NULLWIRE SECURITY

NULLWIRE SECURITY — EVALUACIÓN DE SEGURIDAD Y RETENEDOR

Especificación de Requisitos

Una evaluación de equipo rojo de alcance completo del portal de pacientes, respaldada por un contrato de retención para respuesta a brechas — diseñada para infraestructura regulada por HIPAA.

2026

CONTENIDO

DE UN VISTAZO

CONTROL DE DOCUMENTOS

01
ESPECIFICACIÓN
REQ-2026-0771
Emitido el 22 de enero de 2026

02
PREPARADO POR
Nullwire Security
Seattle, WA 98109

03
PROPIETARIA
Renata Cole
Director de Seguridad de la Información, Meridian Health Systems

04
ESTADO
Para revisión
Línea base fijada en la aprobación

05
REQUISITOS
8
Funcionales y no funcionales

01

INTRODUCCIÓN Y ALCANCE

El portal de pacientes de Meridian Health Systems gestiona hoy resultados de laboratorio, facturación y mensajería para 340 000 pacientes, y nunca ha sido sometido a una evaluación externa de red team. Este es el plan para ponerlo a prueba como corresponde y estar preparados si algo llega a filtrarse.

PROPÓSITO Y PÚBLICO

El portal de pacientes de Meridian Health Systems ha pasado de ser un programador de citas a convertirse en el canal principal para resultados de laboratorio, facturación y mensajería segura en toda su red hospitalaria. Se ha escaneado internamente en busca de vulnerabilidades conocidas cada trimestre, pero nunca ha enfrentado a un adversario externo que encadene pequeñas debilidades de la manera en que lo haría un atacante real, y la brecha de salud promedio todavía tarda más de 200 días en detectarse.

Nullwire Security propone un compromiso de ocho semanas que combina una prueba de penetración de alcance completo — externa, interna e ingeniería social — con un contrato de retención permanente para respuesta a brechas, de modo que Meridian sea evaluado antes de un incidente y esté listo para responder durante uno. Las siguientes secciones exponen el enfoque, el alcance, el cronograma y la inversión.

REQUISITOS FUNCIONALES

ID	REQUISITO	PRIORIDAD
R-01	Las pruebas externas e internas deben incluir el portal de pacientes y sus dos integraciones de terceros nombradas	OBLIGATORIO
R-02	Cuentas de prueba y una carta firmada de reglas de compromiso proporcionadas antes de iniciar las pruebas	OBLIGATORIO
R-03	Todos los hallazgos asignados a la salvaguarda correspondiente de la Regla de Seguridad de HIPAA	OBLIGATORIO

R-04	Hallazgos críticos y altos vueltos a probar y verificados como cerrados antes de la aprobación final	OBLIGATORIO
R-05	Campaña de ingeniería social limitada a la mesa de ayuda y departamentos nombrados	OBLIGATORIO
R-06	El manual de respuesta a brechas incluye roles definidos y un SLA de activación de 4 horas	DESEABLE
R-07	Ningún dato de paciente en producción exfiltrado o retenido más allá de capturas de pantalla de prueba de concepto	OBLIGATORIO
R-08	Informe final entregado en formatos tanto ejecutivo como técnico detallado	DESEABLE

ID	PRIORIDAD	REQUISITO
R-01	Obligatorio	Las pruebas externas e internas deben incluir el portal de pacientes y sus dos integraciones de terceros nombradas
R-02	Obligatorio	Cuentas de prueba y una carta firmada de reglas de compromiso proporcionadas antes de iniciar las pruebas
R-03	Obligatorio	Todos los hallazgos asignados a la salvaguarda correspondiente de la Regla de Seguridad de HIPAA
R-04	Obligatorio	Hallazgos críticos y altos vueltos a probar y verificados como cerrados antes de la aprobación final
R-05	Obligatorio	Campaña de ingeniería social limitada a la mesa de ayuda y departamentos nombrados

01
PRUEBA DE PENETRACIÓN EXTERNA

Activos expuestos a internet, el portal de pacientes y sus API públicas, evaluados hasta la explotación.

02
MOVIMIENTO INTERNO Y LATERAL

Un escenario simulado de endpoint comprometido, evaluando hasta dónde podría desplazarse un atacante una vez dentro.

03
INGENIERÍA SOCIAL

Una simulación de phishing y una campaña de pretexting de mesa de ayuda dirigida al personal.

04
REVISIÓN DE INTEGRACIONES DE TERCEROS

Evaluación de seguridad de las conexiones API con los proveedores de resultados de laboratorio y facturación.

05
RETAINER DE RESPUESTA ANTE BRECHAS

Respuesta a incidentes disponible bajo demanda y un manual de respuesta ensayado y listo para ejecutarse.

06
INFORMES DE CUMPLIMIENTO

Hallazgos vinculados directamente con la Regla de Seguridad de HIPAA para auditoría e informes a la junta directiva.

ESPECIFICACIÓN

ESPECIFICACIÓN DE COMPONENTES

REF.	ÍTEM	ESPECIFICACIÓN	UNIDADES	PLAZO	PRECIO UNITARIO
SPC-01	Alcance y reconocimiento	Reglas de compromiso, enumeración de activos y mapeo de la superficie de ataque	2	2 sem.	$9,500 / wk
SPC-02	Prueba de penetración externa	Evaluación del portal de pacientes y la API expuestos a internet	2	2 sem.	$14,000 / wk

SPC-03	Pruebas internas y de ingeniería social	Escenario simulado de endpoint comprometido y ejercicio de phishing	1	1 sem.	$16,000 / wk
SPC-04	Revisión de integraciones de terceros	Evaluación de seguridad de la API de resultados de laboratorio y del proveedor de facturación	1	1 sem.	$12,000 / wk
SPC-05	Informes y apoyo a la remediación	Informe de hallazgos, mapeo HIPAA y guía de remediación	1	1 sem.	$10,000 / wk
SPC-06	Reprueba y configuración de retención	Reprueba de verificación de correcciones y entrega del manual de respuesta ante brechas	1	1 sem.	$9,000 / wk

Las especificaciones quedan fijadas en el momento de la aceptación; cualquier cambio se gestiona mediante el procedimiento de control de cambios establecido en este documento.

[01]

PRUEBAS DE NIVEL ADVERSARIO

Pruebas externas, internas y de ingeniería social ejecutadas de la forma en que un atacante real las encadenaría.

[02]

INFORMES MAPEADOS A HIPAA

Cada hallazgo mapeado a la salvaguarda correspondiente de la Regla de Seguridad de HIPAA, listo para auditoría e informes a la junta.

[03]

RESPUESTA PERMANENTE

Un manual de respuesta a brechas ensayado y una retención de guardia permanente, para que el próximo incidente esté ensayado, no improvisado.

[01] ▸ SEMANAS 1–2 · ALCANCE Y RECONOCIMIENTO

Reglas de compromiso, enumeración de activos y mapeo de la superficie de ataque.

[02] ▸ SEMANAS 3–5 · PRUEBAS ACTIVAS

Pruebas externas, internas y de ingeniería social contra el alcance acordado.

[03] ▸ SEMANA 6 · HALLAZGOS Y MAPEO HIPAA

Consolidación de hallazgos y mapeo a las salvaguardas relevantes de la Regla de Seguridad de HIPAA.

[04] ▸ SEMANA 7 · APOYO A LA REMEDIACIÓN

Apoyo guiado en la remediación para el equipo de ingeniería antes de la reprueba.

NULLWIRE SECURITY

500 Yale Ave N, Seattle, WA 98109,
Estados Unidos

contact@nullwiresecurity.com · +1 206 555 0189 · nullwiresecurity.com

Nullwire Security LLC · EIN 91-4820376