NULLWIRE SECURITY

PRÉPARÉ POUR MERIDIAN HEALTH SYSTEMS

Cahier des charges

Une évaluation en équipe rouge à périmètre complet du portail patient, adossée à un contrat de réponse aux violations — conçue pour une infrastructure soumise à la réglementation HIPAA.

2026

SOMMAIRE

EN BREF

CAHIER DES CHARGES

SOW-2026-0771

BROUILLON

PRÉPARÉ POUR
Meridian Health Systems — Renata Cole, Directrice de la sécurité des systèmes d'information

PRÉPARÉ PAR
Nullwire Security, Seattle

NUMÉRO DU CAHIER DES CHARGES
SOW-2026-0771

DATE DE DÉBUT
16 février 2026

DURÉE
Évaluation de sécurité et

abonnement de veille

STATUT

Brouillon — pour révision

EN BREF

PÉRIMÈTRE, CALENDRIER ET HONORAIRES

01
FLUX DE TRAVAIL

Évaluation de sécurité et abonnement de veille

Une évaluation en équipe rouge à périmètre complet du portail patient, adossée à un contrat de réponse aux violations — conçue pour une infrastructure soumise à la réglementation HIPAA.

02
DÉBUT

16 février 2026

À la contresignature

03
DURÉE

12 mois

Échelonné selon le calendrier ci-dessous

04
HONORAIRES

$94,000

$94,000, plus taxe de vente (wa — services professionnels exonérés)

05
ACCEPTÉ PAR

Renata Cole

Directrice de la sécurité des systèmes d'information

01

APERÇU ET OBJECTIFS

Une mission de huit semaines associant un test d'intrusion complet à un abonnement permanent de réponse aux incidents, afin que Meridian Health Systems soit testé avant un incident et prêt à réagir pendant celui-ci.

CONTEXTE ET OBJECTIFS

Le portail patient de Meridian Health Systems, initialement un simple planificateur de rendez-vous, est devenu le canal principal pour les résultats de laboratoire, la facturation et la messagerie sécurisée dans l'ensemble de son réseau hospitalier. Il fait l'objet d'analyses internes trimestrielles des vulnérabilités connues, mais il n'a jamais fait face à un adversaire externe capable d'enchaîner de petites faiblesses comme le ferait un véritable attaquant — et le délai moyen de détection d'une violation de données dans le secteur de la santé dépasse toujours 200 jours.

Nullwire Security propose une mission de huit semaines combinant un test d'intrusion à périmètre complet — externe, interne et d'ingénierie sociale — avec un contrat de réponse aux violations permanent, afin que Meridian soit testé avant un incident et prêt à réagir pendant celui-ci. Les sections suivantes présentent la démarche, le périmètre, le calendrier et l'investissement.

LIVRABLES

[01] TESTS

RAPPORT DE TEST D'INTRUSION COMPLET

Constats externes, internes et de mouvement latéral, avec détail des preuves de concept et notation de gravité.

[02] TESTS

ÉVALUATION D'INGÉNIERIE SOCIALE

Résultats des tests de phishing et de manipulation du support technique, avec recommandations de sensibilisation destinées au personnel.

[03] RÉPONSE

PLAN D'INTERVENTION EN CAS DE VIOLATION

Un plan de réponse aux incidents répété, avec rôles définis, filières d'escalade et ligne d'astreinte Nullwire.

[04] CONFORMITÉ

RAPPORT DE CONSTATS CARTOGRAPHIÉ SUR LA NORME HIPAA

Chaque constat rattaché à la mesure de sécurité HIPAA correspondante, prêt pour un audit.

[05] LIVRAISON TECHNIQUE

NOUVEAU TEST DE REMÉDIATION ET VALIDATION

Un nouveau test vérifiant que chaque constat a été corrigé, avec validation écrite.

HORS PÉRIMÈTRE

- Tests d'intrusion physique des installations au-delà des deux centres de données nommés
- Audit du code source des applications de fournisseurs tiers
- Surveillance SOC continue 24 h/24 et 7 j/7 au-delà de la plage d'astreinte de l'abonnement
- Dépôts réglementaires et conseil juridique en notification de violation de données

[01]

DES TESTS AU NIVEAU D'UN VÉRITABLE ADVERSAIRE

Tests externes, internes et d'ingénierie sociale menés selon un enchaînement digne d'un véritable attaquant.

[02]

RAPPORT CARTOGRAPHIÉ SUR LA HIPAA

Chaque constat rattaché à la mesure de sécurité HIPAA correspondante, prêt pour l'audit et le reporting au conseil d'administration.

[03]

UNE RÉPONSE DISPONIBLE EN PERMANENCE

Un plan de réponse aux incidents rodé et une astreinte permanente, pour que le prochain incident soit maîtrisé, pas improvisé.

SPÉCIFICATION

SPÉCIFICATION DU FLUX DE TRAVAIL

RÉF.	ÉLÉMENT	SPÉCIFICATION	CHARGE DE TRAVAIL	DÉLAI	PRIX UNITAIRE
SPC-01	Cadrage et reconnaissance	Règles d'engagement, recensement des actifs et cartographie de la surface d'attaque	2	2 sem.	$9,500 / wk
SPC-02	Test d'intrusion externe	Évaluation du portail patient et de l'API exposés sur Internet	2	2 sem.	$14,000 / wk
SPC-03	Tests internes et d'ingénierie sociale	Scénario de poste compromis simulé et exercice de phishing	1	1 sem.	$16,000 / wk
SPC-04	Examen des intégrations tierces	Évaluation de la sécurité des API des résultats de laboratoire et du prestataire de facturation	1	1 sem.	$12,000 / wk
SPC-05	Rapport et accompagnement à la correction	Rapport de constats, cartographie HIPAA et recommandations de correction	1	1 sem.	$10,000 / wk

Les spécifications sont fixées à l'acceptation ; tout changement est traité selon la procédure de contrôle des modifications définie dans le présent document.

[01] ▸ SEMAINES 1 À 2 · CADRAGE ET RECONNAISSANCE

Règles d'engagement, recensement des actifs et cartographie de la surface d'attaque.

[02] ▸ SEMAINES 3 À 5 · TESTS ACTIFS

Tests externes, internes et d'ingénierie sociale sur le périmètre convenu.

[03] ▸ SEMAINE 6 · CONSTATS ET CARTOGRAPHIE HIPAA

Consolidation des constats et mise en correspondance avec les mesures de sauvegarde pertinentes de la HIPAA Security Rule.

[04] ▸ SEMAINE 7 · ACCOMPAGNEMENT À LA CORRECTION

Accompagnement guidé de l'équipe d'ingénierie pour la correction avant nouveau test.

[05] ▸ SEMAINE 8 · NOUVEAU TEST ET ACTIVATION DU CONTRAT DE MAINTENANCE

Nouveau test de vérification des correctifs et remise du manuel de réponse aux incidents.

CRITÈRES D'ACCEPTATION

RÉF.	EXIGENCE	PRIORITÉ
R-01	Les tests externes et internes doivent inclure le portail patient et ses deux intégrations tierces nommées	OBLIGATOIRE
R-02	Comptes de test et lettre de règles d'engagement signée fournis avant le début des tests	OBLIGATOIRE
R-03	Toutes les constatations associées à la mesure de sauvegarde HIPAA Security Rule concernée	OBLIGATOIRE
R-04	Constatations critiques et élevées retestées et vérifiées comme résolues avant la validation finale	OBLIGATOIRE
R-05	Campagne d'ingénierie sociale limitée au service d'assistance et aux services nommés	OBLIGATOIRE

FLUX DE TRAVAIL	SEMAINES	TAUX	MONTANT
Cadrage et reconnaissance Règles d'engagement, recensement des actifs et cartographie de la surface d'attaque	2	$9,500 / wk	$19,000
Test d'intrusion externe Évaluation du portail patient et de l'API exposés sur Internet	2	$14,000 / wk	$28,000

Tests internes et d'ingénierie sociale Scénario de poste compromis simulé et exercice de phishing	1	$16,000 / wk	$16,000
Examen des intégrations tierces Évaluation de la sécurité des API des résultats de laboratoire et du prestataire de facturation	1	$12,000 / wk	$12,000
Rapport et accompagnement à la correction Rapport de constats, cartographie HIPAA et recommandations de correction	1	$10,000 / wk	$10,000
Sous-total des honoraires			**$94,000**

HONORAIRES	$94,000
TAXE DE VENTE (WA – SERVICES PROFESSIONNELS EXONÉRÉS)	$0
TOTAL	$94,000

TOTAL **$94,000**

Tous les montants sont en USD et hors taxes applicables. Les honoraires sont facturés en trois jalons : 40 % à la signature, 30 % au début de la réalisation, 30 % à la mise en production.

ÉCHÉANCIER DE PAIEMENT

ÉCHÉANCE DE CHAQUE VERSEMENT

N°	JALON	DÉCLENCHEUR	PART	MONTANT
01	Semaines 1 à 2 · Cadrage et reconnaissance	16 février 2026	40%	$37,600

02	Semaines 3 à 5 · Tests actifs	Au démarrage de la livraison	30%	$28,200
03	Semaine 6 · Constats et cartographie HIPAA	À l'acceptation du jalon	30%	$28,200
Total (HT)			**100%**	**$94,000**

Les échéances sont facturées au fur et à mesure des jalons ci-dessus et sont payables dans les 30 jours suivant chaque facture. Tous les montants sont exprimés en USD et s'entendent hors taxe de vente (wa — services professionnels exonérés).

La contresignature ci-dessous entérine le périmètre, le calendrier, les critères d'acceptation et les honoraires définis dans ce cahier des charges, et autorise le début des travaux à la date de début indiquée.

POUR MERIDIAN HEALTH SYSTEMS

RENATA COLE

DIRECTRICE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

Date

POUR NULLWIRE SECURITY

NULLWIRE SECURITY

SIGNATAIRE AUTORISÉ

Date

NULLWIRE SECURITY

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