MCP SERVER | NO CODE | CLOUD HOSTED

CDC Disease Sentinel MCP

Track US disease surges and trends with live CDC data.

CDC Disease Sentinel monitors the CDC's National Notifiable Diseases Surveillance System. It gives your agent the ability to detect real-time spikes, compare current case counts against yearly baselines, and map disease concentration across states or census regions using live, public health data.

A+ Quality Score 96.67/100

cdc | diseases | outbreaks | public-health | nndss | surveillance

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · SEPTEMBER 2026
vinkius.com/en/ai-agent-connect/cdc-disease-sentinel

SCAN TO VIEW

The connectivity layer between AI and the world's software.

Vinkius sits between AI and every application. All communication passes through Vinkius Cloud via the Model Context Protocol (MCP) — with governance, observability, and security at every layer.

Your AI Connections Run Through Vinkius Cloud

The world's largest managed MCP catalog

Vinkius is the connectivity layer where AI connects to the software your business already runs. We handle the hosting, the security, the credentials, the uptime — you get agents that actually do things.

We operate the world's largest managed MCP catalog. Major SaaS platforms, CRMs, databases, and cloud providers — running, monitored, production-ready. This MCP server is hosted and maintained by the Vinkius Cloud for AI Agents.

> *The agent doesn't manage credentials, doesn't manage uptime, doesn't manage security. Vinkius does.*
>
> — Architecture principle

Four Pillars of the Vinkius Runtime

01 — Security by design

Credentials stay encrypted at rest via AES-256. The AI agent never touches raw keys — they're injected into a sandboxed V8 isolate at runtime. Actions are logged, and connections have an emergency kill switch.

02 — Built on MCP Fusion

This MCP server was built with **MCP Fusion**, the open-source framework (Apache 2.0) that powers the entire Vinkius catalog. Schema-as-firewall strips undeclared fields, compiled PII redaction runs at zero overhead, and cryptographic lockfiles produce git-diffable audit trails.

03 — Deterministic observability

Eight immutable metrics per endpoint: request volume, p95 latency, error rate, active connections, cost attribution. A live payload feed logs every tool call with mutation detection.

04 — Autonomous operations

Servers are deployed, monitored, and patched autonomously. New capabilities and security patches ship weekly. Zero-downtime deployments ensure continuous availability across all managed MCP servers.

AES-256	Ed25519	24h TTL	V8 Isolate
Encryption at rest	PKI vault signatures	Ephemeral session keys	Sandboxed execution

One Token. Instant Access.

Every MCP server on Vinkius is accessed through a **Connection Token**. Tokens are generated in the cloud dashboard and produce a unique MCP endpoint URL. Paste this URL into any MCP-compatible client — no SDK required.

A single token can serve **multiple AI clients simultaneously**, or you can issue separate tokens per client for granular access control. Each token tracks its own request count, last activity timestamp, and can be individually enabled or revoked.

MCP ENDPOINT

```
https://edge.vinkius.com/{token}/mcp
```

Claude · Cursor · VS Code · Windsurf · Grok · Gemini

Security Is the Architecture

Security in Vinkius is not a feature — it's the foundation of the runtime. The gateway enforces multiple independent protection layers between AI agents and third-party APIs.

01 — Ed25519 PKI Vault

Every workspace has an Ed25519 Master Key. Session keys are generated ephemerally (24h TTL) and signed by the Master Key. Credentials never leave the vault boundary.

02 — V8 Isolate Sandboxing

Tool code runs inside isolated-vm V8 isolates with 64 MB memory caps and per-request timeouts. No filesystem access, no network access except through the SSRF-guarded fetch bridge.

03 — SSRF Guard

All outbound HTTP requests are DNS-resolved and validated before execution. Private IP ranges (10.x, 172.16-31.x, 192.168.x, AWS metadata 169.254.x) are blocked at the network layer.

04 — DLP & PII Redaction

A ResponseGuard pipeline intercepts every tool response. Configurable redaction patterns strip sensitive fields (emails, SSNs, card numbers) before data reaches the AI agent.

05 — Cryptographic Audit Trail

Every request is signed into a SHA-256 hash chain with Ed25519 signatures. Events form a tamper-proof, SIEM-exportable forensic record.

06 — Honeytoken Trap System

Phantom credentials are injected into isolated environments. If a honeytoken is used outside Vinkius infrastructure, the server is quarantined instantly.

Emergency Kill Switch

EU AI Act Art. 14(1) Compliant

The kill switch is an **emergency halt** mechanism — not a simple toggle. When triggered, it executes three actions atomically:

01 — Server deactivated

The MCP server is immediately taken offline across the entire cluster.

02 — All tokens revoked

Every connection token is invalidated. Total lockout — reconnection blocked until new tokens are issued.

03 — WebSocket connections killed

Active connections terminated via Redis pubsub broadcast. Propagates to every runtime node in the cluster.

Full Visibility. Zero Guesswork.

The Vinkius cloud dashboard includes a full MCP Governance suite — real-time analytics and security controls for production AI operations.

Control Plane

KPI dashboard with request volume, latency, success rate, token consumption, and AI-generated operational briefings.

Agent Activity

Which AI clients are connecting, how often, and what they're doing — real-time session tracking.

FinOps

Cost tracking per tool, payload compression savings, budget optimization signals, and consumption trends.

Tool Health

Slowest and most error-prone tools, with actionable root-cause insights and performance baselines.

Firewall & DLP

PII redaction activity, sensitive data protection counters, and security event timeline.

Incident Log

Error trends, failure rates, status-code breakdowns, and forensic audit trail access.

> Get started at **cloud.vinkius.com** — connect your AI agent in under 60 seconds.

CDC Disease Sentinel MCP

5 tools available
Cloud-hosted on Vinkius

You can use this MCP to turn your AI client into a public health monitor. Instead of digging through messy government spreadsheets, you just ask your agent if a specific disease is spiking in a certain state. The MCP pulls directly from the CDC's NNDSS, providing the latest weekly case counts and comparing them against historical averages. You can check if current numbers are normal, elevated, or a full surge based on a configurable multiplier. It handles the heavy lifting of calculating year-to-date comparisons and 52-week baselines, so your agent can provide a clear verdict on whether a situation is unusual. Whether you need to see the momentum of a single disease over the last few weeks or find out which states are seeing the most cases right now, this tool provides the exact strings and data points your agent needs to give you an accurate answer.

Core Capabilities

01 — Surge Detection

Your agent identifies when disease counts cross specific multipliers to flag unusual activity.

02 — Trend Analysis

The MCP provides weekly case series so your agent can interpret the direction of a disease curve.

03 — Geographic Mapping

Your agent can pinpoint exactly which states or regions are seeing the highest case concentrations.

04 — Historical Comparison

The tool compares current year-to-date totals against the same period from the previous year.

One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/en/ai-agent-connect/cdc-disease-sentinel** — connect your AI agent in three steps.

01 Connect to the MCP through your compatible AI client.

02 Ask your agent a question about disease counts or surges.

03 The MCP pulls the latest data from the CDC NNDSS.

04 The tool calculates trends, surges, or baselines based on your request.

05 Your agent receives the data and answers your question.

The MCP connects your AI client directly to the CDC's surveillance system.

Built For

This MCP is built for professionals who need to monitor public health shifts without manual data entry.

Public Health Analysts

They use the tool to pull reproducible weekly series and official CDC flags.

Journalists

They use it to verify if a headline about a disease spike is backed by real-time data.

Automation Developers

They build scheduled disease pulse digests using server-side delta calculations.

What Changes When You Connect

01 Eliminates manual data retrieval from CDC portals.

02 Provides exact area and disease names for error-free follow-up queries.

03	Computes surge multipliers and baselines server-side.
04	Uses live, stateless data for the most current information.

Real-World Applications

Outbreak Monitoring

An agent can automatically flag when a disease hits a surge threshold in a specific region.

Comparative Research

Researchers can compare current YTD case counts against last year's data to spot shifts.

Regional Health Reports

Users can generate lists of states with the highest reported cases for a specific week.

Trend Verification

Verify if a disease is actually climbing or just fluctuating within normal limits.

Patterns to Avoid

Guessing disease names

AVOID

You ask your agent to check the status of 'the flu' without knowing the exact CDC designation.

✓ INSTEAD

Use `list_diseases` first to get the precise names required for accurate queries.

Manual surge math

AVOID

You try to manually compare this week's counts to last year's totals using raw numbers from a spreadsheet.

✓ INSTEAD

Let the MCP handle the math by using `disease_baseline` to get an immediate comparison against historical averages.

Vague geographic queries

AVOID

You ask your agent which parts of the country are seeing high case counts without a specific disease context.

✓ INSTEAD

Run `state_scan` for a specific disease to get a ranked list of reporting areas.

The Right Fit

Public health professionals and journalists should connect this MCP to get instant, verifiable data. Automation developers looking to build disease pulse digests will find it useful. If you only need static, historical archives rather than live weekly surveillance, you don't need this tool.

CDC Disease Sentinel: 5 Specialized Surveillance Tools

These tools provide direct access to NNDSS data, allowing your agent to calculate trends, detect surges, and map disease concentrations.

#	TOOL	DESCRIPTION
01	list_diseases	This tool provides the exact names of all diseases currently tracked by the CDC's weekly surveillance system.
02	disease_baseline	This tool answers if current disease levels are unusual by comparing the latest week to the 52-week maximum and YTD totals to the same period last year.
03	disease_trend	Use this to see the shape of a disease curve by retrieving weekly case counts for a specific disease over a set number of weeks.
04	state_scan	This tool ranks all reporting areas by case count for a specific disease to show where cases are most concentrated.
05	surge_check	This tool detects spikes by comparing the latest weekly count against the average of previous weeks to return a surge, elevated, or normal verdict.

See It in Action

Real prompts you can use once this MCP is connected to your AI agent through Vinkius Cloud.

U Is there a disease surge this week anywhere in the US?

The surge check identifies spikes in tracked diseases and reports the multiplier verdicts for each.

U Show me the last 16 weeks of national meningitis cases and say if it's trending up.

The agent retrieves the 16-week series for meningitis and analyzes the count momentum.

U Which states report the most norovirus this week?

The agent scans all reporting areas and lists the states with the highest norovirus case counts.

Frequently Asked Questions

01 **Do I need a CDC account to use this MCP?**

No. The MCP uses public CDC open data, so no credentials or accounts are required.

02 **How does the surge detection work?**

The surge check compares the most recent weekly count against the average of the previous weeks to determine if the activity is normal, elevated, or a surge.

03 **Can I check data for a specific state?**

Yes. You can use the state scan or specific disease tools to look at national, state, or census region data.

04 **Is the data real-time?**

The MCP pulls from the latest weekly NNDSS case counts provided by the CDC.

05 **What happens if there are no cases reported?**

The trend tool shows no data for weeks without reported cases rather than assuming a zero.

06 **Do I need credentials?**

No. The dataset is public CDC open data on Socrata, readable without a token (anonymous access is throttled and capped at 500 rows per query — every tool stays well under that). No signup, no key, no per-user state.

07 **How does the surge detector decide ”surge”?**

It divides the latest week's reported cases by the average of the previous N weeks (default 12, configurable). At or above the threshold multiplier (default 2.0) it reports a surge; at half the threshold it reports elevated; special cases (no cases this week, or a baseline with zero cases) are called out explicitly instead of producing a division artifact.

08 **Why do the tools insist on ”exact” disease and area names?**

The CDC portal's query engine only matches values exactly (fuzzy matching silently returns nothing), so list_diseases returns the exact labels to copy, and state_scan returns the exact area names — follow-up calls just copy one of them instead of guessing. If a name doesn't match you get an error that says so, never an empty silent answer.

09 **What data is behind it?**

CDC's NNDSS weekly surveillance: reported notifiable-disease case counts per MMWR week, per geography (national, regions, states, New York City), plus the dataset's own 52-week maximum and YTD comparators. Weeks without reported cases are shown as "no data", not as zeros. MMWR years run July-to-June.

Go Live in 60 Seconds

Get your connection token from **cloud.vinkius.com**, then paste the endpoint URL into any MCP-compatible client.

YOUR MCP ENDPOINT

```
https://edge.vinkius.com/[TOKEN]/mcp
```

CLIENT	WHERE TO CONFIGURE
Claude AI	Profile → Customize → Connectors → "+" → Add custom connector → Paste endpoint
Cursor	Settings → Features → MCP Servers → "+ Add New MCP Server" → Type: SSE → Paste endpoint
VS Code	Ctrl/Cmd+Shift+P → "MCP: Add Server" → add `"cdc-disease-sentinel": { "url": "…" }`
Windsurf	MCP Settings → `mcp_settings.json` → Add endpoint URL
ChatGPT	Settings → Tools & plugins → Add MCP server → Paste endpoint
Gemini	Extensions → Add MCP Server → Paste endpoint URL

ASK AN AI ABOUT THIS

Let your preferred AI explain this MCP server

- Ask ChatGPT
- Ask Claude
- Ask Perplexity
- Ask Gemini
- Ask Grok

READY TO CONNECT

CDC Disease Sentinel is live on Vinkius Cloud.

Get your connection token, paste it into your AI agent, and start building. No SDK. No deployment. Just results.

Start at cloud.vinkius.com →

vinkius.com · support@vinkius.com

INDEPENDENT PLATFORM DISCLAIMER

Vinkius is an independent platform and is not affiliated with, endorsed by, sponsored by, verified by, or otherwise authorized by CDC Disease Sentinel. All third-party trademarks, logos, and brand names are the property of their respective owners. Their use in this document is strictly for informational purposes to identify service compatibility and interoperability.

DOCUMENT INFORMATION

Generated	September 2026
MCP Server	CDC Disease Sentinel MCP
Server ID	`01a0d9c9-1131-7194-948b-72430c45227b`
Platform	Vinkius Cloud for AI Agents
Endpoint	`https://edge.vinkius.com/{token}/mcp`

LICENSE & USAGE

This document is generated automatically by the Vinkius PDF Engine. Content reflects the MCP server configuration at the time of generation and may change as updates are deployed. For the most current information, visit vinkius.com/en/ai-agent-connect/cdc-disease-sentinel.

© 2026 Vinkius · vinkius.com · support@vinkius.com