CLOUDFLARE

Code red: DDoS attacks threaten patient safety

As distributed denial-of-service (DDoS) attacks intensify, healthcare remains a prime target. By overwhelming critical systems, these attacks cause maximum disruption — blocking access to EHR records, scheduling systems, and more. This isn't just downtime; it's a direct threat to patient care and safety.

70%

Most healthcare organizations (70%) have faced moderate-to-severe financial effects from a cyber incident.[1]

#1

Healthcare is the top sector targeted by ransomware attacks[3], which include ransom DDoS attacks.

$10.93M

Compared to other industries, healthcare suffers the highest average breach cost, at $10.93 million.[2]

59%

For more than half (59%) of healthcare organizations, a cyber incident delayed treatments, compromised patient trust, or caused other clinical challenges.[4]

The ripple effect of DDoS attacks

DDoS attacks maliciously flood a server, service, or network with "junk" Internet traffic. Their goal is to overwhelm and shut down online services, impacting the entire healthcare ecosystem:

Patient care paralysis: Attacks on portals, telehealth, and EHRs lock out staff and block patient access to critical services.

Data breach smokescreen: DDoS attacks often distract and overwhelm security teams, providing cover for the simultaneous theft of highly valuable patient data (PHI).

Supply chain disruptions: Attacks can halt clinical trials, medication shipments, and financial operations like claims and pre-authorizations.

The treatment plan: four DDoS security must-haves

1 Visibility and differentiation:
Much like medications that block pain signals while allowing your body to function, your DDoS solution must only block attacks — not "healthy" traffic.

2 Global scale:
A cloud network with unlimited capacity can absorb the largest attacks while keeping your EHR portals, mHealth apps, and other digital services fast and secure.

4 Protection for every connection:
DDoS mitigation for external-facing apps and networks is a critical first line of defense. But if an attack does succeed, having zero trust security can prevent your internal systems and data from getting breached.

3 Adaptive defense:
The larger and more robust the mitigation network, the richer the intelligence it can provide on evolving attack patterns. This helps boost "immunity" against future attacks.

Mitigate the most advanced DDoS attacks

> Cloudflare's ease of use, automatic updates, and automatic threat protection save us time and manpower while allowing us to maintain a high level of cybersecurity against threats that could harm our patients and our business.

Wisut Ua-Anant
Chief Digital MarTech Officer

Bumrungrad International HOSPITAL

Read their story

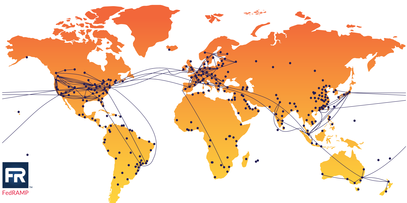
Cloudflare's integrated L3-7 DDoS protection monitors, prevents, and mitigates attacks before they can harm your organization or patient care.

234 billion cyber threats

are blocked (on average) by Cloudflare every single day[4]

449 Tbps of network capacity

makes Cloudflare capable of absorbing the largest DDoS attacks — including the **world's largest DDoS attack**[5] — a record-breaking 29.7 Tbps.



FedRAMP

2-3 seconds

is the average time it takes Cloudflare's always-on protection to detect and block malicious DDoS traffic

Over 20% of the web

sits behind our network, relying on Cloudflare to be fast, secure, reliable, and private for whatever users are doing online.

CLOUDFLARE

Enhance protection against DDoS attacks and other threats, deliver seamless patient experiences, and boost compliance — all with Cloudflare's single, secure cloud platform.

Learn how

Sources:

1. Emily Olsen, "Most healthcare organizations face significant financial, operational impact from cyber threats: survey," Healthcare Dive, 6 November 2025
2. Mike Elgan, "Cost of a data breach: The healthcare industry," IBM, accessed 6 November 2025
3. Steve Alder, "Q1 2025 Ransomware Report," The HIPAA Journal, 10 April 2025
4. As of Q3 2025 (source: Cloudflare)
5. As of October 2025 (source: Cloudflare)