NULLWIRE SECURITY

NULLWIRE SECURITY — AVALIAÇÃO DE SEGURANÇA E CONTRATO DE RETENÇÃO

Especificação de Requisitos

Uma avaliação red-team de escopo completo do portal do paciente, apoiada por um contrato de resposta a violações — desenvolvida para infraestrutura regulada pela HIPAA.

2026

SUMÁRIO

RESUMO GERAL

CONTROLE DE DOCUMENTOS

01
ESPECIFICAÇÃO
REQ-2026-0771
Emitido em 22 de janeiro de 2026

02
PREPARADO POR
Nullwire Security
Seattle, WA 98109

03
PROPRIETÁRIA
Renata Cole
Diretor de Segurança da Informação, Meridian Health Systems

04
STATUS
Para revisão
Linha de base definida na aprovação

05
REQUISITOS
8
Funcionais e não funcionais

01

INTRODUÇÃO E ESCOPO

O portal do paciente da Meridian Health Systems agora reúne resultados de exames, faturamento e mensagens de 340.000 pacientes — e nunca passou por uma avaliação externa de red team. Este é o plano para testá-lo de forma adequada e estar preparado caso algo passe despercebido.

OBJETIVO E PÚBLICO-ALVO

O portal do paciente da Meridian Health Systems evoluiu de um agendador de consultas para o principal canal de resultados de exames, faturamento e mensagens seguras em toda a sua rede hospitalar. Ele é escaneado internamente em busca de vulnerabilidades conhecidas a cada trimestre, mas nunca enfrentou um adversário externo que encadeia pequenas fraquezas da forma como um atacante real faria — e o tempo médio para detectar uma violação de dados na área da saúde ainda ultrapassa 200 dias.

A Nullwire Security propõe um projeto de oito semanas que combina um teste de invasão de escopo completo — externo, interno e de engenharia social — com um contrato permanente de resposta a violações, para que a Meridian seja testada antes de um incidente e esteja pronta para responder durante um.

As seções a seguir apresentam a abordagem, o escopo, o cronograma e o investimento.

REQUISITOS FUNCIONAIS

ID	REQUISITO	PRIORIDADE
R-01	Os testes externos e internos devem incluir o portal do paciente e suas duas integrações nomeadas de terceiros	OBRIGATÓRIO
R-02	Contas de teste e uma carta assinada de regras de engajamento fornecidas antes do início dos testes	OBRIGATÓRIO

R-04	Descobertas críticas e altas retestadas e verificadas como resolvidas antes da aprovação final	OBRIGATÓRIO
R-05	Campanha de engenharia social limitada à central de atendimento e aos departamentos nomeados	OBRIGATÓRIO
R-06	Runbook de resposta a violações inclui funções definidas e um SLA de ativação de 4 horas	DESEJÁVEL
R-07	Nenhum dado de paciente em produção exfiltrado ou retido além de capturas de tela de prova de conceito	OBRIGATÓRIO
R-08	Relatório final entregue em formatos executivo e técnico detalhado	DESEJÁVEL

ID	PRIORIDADE	REQUISITO
R-01	Obrigatório	Os testes externos e internos devem incluir o portal do paciente e suas duas integrações nomeadas de terceiros
R-02	Obrigatório	Contas de teste e uma carta assinada de regras de engajamento fornecidas antes do início dos testes
R-03	Obrigatório	Todas as descobertas mapeadas para a salvaguarda relevante da Regra de Segurança da HIPAA
R-04	Obrigatório	Descobertas críticas e altas retestadas e verificadas como resolvidas antes da aprovação final

R-05	Obrigatório	Campanha de engenharia social limitada à central de atendimento e aos departamentos nomeados

01
TESTE DE INVASÃO EXTERNO

Ativos voltados para a internet, o portal do paciente e suas APIs públicas, testados até a exploração.

02
MOVIMENTO INTERNO E LATERAL

Um cenário simulado de endpoint comprometido, testando até onde um invasor poderia se mover uma vez dentro da rede.

03
ENGENHARIA SOCIAL

Uma simulação de phishing e uma campanha de pretexting de help desk contra a equipe.

04
REVISÃO DE INTEGRAÇÕES DE TERCEIROS

Avaliação de segurança das conexões de API com fornecedores de resultados laboratoriais e faturamento.

05
CONTRATO DE RESPOSTA A VIOLAÇÕES

Resposta a incidentes sob demanda e um runbook de RI ensaiado e pronto para execução.

06
RELATÓRIO DE CONFORMIDADE

Achados mapeados diretamente para a HIPAA Security Rule, para auditoria e relatórios à diretoria.

ESPECIFICAÇÃO

ESPECIFICAÇÃO DE COMPONENTES

SPC-02	Teste de invasão externo	Avaliação do portal do paciente e da API expostos à internet	2	2 sem.	$14,000 / wk
SPC-03	Testes internos e de engenharia social	Cenário simulado de endpoint comprometido e exercício de phishing	1	1 sem.	$16,000 / wk
SPC-04	Revisão de integrações de terceiros	Avaliação de segurança das APIs de resultados de exames e do fornecedor de faturamento	1	1 sem.	$12,000 / wk
SPC-05	Relatório e suporte à correção	Relatório de achados, mapeamento HIPAA e orientação de correção	1	1 sem.	$10,000 / wk
SPC-06	Reteste e configuração de retenção	Reteste de verificação de correções e entrega do manual de resposta a violações	1	1 sem.	$9,000 / wk

As especificações são fixadas no momento da aceitação; qualquer alteração é tratada por meio do processo de controle de mudanças definido neste documento.

[01]

TESTES EM NÍVEL DE ADVERSÁRIO REAL

Testes externos, internos e de engenharia social executados da forma como um atacante real os encadearia.

[02]

RELATÓRIO MAPEADO À HIPAA

Cada achado mapeado à salvaguarda correspondente da HIPAA Security Rule, pronto para auditoria e relatórios ao conselho.

[03]

RESPOSTA SEMPRE ATIVA

Um manual de resposta a violações ensaiado e um contrato de plantão, para que o próximo incidente seja ensaiado, não improvisado.

[01] ▸ SEMANAS 1–2 · DEFINIÇÃO DE ESCOPO E RECONHECIMENTO

Regras de engajamento, inventário de ativos e mapeamento da superfície de ataque.

[02] ▸ SEMANAS 3–5 · TESTES ATIVOS

Testes externos, internos e de engenharia social conforme o escopo acordado.

[03] ▸ SEMANA 6 · ACHADOS E MAPEAMENTO HIPAA

Achados consolidados e mapeados às salvaguardas relevantes da HIPAA Security Rule.

[04] ▸ SEMANA 7 · SUPORTE À CORREÇÃO

Suporte orientado à correção para a equipe de engenharia antes do reteste.

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