

Is 23healthcare.com a scam? TrustSniffer's high-risk assessment: 0/100

23healthcare.com

Verdict

0

OUT OF 100

CRITICAL RISK

23healthcare.com shows high-risk / scam indicators.

This assessment found strong scam indicators. Do not pay, sign in, or share personal details with this site.

Sensitive Interaction Risk

Governance Risk

Assessed 2026-08-18 by automated analysis. Classification confidence 75%.

What this site appears to be

Commercial clinic website promoting stem cell and cell-based therapies with service descriptions, treatable-conditions lists, a patient inquiry form requesting medical history, contact details and a Malaysian physical address. Clinical/regulatory claims are present but lack detailed verifiable citations on the page.

Evidence status and limitations

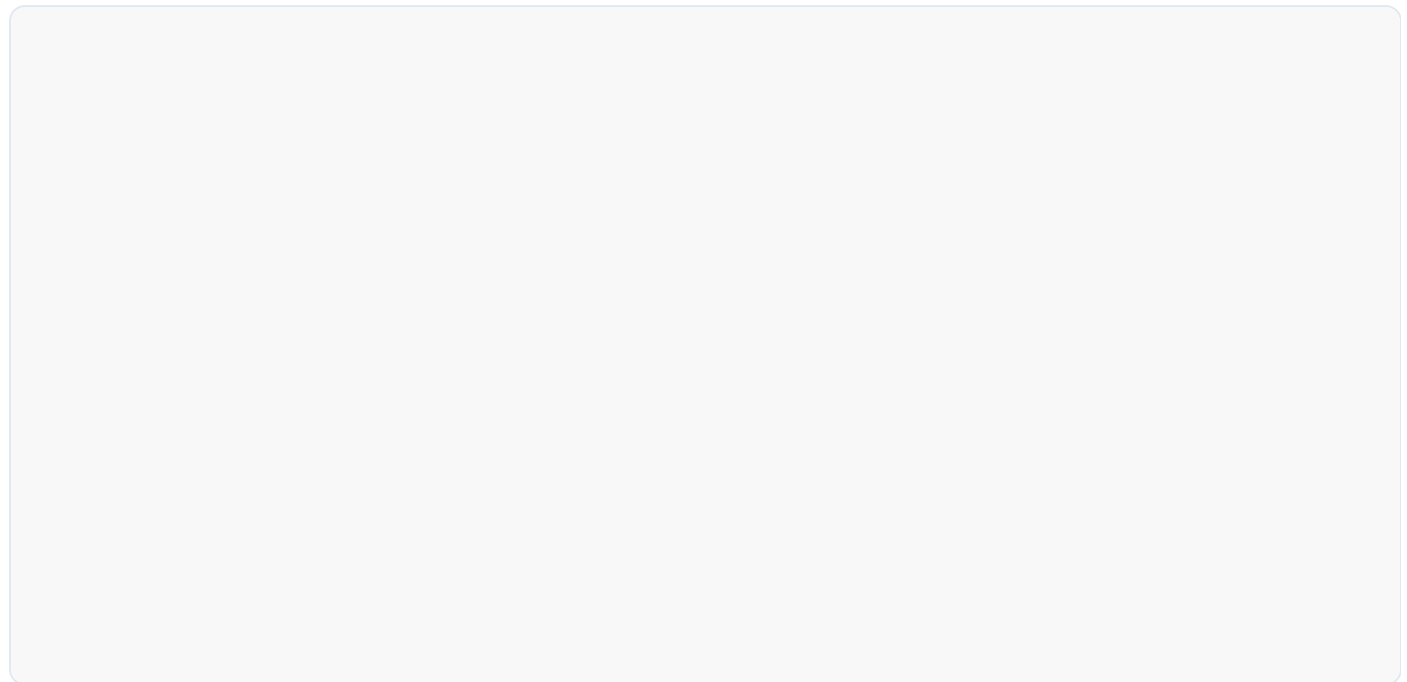
- Evidence completeness: UNKNOWN
- The real-world operator identity was not independently verified.
 - Module-level completeness metadata is unavailable for this legacy report.

At a glance

The checks that decide most of this verdict.		
Malware engines	12 flagged it VirusTotal	RISK
Google Safe Browsing	Not listed Google	CLEAR
Abuse reports on the host	0 reports AbuseIPDB; shared hosting inflates this count	NOTED
Domain age	6.6 years old Registered history	CLEAR
Web archive	Archived since 2021 413 snapshots	CLEAR

The page as captured

<https://23chealthcare.com/>



What 23chealthcare.com served when TrustSniffer captured it on 2026-08-18. The page may look different now.

Key findings

- Automated classification: Sensitive Interaction Risk.
- Domain age: 3 to 10 years (registration continuity).
- Public web-archive history exists since 2021.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.

Full analysis

Security Alert

Fortinet, Sophos flagged this site in external intelligence checks, indicating elevated compromise/scam exposure that requires immediate caution.

23C Healthcare is a commercial medical-clinic website presenting stem-cell and cell-based treatment services, condition-specific treatment information, and an inquiry pathway intended to convert prospective patients into consultations or clinical procedures.

Scam/Impersonation Risk

Confirmed external reputation contradictions make this unsuitable for sensitive interaction. The domain is blacklisted by external reputation sources, with multiple malicious detections recorded, and the deterministic assessment treats this as a material threat signal rather than a minor reputational concern. Interaction testing also identified hidden forms and password-bearing external submissions, although the visible site is presented as a medical-clinic landing page rather than a conventional login portal. No separate identity contradiction or

explicit brand-impersonation finding was established; the principal concern is the convergence of blacklist and behavioral signals. The domain's established registration and archival continuity do not neutralize those findings.

EVIDENCE

- External reputation telemetry: the domain is blacklisted by 2 external sources; 12 malicious and 2 suspicious detections were recorded across 19 evaluations.
- Domain registration record: registered 2020-01-09, approximately 6.61 years old, with expiration on 2027-01-09.
- Web archive: 413 snapshots from 2021-11-23 through 2026-04-20, spanning 6 tracked years.
- Homepage interaction testing: 2 hidden forms were detected across 2 runs, including 2 external password-form submissions.

Regulatory Verification Notes

The site makes high-stakes clinical claims about mesenchymal stem cells, natural-killer cells, and prospective MCAR-T treatment, and lists conditions including autism, cerebral palsy, multiple sclerosis, spinal injuries, stroke, and motor-neuron diseases. These claims are not accompanied on the page by detailed regulatory citations or peer-reviewed support, creating a significant evidence gap for medical decisions. The available material does not disclose a license or registration number, so the clinic's authorization and the legal identity responsible for treatment remain matters for independent confirmation rather than established facts. The site presents a Malaysian physical address and patient inquiry process, but those on-page details do not independently verify the operator. Transport encryption is present, but the certificate uses domain validation only and does not authenticate the medical operator.

EVIDENCE

- Treatment material: clinical efficacy and treatable-condition claims are presented without detailed verifiable citations on the page.
- Clinic/contact material: a Malaysian physical address and an inquiry form requesting contact details and medical history are displayed.
- Hosting telemetry: served from AS13335, CLOUDFLARENET — Cloudflare, Inc., US.
- TLS telemetry: certificate issued by WE1 at DV validation level, valid to 2026-10-09T16:45:22+00:00.

What to Verify Next

Before any clinical, financial, or data-sharing engagement, an independent Malaysian healthcare-registry check should confirm the responsible legal entity, facility authorization, and the credentials of the clinicians involved. The treatment claims should be mapped to regulator-recognized indications and supporting clinical evidence rather than relying on the site's summaries. The inquiry process should also be validated through an independently sourced contact route, with confirmation of consent, medical-record handling, retention, and escalation procedures before sensitive information is transmitted.

EVIDENCE

- Legal and contact pages: independently match the stated operator and physical location to an official healthcare or corporate registry.
- Treatment pages: obtain regulator references and peer-reviewed evidence for each proposed therapy and condition.
- Inquiry workflow: confirm the identity of the receiving organization and its patient-data safeguards through an independently verified channel.

Summary Verdict

The overall posture is **critical**, with sensitive-interaction risk taking precedence over the site's professional presentation and established web presence. Available evidence does not support treating the website as trustworthy for operational engagement, and the operator's real-world identity remains unverified.

Infrastructure Integrity

The website is protected by Cloudflare CDN/WAF infrastructure, and all observed addresses were CDN edge servers rather than an independently observable origin. This provides a meaningful mitigation against direct infrastructure exposure, but it is only a protective hosting characteristic and does not establish legitimacy or offset the external reputation findings.

EVIDENCE

- Infrastructure: Cloudflare CDN/WAF protection was detected; 4 observed addresses were identified as edge servers and 0 origin candidates were identified.
- Edge telemetry: observed IPv4 and IPv6 addresses resolved through Cloudflare edge infrastructure in the United States.

Closing Assessment

Activity should remain limited to passive review until independent legal, clinical, and data-handling checks are completed; credentials, medical records, and payment details should not be submitted.

Written analysis generated 2026-08-18 by the TrustSniffer Analysis Engine from the evidence in this report.

What the analysis found

2 findings contributed to this verdict, raised by registration and ownership, analysis engine, behaviour in a sandbox, page content, external reputation.

01 Governance Risk

- The registration record withholds contact details for the operator.
Registration and ownership rule:KF_WHOIS_HIDDEN
- Registration details are held behind a privacy service, so no operator is named publicly. This is common and legal, and it also means there is nobody to check.
Registration and ownership rule:KF_WHOIS_PRIVATE

02 Sensitive Interaction Risk

- The analysis matched a pattern TrustSniffer treats as a direct threat to a visitor.
Analysis engine signal:direct_threat
- The structure of the page changed sharply while it was loading.
Behaviour in a sandbox rule:BEHAV_DOM_DENSITY_SPIKE
- The page asks visitors for sensitive information.
Page content rule:PAGE_FORM_SENSITIVE
- The page contained a form a visitor cannot see.
Behaviour in a sandbox rule:BEHAV_HIDDEN_FORMS
- The page rewrote itself after it was interacted with, so what a visitor first sees is not what they end up on.
Behaviour in a sandbox rule:BEHAV_DOM_DIFF_AFTER_INTERACTION
- An external threat feed lists this domain: either Google Safe Browsing marked it malicious, or a significant number of malware engines flagged it.
External reputation rule:EXT_BLACKLIST_CRITICAL

Identity verification

Status	UNVERIFIED
Identity score	30/100
Identity verification confidence	25%

- No on-site identity signals detected

Identity verification measures whether the site can be independently connected to a real-world brand or person. It is separate from the classification confidence.

What TrustSniffer observed

First-party facts recorded during the assessment of 23chealthcare.com.

- The request stayed on 23chealthcare.com. It was not redirected to another domain. CLEAR
- Registration is published under NAMECHEAP INC. CLEAR
- DNS for this domain is served by cloudflare.com, across 2 name servers. NOTED
- The registration is paid up to 2027-01-09. NOTED
- The earliest public archive of this site is from 2021-11-23. CLEAR
- It is hosted on CLOUDFLARENET, from a server in US. NOTED

Domain intelligence

Registrar	NAMECHEAP INC
Hosting	CLOUDFLARENET - Cloudflare, Inc., US
Country	US

Server IP	2606:4700:3035::6815:6ba
Name servers	ELINORE.NS.CLOUDFLARE.COM, MACIEJ.NS.CLOUDFLARE.COM
SSL issuer	WE1
SSL expiry	2026-10-09
Domain age	6.61 years (continuous registration)
Domain expiry	2027-01-09
Archive first seen	2021-11-23
Archive snapshots	413
Reputation	VirusTotal: 12 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about 23healthcare.com at assessment time. It is a starting point for your own judgement, not a guarantee: a high score means the signals were consistent with a legitimately operated site, a low or critical score means several risk patterns were present.

TrustSniffer assesses a website from the evidence it can collect at a point in time: domain registration and age, hosting and certificate, the content the site served, and third-party reputation feeds. A score is a summary of that evidence, not a guarantee and not a legal finding. There is no human rating and no user review in it. A site can change after it is assessed.

This report online: <https://trustsniffer.com/report/23healthcare.com> · assessed 2026-08-18