

MCP SERVER

NO CODE

CLOUD HOSTED

Care Records Transfer Plan MCP

Secure medical documentation transfers with strict consent protocols.

Care Records Transfer Plan MCP handles the heavy lifting of moving sensitive medical and care documentation. It enforces mandatory consent rules and maintains a verifiable chain of custody for every record. Your AI client uses this to build checklists, draft formal requests, monitor transfer progress, and follow specific escalation paths when records go missing.

A+ Quality Score 100/100

medical-records

consent

chain-of-custody

data-transfer

healthcare-compliance



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 Records Transfer Plan MCP

4 tools available

Cloud-hosted on Vinkius

Moving medical records isn't just about moving files; it's about maintaining a legal and ethical paper trail. This MCP acts as a management engine that enforces safety rules like Consent-Before-Sharing to ensure no data moves without authorization. You can rely on it to maintain a verifiable chain of custody throughout the entire process. Instead of manually tracking every step, you let your AI client manage the logistics. It builds the task lists you need to follow, drafts the formal messages required for origin and destination parties, and keeps a real-time eye on the status of every transfer. If a record is denied or a file goes missing, the MCP provides the exact escalation steps needed to resolve the issue. It turns a high-risk manual process into a structured, auditable workflow that keeps your documentation compliant and your transfers moving.

Core Capabilities

01 — Consent Enforcement

Your agent checks for required permissions before any data movement occurs.

02 — Chain of Custody

The MCP maintains a record of who has handled the documentation at every stage.

03 — Task Automation

Your AI client generates actionable checklists to guide the transfer process.

04 — Status Monitoring

The tool provides real-time updates on the progress of medical record movements.

05 — Error Resolution

Your agent accesses specific escalation protocols when transfers hit a roadblock.

One Click on Vinkius — From Prompt to Execution

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

- 01
- Connect your preferred MCP-compatible client to Vinkius.
- 02
- Ask your AI client to generate a transfer checklist for a specific request.
- 03
- Use the tool to draft necessary messages to the involved parties.
- 04
- Monitor the transfer progress and custody status through the AI interface.
- 05
- Follow the provided escalation steps if any issues arise during the process.

Connect your AI client to the Vinkius-hosted MCP to start managing transfers immediately.

Built For

Healthcare professionals and administrators who need to move patient data between facilities without breaking compliance rules.

Medical Records Coordinators

They hand off the task of tracking document movement and drafting requests to the AI.

Clinical Administrators

They use the MCP to ensure consent is verified before staff share sensitive files.

Health Information Managers

They rely on the chain of custody data to maintain audit readiness.

What Changes When You Connect

- 01
- Enforces Consent-Before-Sharing rules to prevent unauthorized data movement.
- 02
- Maintains a verifiable chain of custody for every medical record transferred.

- 03 Reduces manual errors by generating structured task checklists.
- 04 Provides immediate escalation paths for missing or denied records.

Real-World Applications

Patient Transfers

Moving clinical notes from a primary doctor to a specialist hospital.

Missing Data Recovery

Following escalation steps when a required lab result is not found in the transfer.

Audit Preparation

Using the chain of custody logs to prove documentation was handled correctly.

Formal Communication

Drafting standardized request messages to origin and destination parties.

Patterns to Avoid

Manual checklist creation

❌ AVOID

A coordinator tries to write out every single step for a complex patient transfer on a notepad. This leads to missed steps and compliance gaps.

✓ INSTEAD

Let your agent build the full protocol automatically using `generate_transfer_checklist` to ensure nothing is skipped.

Guessing escalation paths

❌ AVOID

When a specialist denies a record request, the admin spends an hour searching through policy manuals to find out who to call next.

✓ INSTEAD

Immediately use `get_escalation_steps` to find the exact protocol for handling denied consent or missing files.

Informal request drafting

❌ AVOID

Staff send quick, unformatted emails to other hospitals that lack the necessary legal or formal language for record transfers.

✓ INSTEAD

Use draft_request_messages to produce the specific, formal wording required for both origin and destination parties.

The Right Fit

Healthcare administrators and medical record coordinators should connect this MCP if they manage high-volume patient data transfers. It is not for general office staff or non-clinical personnel. The decision depends on whether your facility requires a verifiable chain of custody for every document moved.

Care Records Transfer Plan 4 Tools

These tools manage the logistics, communication, and error handling for moving medical documentation between facilities.

#	TOOL	DESCRIPTION
01	draft_request_messages	This tool generates formal communication templates for the parties involved in the transfer. It creates the specific wording needed for both the origin and destination contacts.
02	track_transfer_status	This tool gives your AI client a real-time snapshot of the transfer. It monitors both the progress and the current chain-of-custody status.
03	generate_transfer_checklist	This tool builds a structured list of every step required to complete a transfer. It ensures no part of the protocol is skipped during execution.
04	get_escalation_steps	This tool provides specific instructions for handling problems. Use it when you encounter missing records or denied consent requests.

See It in Action

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

U Create a transfer checklist for clinical notes from Dr. Smith to City Hospital via secure portal by tomorrow.



The transfer checklist includes: 1. Consent Verification for clinical notes, 2. Record Gathering, 3. Secure Portal Upload, and 4. Delivery Confirmation.

U Draft a message to the origin contact to request lab results for the transfer.



Dear Origin Contact, please provide the requested lab results to facilitate the transfer to the destination contact.

U What are the next steps if the lab results are missing?



The required action is to initiate an Origin Provider Audit to locate the missing lab results.

Frequently Asked Questions

01 How does this MCP ensure medical data is handled safely?

It enforces a Consent-Before-Sharing rule and maintains a strict chain of custody for all documentation.

02 What happens if a record transfer is denied?

The MCP provides specific escalation steps to help you handle denied consent or missing records.

03 Can I use this with Claude or Cursor?

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

04 Does Vinkius host the MCP?

Yes, Vinkius hosts and manages the MCP so it is ready to use as soon as you connect your client.

05 What kind of documentation can be managed?

The MCP is designed for medical and care documentation, including clinical notes and lab results.

06 How does the server ensure data security?

The server enforces strict Chain-of-Custody tracking and requires Consent-Before-Sharing to ensure no records are moved without explicit permission.

07 What happens if consent is denied?

If consent is denied, you can use `get\_escalation\_steps` to find the appropriate path, which typically prioritizes Patient Advocacy or Legal Review.

08 Can I track the location of the records?

Yes, by using `track\_transfer\_status`, you can see if the data is At Origin, In Transit, or Received.

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-records-transfer-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 Records Transfer 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 Records Transfer 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 Records Transfer Plan MCP
Server ID	01a0d525-a8ef-7376-8843-f043fa664d1e
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-records-transfer-plan.