

M C P S E R V E R

N O C O D E

C L O U D H O S T E D

Care Emergency Contact Plan MCP

Organize your emergency protocols and contact escalation paths.

Care Emergency Contact Plan MCP manages your emergency contact protocols and notification sequences. It lets your AI client handle complex escalation paths, verify what information can be shared with specific contacts, and generate printable contact cards. You can also track mandatory audit schedules to keep your safety data accurate and up to date.

A+ Quality Score 100/100

emergency

contacts

protocol

safety

notification



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.

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.

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.

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

Encryption at rest

Ed25519

PKI vault signatures

24h TTL

Ephemeral session keys

V8 Isolate

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.

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.

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.

06 — Honeypot Trap System

Phantom credentials are injected into isolated environments. If a honeypot 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.

FinOps

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

Firewall & DLP

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

Agent Activity

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

Tool Health

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

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.

Care Emergency Contact Plan MCP

4 tools available

Cloud-hosted on Vinkius

You can use this MCP to build a structured framework for emergency response. Instead of digging through spreadsheets during a crisis, you let your AI agent manage the heavy lifting of contact protocols. It handles the logic of who gets notified first and what specific details they are allowed to see based on their role.

When an incident occurs, your agent uses the data to follow a pre-set escalation path, ensuring the right people are reached in the correct order. It also keeps your safety data from getting stale by tracking required quarterly audits. You can quickly pull printable summaries for authorized contacts or check if a specific person has permission to access sensitive information. It's about making sure your emergency response is predictable, permission-based, and ready when it matters.

Core Capabilities

01 — Escalation Logic

Your agent calculates the exact order of notifications during an emergency.

02 — Permission Management

The AI checks role-based boundaries to prevent unauthorized data sharing.

03 — Contact Documentation

Your agent creates printable cards for authorized individuals.

04 — Audit Tracking

The MCP identifies when your contact plans need a mandatory review.

One Click on Vinkius — From Prompt to Execution

Available at vinkius.com/en/ai-agent-connect/care-emergency-contact-plan — connect your AI agent in three steps.

- 01 Connect your preferred MCP-compatible client to Vinkius.
- 02 Define your contact roles and notification sequences.
- 03 Ask your agent to generate a notification path or contact card.
- 04 Use the agent to verify information permissions before sharing data.

Connect the MCP to your AI client to start managing emergency protocols.

Built For

This MCP is built for professionals managing safety protocols and emergency response plans.

Safety Officers

They hand off the management of contact lists and escalation paths to the AI.

Care Coordinators

They use the AI to ensure information boundaries are respected during medical incidents.

Emergency Managers

They rely on the AI to trigger the correct notification sequences automatically.

What Changes When You Connect

- 01 Automates the calculation of step-by-step notification paths.
- 02 Enforces data privacy by checking role-based information boundaries.

-
- 03** Maintains data accuracy through scheduled audit tracking.
-
- 04** Provides instant printable contact summaries for authorized users.
-

Real-World Applications

Medical Incident Response

Your agent follows a specific sequence to notify family members while restricting sensitive data to authorized personnel.

Facility Safety Audits

You use the review schedule to ensure all emergency contact information is updated every quarter.

Rapid Contact Retrieval

During an emergency, your agent generates a printable card for a primary contact immediately.

Role-Based Access Control

The AI prevents a neighbor or unauthorized contact from seeing private medical details during a call.

Patterns to Avoid

Manual escalation guessing

❌ AVOID

During a crisis, a manager tries to remember the exact order of family members to call. They end up calling a secondary contact before the primary one.

✓ INSTEAD

Let your agent handle the logic by using `generate_notification_sequence` to get the exact order of notifications.

Ignoring data privacy

❌ AVOID

A staff member shares a full medical history with a neighbor who is listed as an emergency contact. This violates privacy protocols.

✓ INSTEAD

Always use `check_information_boundaries` to see exactly what a specific contact is allowed to know based on their role.

Outdated contact lists

❌ AVOID

A safety officer realizes during an incident that the contact list hasn't been updated in a year. The phone numbers are all wrong.

✓ INSTEAD

Stay compliant and accurate by using `get_review_schedule` to track when your next mandatory audit is due.

The Right Fit

Safety officers and care coordinators should connect this MCP if they manage high-stakes emergency response plans. Organizations with loose, unverified contact lists should avoid it. You need this if your response depends on strict, role-based information boundaries.

Care Emergency Contact Plan 4 Tools

These tools manage notification logic, role-based data permissions, and mandatory audit schedules.

#	TOOL	DESCRIPTION
01	get_review_schedule	This tool provides your next required contact plan audit. Use it to maintain data integrity through regular reviews.
02	check_information_boundaries	This tool determines what specific information a contact is permitted to receive. It checks permissions based on the contact's assigned role.
03	generate_notification_sequence	This tool calculates the step-by-step escalation path for an emergency. It defines the order in which people must be notified.
04	get_contact_card	This tool generates a formatted, printable summary for an authorized contact. It's useful for quick physical reference during an incident.

See It in Action

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

U Generate a contact card for contact ID 'user-123'.



Name: Jane Doe, Role: Spouse, Method: Phone Call, Number: +1-555-0101, Location: New York, USA

U What is the notification sequence for an 'Immediate' priority emergency?



1. John Doe (Phone Call), 2. Mary Smith (SMS), 3. Local Police (Voice).

U Can a neighbor receive medical details during a 'Medical' incident?



No, for a 'Medical' incident, a neighbor is restricted to notification only and cannot access sensitive medical data.

Frequently Asked Questions

01 How does this MCP handle data privacy?

The MCP uses the `check_information_boundaries` tool to ensure contacts only receive information permitted by their specific role.

02 Can I print contact information?

Yes, the `get_contact_card` tool creates formatted, printable summaries for authorized contacts.

03 How often should I review my emergency contacts?

The MCP tracks mandatory quarterly audits through the `get_review_schedule` tool to keep your data current.

04 What happens during an emergency notification?

The agent uses the `generate_notification_sequence` tool to follow a pre-calculated, step-by-step escalation path.

05 Which AI clients can use this MCP?

You can connect this MCP to any compatible client like Claude, Cursor, Windsurf, or VS Code.

06 How can I see the contact details for a specific person?

You can use the `'get_contact_card'` tool by providing the specific contact ID to generate a printable summary.

07 How does the notification order work?

The system uses `'generate_notification_sequence'` to follow a strict call-tree hierarchy, ensuring contacts are reached in the correct priority order.

08 How often should I review my contact plan?

The plan requires a quarterly review. You can check your next scheduled audit using `'get_review_schedule'`.

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 <code>"care-emergency-contact-plan": { "url": "..." }</code>
 Windsurf	MCP Settings → <code>mcp_settings.json</code> → 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

Care Emergency Contact Plan 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 Care Emergency Contact Plan. 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	Care Emergency Contact Plan MCP
Server ID	01a0d435-8f8e-7366-8c87-43542b1c36e5
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/care-emergency-contact-plan.