

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 Document Access Plan MCP

Secure healthcare data access with least-privilege protocols.

Care Document Access Plan MCP manages sensitive healthcare document permissions and security protocols. It helps you enforce least-access rules, plan secure document storage, track permission expirations, and handle emergency break-glass access through your AI client.

A+ Quality Score 100/100

healthcare

security

compliance

access-control

data-retention



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 Document Access Plan MCP

4 tools available

Cloud-hosted on Vinkius

You can use this MCP to manage how sensitive healthcare data is handled across your organization. It focuses on the principle of least privilege, ensuring that staff members only see the specific documents they need to do their jobs. Instead of manually auditing access logs, you can ask your AI client to map out exactly who has permission to view certain medical records or sensitive files.

When you need to move data, the MCP helps you plan where those files should live to meet security requirements. It also keeps an eye on your compliance by identifying when permissions or documents are about to expire. If a critical situation arises, the MCP provides the specific protocols and contact info needed to trigger emergency access. It's a way to bring structured security planning directly into your AI-driven workflows.

Core Capabilities

01 — Access Mapping

Your agent uses this to define which staff members can view specific healthcare files.

02 — Storage Planning

Your AI client uses this to determine the most secure location for sensitive data.

03 — Expiration Tracking

Your agent uses this to flag documents or permissions that are nearing their end date.

04 — Emergency Protocols

Your AI client uses this to retrieve break-glass instructions when immediate access is required.

One Click on Vinkius — From Prompt to Execution

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

- 01

Connect your preferred MCP-compatible client to Vinkius.
- 02

Ask your AI client to perform a specific security task like mapping permissions.
- 03

The MCP executes the requested tool to pull or generate data.
- 04

Your agent presents the structured security information or plan directly in your chat.

Connect your AI client to Vinkius and start managing healthcare access through natural language.

Built For

This MCP is built for healthcare administrators and security officers managing sensitive patient data.

Compliance Officers

They use the MCP to verify that least-access principles are being followed.

Healthcare Administrators

They use the tool to manage staff permissions and document lifecycles.

IT Security Staff

They use the storage and emergency tools to maintain data integrity and availability.

What Changes When You Connect

- 01

Enforces least-access rules to limit data exposure.
- 02

Prevents service gaps by tracking permission expirations.
- 03

Provides clear instructions for emergency data access.

04 Automates the creation of secure document storage plans.

Real-World Applications

Permission Auditing

You can quickly generate a matrix to see if a specific nurse or doctor has the correct level of access.

Secure Data Migration

Use the storage map tool to plan where to move files when upgrading your security infrastructure.

Compliance Management

Monitor upcoming expirations to ensure all medical documents remain valid and compliant.

Crisis Response

Retrieve break-glass protocols instantly when a staff member needs urgent access to a locked file.

Patterns to Avoid

Manual permission auditing

❌ AVOID

You spend hours scrolling through spreadsheets to see if a new nurse has access to patient files.

✓ INSTEAD

Ask your agent to run ``get_permission_matrix`` to instantly see authorized personnel for specific document types.

Reactive expiration management

❌ AVOID

You realize a critical document permission expired only after a staff member is blocked from a file.

✓ INSTEAD

Use ``get_renewal_reminders`` to catch upcoming expirations before they cause service gaps.

Guessing storage locations

❌ AVOID

You move sensitive files to a new folder without checking if it meets your security requirements.

✓ INSTEAD

Run ``generate_storage_map`` to build a deployment plan based on your specific security needs.

The Right Fit

Healthcare administrators and security officers should connect this MCP to manage sensitive data lifecycles. IT staff who need to automate least-access enforcement will find it useful. If your organization does not handle regulated medical records or requires strict permission auditing, you don't need this MCP.

Care Document Access Plan 4 Tools

These tools manage healthcare data permissions, storage planning, and emergency access protocols.

#	TOOL	DESCRIPTION
01	get_emergency_access_instructions	This tool provides the specific protocols and contact details needed to trigger break-glass access during a crisis.
02	get_permission_matrix	This tool generates a structured map showing which personnel are authorized to access specific document types under least-access rules.
03	get_renewal_reminders	This tool identifies upcoming document or permission expirations to help you avoid service interruptions.
04	generate_storage_map	Use this to create a secure deployment plan for document placement based on your security needs and user preferences.

See It in Action

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

U Generate a permission matrix for Dr. Smith (Doctor) and Nurse Jones (Nurse) for Medical Records.



The permission matrix shows Dr. Smith has 'read' and 'write' access to Medical Records, while Nurse Jones has 'read' access.

U Where should I store highly sensitive Medical Records?



Medical Records should be stored in a High-Security Vault to meet security requirements.

U Are there any upcoming document expirations in the next 30 days?



Yes, the Identity Document for Patient ID-442 is set to expire in 12 days.

Frequently Asked Questions

01 How does this MCP handle emergency access?

It provides specific protocols and contact information needed to trigger break-glass access for critical situations.

02 Can I use this with Claude or Cursor?

Yes, you can connect this MCP to any MCP-compatible client including Claude, Cursor, and Windsurf.

03 What is the least-access principle mentioned?

It is a security rule where personnel are only granted the minimum level of access required to perform their specific job functions.

04 Does this help with document expiration?

Yes, the renewal reminders tool identifies upcoming expirations for documents or permissions to prevent interruptions.

05 How does it help with data storage?

The MCP can generate a secure storage map to plan where documents should be held based on security requirements.

06 How does the server enforce security?

The server uses the Least-Access Principle via the ``get_permission_matrix`` tool to ensure users only have the minimum permissions required for their roles.

07 Can I plan where to store medical records?

Yes, you can use ``generate_storage_map`` to create a secure deployment plan based on your specific storage preferences and document sensitivity.

08 What happens in an emergency?

You can retrieve specific break-glass protocols using ``get_emergency_access_instructions`` to handle urgent access needs safely.

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-document-access-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 Document Access 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 Document Access 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 Document Access Plan MCP
Server ID	01a0d435-5f56-708b-acb4-56f2ece7a040
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-document-access-plan.