole

01

ZUSAMMENFASSUNG DER ÄNDERUNG

Meridian bat um eine Erweiterung des Prüfumfangs auf die Patientenportal-Instanz des kürzlich übernommenen Fairview Medical Center, einschließlich einer zusätzlichen Woche externer Tests und eines zweiten HIPAA-Mapping-Durchlaufs, für eine überarbeitete Gesamtsumme von 111.500 $.

BEGRÜNDUNG

Das Patientenportal von Meridian Health Systems hat sich von einem einfachen Terminplaner zum primären Kanal für Laborergebnisse, Abrechnung und sichere Nachrichten im gesamten Krankenhausnetzwerk entwickelt. Es wird vierteljährlich intern auf bekannte Schwachstellen gescannt, stand jedoch noch nie einem externen Angreifer gegenüber, der kleine Schwachstellen so verkettet, wie es ein echter Angreifer tun würde – und ein durchschnittlicher Datenschutzvorfall im Gesundheitswesen wird immer noch erst nach über 200 Tagen entdeckt.

Nullwire Security schlägt ein achtwöchiges Engagement vor, das einen umfassenden Penetrationstest – extern, intern und Social Engineering – mit einem laufenden Breach-Response-Abonnement kombiniert, sodass Meridian vor einem Vorfall getestet und während eines Vorfalls reaktionsbereit ist. Die folgenden Abschnitte erläutern den Ansatz, den Leistungsumfang, den Zeitplan und die Investition.

DIE HERAUSFORDERUNG

Interne Schwachstellenscans erkennen bekannte CVEs, übersehen jedoch verkettete Exploits, falsch konfigurierte Drittanbieter-Integrationen und die menschlichen Schwachstellen, auf die eine Phishing-Kampagne abzielen würde. Die Labor-Ergebnis-API und die Anbindung des Abrechnungsdienstleisters von Meridian wurden noch nie unabhängig geprüft.

Operativ wurden Erkennung und Reaktion noch nie anhand eines realen Szenarios geprobt. Käme es tatsächlich zu einem Sicherheitsvorfall, wäre der vorliegende Incident-Response-Plan ungetestet, und dem Team ist nicht bekannt, wie lange die Eindämmung tatsächlich dauern würde.

UNSER ANSATZ

Wir führen das Engagement so durch, wie es ein echter Angreifer tun würde: externe Aufklärung und Exploitation, laterale Bewegung von einem simulierten kompromittierten Endpunkt aus sowie eine Social-Engineering-Kampagne gegen den Helpdesk, ergänzt durch eine gezielte Prüfung der beiden Drittanbieter-Integrationen, über die Patientendaten laufen.

Die Ergebnisse werden direkt der HIPAA Security Rule zugeordnet und mit einem Nachtest zur Behebung zurückgegeben, sodass nichts als abgeschlossen markiert wird, bevor die Behebung verifiziert ist. Das Breach-Response-Abonnement hält anschließend dasselbe Team einsatzbereit, sodass der nächste Vorfall geprobt statt improvisiert abläuft.

POSITION	ÄNDERUNG (HINZUFÜGEN/ENTFERNEN/ÄNDERN)	BESCHREIBUNG
Umfang	1 Patientenportal-Instanz (Meridian-Hauptsitz)	2 Patientenportal-Instanzen (Meridian-Hauptsitz + Fairview Medical Center)
Externe Tests	2 Wochen	3 Wochen (+1 Woche)
Geprüfte Drittanbieter-Integrationen	2 Integrationen	3 Integrationen (+1 Abrechnungs-Gateway)
Auftragsgebühr	$94,000	111.500 $ (+17.500 $)
Lieferung des Abschlussberichts	Woche 8	Woche 9 (+1 Woche)

[01] ▸ WOCHEN 1–2 · SCOPING & AUFKLÄRUNG

Regeln des Engagements, Erfassung der Assets und Mapping der Angriffsfläche.

[02] ▸ WOCHEN 3–5 · AKTIVE TESTS

Externe, interne und Social-Engineering-Tests gemäß vereinbartem Umfang.

[03] ▸ WOCHE 6 · ERGEBNISSE & HIPAA-MAPPING

Konsolidierung der Ergebnisse und Zuordnung zu den relevanten Schutzmaßnahmen der HIPAA Security Rule.

[04] ▸ WOCHE 7 · UNTERSTÜTZUNG BEI DER BEHEBUNG

Begleitete Unterstützung des Engineering-Teams bei der Behebung vor dem Nachtest.

TÄTIGKEIT	STUNDEN	SATZ	BETRAG
Scoping & Aufklärung Regeln des Engagements, Erfassung der Assets und Mapping der Angriffsfläche	2	$9,500 / wk	$19,000
Externer Penetrationstest Bewertung des internetzugänglichen Patientenportals und der API	2	$14,000 / wk	$28,000
Interne & Social-Engineering-Tests Simuliertes Szenario mit kompromittiertem Endpunkt und Phishing-Übung	1	$16,000 / wk	$16,000
Prüfung der Drittanbieter-Integrationen Sicherheitsbewertung der API von Labor-Ergebnis- und Abrechnungsdienstleistern	1	$12,000 / wk	$12,000
Berichterstattung & Unterstützung bei der Behebung Ergebnisbericht, HIPAA-Mapping und Anleitung zur Behebung	1	$10,000 / wk	$10,000
Zusätzliche Gebühr			**$94,000**

URSPRÜNGLICHER VERTRAGSWERT (SOW-2026-0771) $94,000

ZUSÄTZLICHE GEBÜHR (DIESER ÄNDERUNGSANTRAG)	$94,000
NEUE GESAMTSUMME	$111,500

NEUE GESAMTSUMME **$111,500**

Alle Beträge verstehen sich in USD und exklusive anfallender Steuern. Die zusätzliche Gebühr wird gemäß dem Meilensteinplan des ursprünglichen SOW abgerechnet: 50 % bei Genehmigung dieser Änderung und 50 % beim Go-Live.

ZAHLUNGSPLAN

FÄLLIGKEIT DER EINZELNEN RATEN

NR.	MEILENSTEIN	AUSLÖSER	ANTEIL	BETRAG
01	Wochen 1–2 · Scoping & Aufklärung	16. Februar 2026	50%	$47,000
02	Wochen 3–5 · Aktive Tests	Bei Lieferbeginn	50%	$47,000
Gesamt (netto)			**100%**	**$94,000**

Die Raten werden entsprechend den oben genannten Meilensteinen in Rechnung gestellt und sind innerhalb von 30 Tagen nach Rechnungsdatum fällig. Alle Beträge verstehen sich in USD zzgl. Umsatzsteuer (wa — professionelle Dienstleistungen befreit).

ANNAHMEN UND GENEHMIGUNGSBEDINGUNGEN

Testkonten und ein unterschriebenes Schreiben zu den Regeln des Engagements werden vor Testbeginn bereitgestellt; ein Stakeholder ist befugt, Änderungen am Umfang bei jeder Phase zu genehmigen; und die Tests beschränken sich auf das Patientenportal und seine beiden benannten Drittanbieter-Integrationen. Änderungen daran wirken sich auf Zeitplan und Kosten aus, worüber wir vor der Umsetzung schriftlich Einvernehmen herstellen würden. Das Honorar gilt für Engagements, die bis zum 6. März 2026 beginnen.

Mit der Unterschrift unten werden der Umfang, der überarbeitete Zeitplan und die zusätzliche Gebühr dieses Änderungsantrags genehmigt, und die entsprechende Änderung des ursprünglichen Leistungsverzeichnisses wird autorisiert.

FÜR MERIDIAN HEALTH SYSTEMS

RENATA COLE
CHIEF INFORMATION SECURITY OFFICER

Datum

FÜR NULLWIRE SECURITY

NULLWIRE SECURITY
BEVOLLMÄCHTIGTER UNTERZEICHNER

Datum

NULLWIRE SECURITY

500 Yale Ave N, Seattle, WA 98109, United States
contact@nullwiresecurity.com · +1 206 555 0189 · nullwiresecurity.com
Nullwire Security LLC · EIN 91-4820376