SOLICITAÇÃO DE ALTERAÇÃO

SOLICITAÇÃO DE ALTERAÇÃO

Avaliação de Segurança e Contrato de Retenção

DE

NULLWIRE SECURITY

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

PARA

MERIDIAN HEALTH SYSTEMS

4400 Forbes Blvd, Columbus, OH 43219,
United States

Esta solicitação de mudança altera o escopo de trabalho referenciado abaixo. Ela só entra em vigor depois que ambas as partes a assinarem.

SOLICITAÇÃO DE MUDANÇA Nº	DATA DE VIGÊNCIA	ALTERA	EMITIDO
CR-2026-0225	16 de fevereiro de 2026	SOW-2026-0771	22 de janeiro de 2026

Nullwire Security LLC

RESUMO GERAL

SOLICITAÇÃO DE ALTERAÇÃO

CR-2026-0225

ENVIADO

SOLICITAÇÃO DE ALTERAÇÃO	DATA DE ABERTURA	SOW DE ORIGEM	URGÊNCIA
CR-2026-0225	22 de janeiro de 2026	SOW-2026-0771 · Teste de Invasão do Portal	Alta

STATUS	SOLICITADO POR	RESPOSTA NECESSÁRIA ATÉ
ENVIADO	Nullwire Security, Seattle	6 de março de 2026

RESUMO GERAL

O QUE ESTA MUDANÇA ALTERA

01 ALTERA
SOW-2026-0771
Escopo de trabalho

02 TAXA ADICIONAL
$94,000
$94,000, mais imposto sobre vendas (wa — serviços profissionais isentos)

03 VALOR REVISADO DO CONTRATO
$111,500
Incluindo esta mudança

04 VIGÊNCIA
16 de fevereiro de 2026
Mediante aprovação de ambas as partes

05 SOLICITADO POR
Nullwire Security
Aprovado por Renata Cole

01

RESUMO DA ALTERAÇÃO

A Meridian solicitou a expansão do escopo da avaliação para incluir a instância do portal do paciente do recém-adquirido Fairview Medical Center, adicionando uma semana de testes externos e uma segunda rodada de mapeamento HIPAA, totalizando um valor revisado de $111,500.

JUSTIFICATIVA

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.

O DESAFIO

As varreduras internas de vulnerabilidade detectam CVEs conhecidas, mas não identificam explorações encadeadas, integrações de terceiros mal configuradas nem os pontos fracos humanos que uma campanha de phishing exploraria. A API de resultados de exames da Meridian e a conexão com o fornecedor de faturamento nunca foram avaliadas de forma independente.

Operacionalmente, a detecção e a resposta nunca foram ensaiadas em um cenário real. Se ocorresse uma violação, o plano de resposta a incidentes registrado nunca foi testado, e a equipe não sabe, na prática, quanto tempo levaria a contenção.

NOSSA ABORDAGEM

Conduzimos o projeto como um adversário real faria: reconhecimento e exploração externos, movimentação lateral a partir de um endpoint comprometido simulado, e uma campanha de engenharia social contra a central de atendimento, somados a uma revisão dedicada das duas integrações de terceiros que carregam dados de pacientes.

Os achados são mapeados diretamente à HIPAA Security Rule e devolvidos com um reteste de correção, de modo que nada seja marcado como resolvido até que a correção seja verificada. O contrato de resposta a violações mantém então essa mesma equipe de plantão, para que o próximo incidente seja ensaiado, não improvisado.

ITEM	ALTERAÇÃO (ADICIONAR/REMOVER/MODIFICAR)	DESCRIÇÃO
Escopo	1 instância do portal do paciente (sede da Meridian)	2 instâncias do portal do paciente (sede da Meridian + Fairview Medical Center)
Testes externos	2 semanas	3 semanas (+1 semana)
Integrações de terceiros revisadas	2 integrações	3 integrações (+1 gateway de faturamento)
Taxa do projeto	$94,000	$111,500 (+$17,500)
Entrega do relatório final	Semana 8	Semana 9 (+1 semana)

[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.

ATIVIDADE	HORAS	TAXA	VALOR
Definição de escopo e reconhecimento Regras de engajamento, inventário de ativos e mapeamento da superfície de ataque	2	$9,500 / wk	$19,000
Teste de invasão externo Avaliação do portal do paciente e da API expostos à internet	2	$14,000 / wk	$28,000
Testes internos e de engenharia social Cenário simulado de endpoint comprometido e exercício de phishing	1	$16,000 / wk	$16,000
Revisão de integrações de terceiros Avaliação de segurança das APIs de resultados de exames e do fornecedor de faturamento	1	$12,000 / wk	$12,000
Relatório e suporte à correção Relatório de achados, mapeamento HIPAA e orientação de correção	1	$10,000 / wk	$10,000
Taxa adicional			**$94,000**

VALOR ORIGINAL DO CONTRATO (SOW-2026-0771)	$94,000
TAXA ADICIONAL (ESTA SOLICITAÇÃO DE ALTERAÇÃO)	$94,000
NOVO TOTAL	$111,500

NOVO TOTAL **$111,500**

Todos os valores estão em dólares americanos (USD) e não incluem os impostos aplicáveis. A taxa adicional é cobrada de acordo com o cronograma de marcos do SOW de origem: 50% na aprovação desta alteração e 50% no lançamento.

CRONOGRAMA DE PAGAMENTO

QUANDO CADA PARCELA VENCE

N.º	MARCO	GATILHO	PARCELA	VALOR
01	Semanas 1–2 · Definição de escopo e reconhecimento	16 de fevereiro de 2026	50%	$47,000
02	Semanas 3–5 · Testes ativos	No início da entrega	50%	$47,000
Total (sem impostos)			**100%**	**$94,000**

As parcelas são faturadas conforme os marcos acima e são pagáveis em até 30 dias após cada fatura. Todos os valores estão em USD e não incluem imposto sobre vendas (wa — serviços profissionais isentos).

PREMISSAS E CONDIÇÕES DE APROVAÇÃO

Contas de teste e uma carta assinada com as regras de engajamento são fornecidas antes do início dos testes; um representante é autorizado a aprovar alterações de escopo em cada etapa; e os testes ficam limitados ao portal do paciente e às suas duas integrações de terceiros nomeadas. Alterações a esses itens afetam o cronograma e o custo, o que acordaríamos por escrito antes de prosseguir. O valor é válido para projetos iniciados até 6 de março de 2026.

A assinatura abaixo aprova o escopo, o cronograma revisado e a taxa adicional estabelecidos nesta solicitação de alteração, e autoriza a alteração correspondente do contrato de serviço de origem.

PELA MERIDIAN HEALTH SYSTEMS

RENATA COLE

DIRETORA DE SEGURANÇA DA INFORMAÇÃO

Data

PELA NULLWIRE SECURITY

NULLWIRE SECURITY

SIGNATÁRIO AUTORIZADO

Data

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