NULLWIRE SECURITY

NULLWIRE SECURITY — ÉVALUATION DE SÉCURITÉ ET PRESTATION D'ABONNEMENT

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

CONTRÔLE DOCUMENTAIRE

01 SPÉCIFICATION
REQ-2026-0771
Émis le 22 janvier 2026

02 PRÉPARÉ PAR
Nullwire Security
Seattle, WA 98109

03 PROPRIÉTAIRE
Renata Cole
Directeur de la sécurité des systèmes d'information, Meridian Health Systems

04 STATUT
Pour révision
Version de référence figée à l'approbation

05 EXIGENCES
8
Fonctionnelles et non fonctionnelles

01

INTRODUCTION ET PÉRIMÈTRE

Le portail patient de Meridian Health Systems héberge désormais les résultats de laboratoire, la facturation et la messagerie de 340 000 patients — et n'a jamais fait l'objet d'une évaluation externe par une équipe de red team. Voici le plan pour le tester rigoureusement, et pour être prêt si une faille venait à être exploitée.

OBJET ET PUBLIC VISÉ

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.

EXIGENCES FONCTIONNELLES

ID	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
R-06	Le manuel de réponse aux incidents inclut des rôles définis et un SLA d'activation de 4 heures	SOUHAITABLE
R-07	Aucune donnée patient de production exfiltrée ni conservée au-delà de captures d'écran de preuve de concept	OBLIGATOIRE
R-08	Rapport final livré en formats détaillés exécutif et technique	SOUHAITABLE

ID	PRIORITÉ	EXIGENCE
R-01	Obligatoire	Les tests externes et internes doivent inclure le portail patient et ses deux intégrations tierces nommées
R-02	Obligatoire	Comptes de test et lettre de règles d'engagement signée fournis avant le début des tests
R-03	Obligatoire	Toutes les constatations associées à la mesure de sauvegarde HIPAA Security Rule concernée
R-04	Obligatoire	Constatations critiques et élevées retestées et vérifiées comme résolues avant la validation finale

R-05	Obligatoire	Campagne d'ingénierie sociale limitée au service d'assistance et aux services nommés

01

TEST D'INTRUSION EXTERNE

Actifs exposés sur Internet, le portail patient et ses API publiques, testés jusqu'à l'exploitation.

02

MOUVEMENT LATÉRAL ET INTERNE

Un scénario simulé de terminal compromis, testant jusqu'où un attaquant pourrait se déplacer une fois à l'intérieur.

03

INGÉNIERIE SOCIALE

Une simulation d'hameçonnage et une campagne de prétexte auprès du service d'assistance visant le personnel.

04

EXAMEN DES INTÉGRATIONS TIERCES

Évaluation de sécurité des connexions API avec les prestataires de résultats de laboratoire et de facturation.

05

FORFAIT DE RÉPONSE AUX INCIDENTS

Réponse aux incidents sur appel et un plan d'intervention répété et prêt à exécuter.

06

RAPPORTS DE CONFORMITÉ

Constats directement rattachés à la règle de sécurité HIPAA pour l'audit et le reporting au conseil d'administration.

SPÉCIFICATION

SPÉCIFICATION DES COMPOSANTS

RÉF.	ÉLÉMENT	SPÉCIFICATION	UNITÉS	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
SPC-06	Contre-test et mise en place de la maintenance	Contre-test de vérification des correctifs et transmission du plan d'intervention en cas d'incident	1	1 sem.	$9,000 / 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]

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.

[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.

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