Objectives

- Protect patient and admin data from bots and attackers
- Comply with HIPAA-aligned security hygiene (where possible via infra layer)
- Replace WordPress plugins (like Limit Login Attempts) with Cloudflare WAF rules
- Minimize server load and attack surface via edge controls

Edge-Level Login Protection

Replace Limit Login Attempts plugin with:

- Rate limiting rule for /wp-login.php
- 5 attempts per 10 minutes per IP
- Action: Managed Challenge
- Block access to /wp-login.php and /wp-admin from outside US/CA (if possible based on staff location)

Threat Intelligence Rules

Enable Cloudflare Managed Rulesets

- OWASP Core Ruleset
- WordPress-specific Ruleset
- PHP Injections, XSS, and SQLi protections
  Block high-risk traffic using threat scores:

Bot Mitigation

- Enable Bot Fight Mode
- Challenge requests with suspicious or blank user agents:

Form & API Protection

- Rate Limit: Any form endpoint (e.g., /contact/, /api/form)
- 10 requests per 10 minutes per IP
- Use Challenge or Block if abused

Sensitive Area Lockdown

- Restrict wp-admin, /xmlrpc.php, and dashboard tools:
- Block xmlrpc.php entirely.

Visibility & Monitoring

Set up email/slack/webhook alerts for

- High WAF activity
- Rate limit triggers
- Managed Challenge volume spikes

Review & Tune

Monthly

- Audit Cloudflare user access
- Deep dive into Cloudflare Analytics (top paths, agents, referrers)
- Check Firewall Events (Blocked, JS Challenge)
- Review login attempts and rate limits
- Tune WAF rules based on new activity

- Update allow/block lists

Sample WAF Rules

Block SQL Injection in URL Parameters

Rule: (http.request.uri.query contains "UNION SELECT" or http.request.uri.query contains "'--")
Action: Block

Block Directory Traversal Attempts

Rule: (http.request.uri.path contains "../" or http.request.uri.path contains "%2e%2e%2f")
Action: Block

Block Non-Standard HTTP Methods

Rule: (http.request.method in {"PUT" "DELETE" "OPTIONS"})
Action: Block

Challenge Blank or Suspicious User Agents

Rule: (http.user_agent eq "" or http.user_agent contains "python-requests")
Action: Managed Challenge

Geo-Block wp-admin Access

Rule: (http.request.uri.path contains "/wp-admin" and not ip.geoip.country in {"US" "CA"})
Action: Block

Challenge Based on Threat Score

Rule: (cf.threat_score gt 40)
Action: Managed Challenge

Rate Limit Contact Form Abuse

Path: Few different paths on the site, this is related to gravity forms

Rate Limit: 10 requests per 10 minutes per IP
Action: Challenge