MCP SERVER | NO CODE | CLOUD HOSTED

Optum Eligibility MCP

Verify coverage and financial status instantly.

Optum Eligibility MCP instantly verifies patient healthcare coverage and financial status using Optum APIs. Check active insurance policies via X12 270/271 mappings, determine current deductibles, and confirm if a specific doctor is in-network before the appointment starts.

A+ Quality Score 100/100

patient-eligibility | insurance-verification | healthcare-data | phi-management

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · JUNE 2026

vinkius.com/mcp/optum-eligibility

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.

Optum Eligibility MCP

5 tools available
Cloud-hosted on Vinkius

Need to run front-desk operations without manual phone calls? This MCP handles real-time patient verification using Optum APIs. You can instantly check if a patient has active coverage, even extracting their remaining out-of-pocket limits and deductible amounts. It also confirms whether a specific doctor or facility is in-network for that policy. Because this focuses entirely on reading demographics and status checks—not changing claims data—it keeps things secure and compliant. With Vinkius, you connect your preferred AI client once and gain instant access to run these critical medical checks directly from your agent.

Core Capabilities

01 — Confirming coverage

Run advanced X12 transactions to determine if a patient's insurance policy is currently active.

02 — Determining out-of-pocket costs

Extract the remaining deductible amounts and maximum limits for any given health plan member.

03 — Validating provider status

Check if a medical facility or doctor is listed as in-network under the patient's policy.

04 — Finding patient records

Search the database using specific demographic details to locate an accurate patient record.

05 — Checking service requirements

Pull detailed coverage rules that show if a medical procedure needs prior authorization.

One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/mcp/optum-eligibility** — connect your AI agent in three steps.

01 You authorize the MCP by securely substituting your institutional client ID into the runtime module.

02 Your AI agent calls the necessary tool, providing specific patient identifiers or service codes.

03 The system executes the API call against Optum and returns structured data detailing eligibility status, deductibles, or network confirmation.

The bottom line is: you get accurate, real-time insurance verification results without leaving your AI workspace.

Built For

This MCP is for hospital receptionists and clinic managers who spend too much time on the phone confirming basic patient eligibility. If manual phone calls to insurance carriers are slowing down patient intake, this tool saves you hours of work every week.

Hospital Receptionist

Uses the MCP to run checks for active coverage and verify if a provider is in-network right before the patient arrives.

Clinic Manager

Manages intake by using this MCP to automatically check deductibles and identify if specialized services require prior authorization.

Healthcare Tech Integrator

Builds automated patient flow systems that need reliable, real-time data on eligibility without needing deep API knowledge.

What Changes When You Connect

01 Stop guessing on payment. Use opt_get_deductibles to get the exact remaining out-of-pocket maximums for a patient, so front desk staff know exactly what's owed.

02 Avoid service delays by running opt_verify_provider_network before appointments. This confirms if a doctor or facility is actually in-network for that specific policy.

03 Speed up intake with opt_check_eligibility. It runs real-time X12 checks, giving immediate confirmation of active coverage status instead of waiting on hold with an insurance carrier.

04 Handle complex medical needs by calling opt_get_benefit_details. This tool tells you if a service requires prior authorization before you even schedule it.

05 Eliminate manual lookups. Optum Eligibility allows your agent to use opt_search_patient_demographics, finding patient records quickly using only basic demographic info.

Real-World Applications

A new specialist is called in for a consult.

The clinic manager needs to know immediately if the specialist's facility accepts the policy. They ask their agent, which uses opt_verify_provider_network to confirm the status, preventing billing headaches later.

A patient arrives and seems confused about costs.

The receptionist asks their AI client to run opt_get_deductibles for the member's ID. The agent returns the remaining deductible amount ($1,250), letting staff give accurate cost estimates upfront.

Checking coverage for a specialized procedure.

A patient needs an MRI. Instead of calling insurance, staff use opt_get_benefit_details to confirm if the specific service requires prior authorization before booking the test.

Handling walk-in patients with partial records.

Staff only have a name and date of birth. They prompt their agent to run opt_search_patient_demographics first, locating the correct record ID before running any other eligibility checks.

Patterns to Avoid

Treating it like a general database search

✗ AVOID

Using a generic client tool to just 'find' insurance info. This fails because basic searching doesn't validate active status or deductibles.

✓ INSTEAD

To get accurate financial and coverage data, you must use specific tools like opt_check_eligibility (for active status) and opt_get_deductibles (for costs).

Relying on outdated policy documents

✗ AVOID

A manager reads an old internal document that says a service is covered, but the patient's current plan changed.

✓ INSTEAD

Always verify real-time status using opt_get_benefit_details. This tool checks the actual coverage rules tied to the patient's policy.

Assuming providers are always in-network

✗ AVOID

Staff schedule a patient with Dr. X because they know them, but fail to check if Dr. X is currently accepted by the insurance plan.

✓ INSTEAD

Before scheduling or confirming care, run opt_verify_provider_network to guarantee that facility and doctor are in-network for the member.

The Right Fit

Use this MCP when your workflow requires real-time financial validation of patient coverage. If you need to know *if* a policy is active, or *how much* the deductible is remaining, this tool is essential. Don't use it if all you need is static demographic data—a general record lookup might suffice. However, never rely on simple demographics alone; always follow up with opt_check_eligibility to confirm actual coverage status. If your goal is merely to manage billing codes without checking the patient first, this MCP isn't built for that. Its strength lies in front-line validation.

The headache of manual insurance verification

Right now, checking a patient's eligibility usually means calling them into the office, having staff manually input policy numbers into one portal, then logging onto another system to check deductibles. It's a cycle of clicking through three different tabs and copy-pasting data between systems just to confirm basic status.

With this MCP, your AI agent handles that entire sequence automatically. You simply ask for the eligibility check, and it runs advanced X12 transactions in seconds, giving you immediate confirmation—no phone calls or manual logins required.

Optum Eligibility: Knowing Costs Before Care

The biggest time sink is confirming if a provider is actually accepted and what the patient will pay. Staff waste minutes verifying network status or calling to determine if an MRI needs prior authorization before they even book the appointment.

This MCP gives you certainty. You can use opt_verify_provider_network and opt_get_benefit_details together, making sure every service is covered and that the doctor accepts the policy right out of the gate.

Optum Eligibility: 5 Tools for Medical Verification

These tools let your agent perform core front-desk functions, including checking eligibility, verifying costs, searching records, and confirming provider status.

#	TOOL	DESCRIPTION
01	`opt_check_eligibility`	Verify if a patient has active healthcare coverage. Maps to X12 270/271 EDI transactions securely
02	`opt_get_benefit_details`	Pulls granular coverage rules indicating if a specific medical service requires prior authorization
03	`opt_get_deductibles`	Extract remaining out-of-pocket maximums and deductibles for a specific health plan member
04	`opt_search_patient_demographics`	Search the healthcare database for a patient record matching specific demographic parameters securely
05	`opt_verify_provider_network`	Checks if a specific doctor or medical facility is In-Network for the given patient policy

See It in Action

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

U Check the remaining deductibles and out-of-pocket maximum amounts for patient ID 99281.

Query completed. Patient 99281 has a remaining active deductible of $1,250 towards an annual ceiling.

U Find if John Doe is currently eligible for an MRI under policy HDHP-77.

Eligibility verified. John Doe is active under HDHP-77 but MRIs require prior authorization before service delivery.

U List all dependents covered under Member ID UB-11202.

Located dependents under subscriber UB-11202: 1 Spouse (Active) and 2 Toddler dependents (Active) currently attached.

Frequently Asked Questions

01 **What does opt_check_eligibility do?**

opt_check_eligibility verifies if a patient has active healthcare coverage. It uses secure X12 270/271 mappings to confirm the current status of their insurance policy.

02 **Can I find out the deductible using opt_get_deductibles?**

Yes, opt_get_deductibles extracts the remaining out-of-pocket maximums and deductibles for a specific member. This is crucial for giving accurate cost estimates.

03 **How do I check if a doctor is in-network?**

You run opt_verify_provider_network to check the status of any given medical facility or doctor against the patient's policy. This prevents billing surprises later on.

04 **Is this for reading data only, or can it change claims?**

This MCP is engineered strictly for reading PHI demographics and status. It deliberately excludes any financial claim mutations, keeping the process secure.

05 **How do I start checking eligibility with opt_search_patient_demographics?**

First, you use opt_search_patient_demographics to find the correct patient record ID using available demographics. Then, you pass that ID to other tools for verification.

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 `"optum-eligibility": { "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

Optum Eligibility 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 Optum Eligibility. 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	June 2026
MCP Server	Optum Eligibility MCP
Server ID	`019d75eb-720b-73e0-a309-0c5dc1923689`
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/mcp/optum-eligibility.