Rehmo API v1

Guia Oficial

de

Implementação de Webhooks

Documento oficial para implementação de endpoint Webhook do lado do cliente.
Este guia foi elaborado para equipes técnicas de todos os níveis.

1. Introdução

Este documento descreve de forma detalhada como implementar um endpoint HTTP capaz de receber eventos enviados pela Rehmo API v1 via Webhooks. O objetivo é permitir integração segura, confiável e simples, mesmo para equipes sem experiência prévia com Webhooks ou segurança HMAC.

2. Conceito de Webhook na Rehmo API

Webhooks são notificações automáticas enviadas pela Rehmo sempre que um evento clínico relevante ocorre. Ao invés do seu sistema consultar a API repetidamente, a Rehmo envia os dados diretamente para você.

- Características principais:
    - Comunicação via HTTP POST
    - Envio de dados no formato JSON
    - Segurança via assinatura HMAC SHA-256
    - Entrega assíncrona com tentativas automáticas (retry)

3. Pré-requisitos para Implementação

1. Antes de iniciar, sua equipe deverá providenciar:
    1. Uma URL pública acessível via HTTP ou HTTPS
    2. Um segredo (secret) compartilhado com a Rehmo
    3. Um servidor capaz de receber requisições HTTP POST

4. Estrutura da Requisição Webhook

Quando um evento ocorre, a Rehmo envia uma requisição HTTP POST para a URL cadastrada, contendo cabeçalhos específicos e um corpo JSON.

4.1 Headers Enviados

- Content-Type: application/json
- X-Rehmo-Event: nome do evento
- X-Rehmo-Signature: assinatura HMAC SHA-256 do payload

5. Exemplo de Payload

Abaixo está um exemplo real de payload enviado pela Rehmo:


```
{
  "device": "ABC123",
  "paciente_id": 42,
  "alerts": [
    {
      "type": "tachycardia",
      "severity": "high",
      "metric": "heartrate",
      "value": 135,
      "message": "Frequência cardíaca elevada",
      "datetime": "2026-02-06T10:15:00Z",
      "source": "realtime"
    }
  ],
  "generated_at": "2026-02-06T10:15:03Z"
}
```


6. Segurança – Validação da Assinatura

Todas as requisições de Webhook são assinadas digitalmente para garantir que os dados realmente foram enviados pela Rehmo e não foram alterados.

2. Etapas obrigatórias de validação:

    4. Ler o corpo bruto da requisição (raw body)
    5. Calcular o HMAC SHA-256 utilizando o secret
    6. Comparar com o valor recebido no header X-Rehmo-Signatre

7. Exemplo de Implementação em PHP

```php
<?php
$rawBody = file_get_contents('php://input');
$receivedSignature = $_SERVER['HTTP_X_REHMO_SIGNATURE'] ?? '';

$secret = 'SEU_SECRET_AQUI';
$expectedSignature = hash_hmac('sha256', $rawBody, $secret);

if (!hash_equals($expectedSignature, $receivedSignature)) {
    http_response_code(401);
    exit('Assinatura inválida');
}

$data = json_decode($rawBody, true);

// Processar os dados recebidos aqui

http_response_code(200);
echo 'OK';
?>
```

8. Boas Práticas

- Sempre validar a assinatura antes de processar o payload
- Responder rapidamente com HTTP 200
- Processar dados de forma assíncrona
- Registrar logs para auditoria

9. Política de Retry e Falhas

Caso o endpoint do cliente não responda corretamente, a Rehmo tentará reenviar o evento automaticamente até 5 vezes, com intervalos progressivos. Falhas de Webhook não impactam a API REST.

10. Suporte

Em caso de dúvidas técnicas ou problemas na implementação, entre em contato com o suporte técnico da Rehmo.