Norris Codex

TECHNICAL COMPLIANCE BRIEF

For county & provider IT directors, security officers, privacy officers, and procurement reviewers — readable in fifteen minutes.

MINNEAPOLIS, MN 55407

PATENT PENDING

Norris Codex is documentation-quality infrastructure for Minnesota Home & Community-Based Services case management — a Chrome-based workflow engine used by lead-agency waiver case managers and 245D provider staff who also work in SSIS, MnCHOICES, Procentive, and InSync. It runs **alongside** those systems without integrating with, reading, or modifying them, produces audit-ready outputs in under 120 seconds, and is **designed from inception to operate without ingesting Protected Health Information (PHI) at the architectural layer**. Two properties recur throughout: it does not ingest PHI, and its outputs are **source-bound** — the engine structures and checks what the worker records and does not manufacture case-specific facts. "Audit-ready" means structured to the DHS 245D Service Recipient Record Checklist and related § 245D record-management requirements.

1 Purpose of this brief

This brief answers the specific technical, privacy, and compliance questions an IT director asks before allowing the Norris Codex Chrome workflow engine to run on county or provider case-manager workstations. It is paired with the Norris Codex one-page product overview.

2 How the extension interacts with the page (isolation discipline)

The extension uses explicit context isolation and reads text **only on an explicit, affirmative user action**. There is no background scraping, no automatic page-content harvest, no listener that reads content when the user is not engaging the extension, and no script injection into any host page.

2.1 Explicit user action required

For browser content, the extension reads text only when the user (a) highlights text and invokes Norris Codex from the right-click menu, (b) presses the designated shortcut while text is selected, or (c) pastes text into the extension panel. Absent one of these actions, it reads nothing. For desktop applications such as SSIS, only method (c) applies.

2.2 Explicit context isolation

The extension runs in an isolated execution context under Chrome Manifest V3. It shares no variables, globals, or DOM access with any host page; it cannot read a host page's passwords, form data, cookies, or session storage, and a host page cannot read the extension's internal state. Enforced by Chrome at the runtime level.

2.3 No script injection into host pages

It injects no scripts into any host web page (MnCHOICES, Procentive, InSync web interfaces). It does not modify a host page's DOM and does not alter form submission, network requests, or rendering.

2.4 SSIS & systems of record — no integration, no overlay

SSIS is a desktop application, not a browser page, so the extension has **no technical ability to read, overlay, integrate with, or modify SSIS** — or any system of record. Content reaches Norris Codex only if a case manager deliberately copies and pastes it. By design it is a user-driven copy-paste assistant — not a screen-scraper, integration, overlay, or agent.

3 Output integrity & anti-fabrication controls

Source-bound generation. Every element of an artifact derives from the text the user supplies. The workflow does not infer, estimate, or manufacture case-specific facts — durations, times, observations, identifiers — absent from the input.

The "Information Required" rule. When a required element is not supported by the input, the workflow writes `INFORMATION REQUIRED` rather than a plausible value. It flags the gap for the human to complete, never fills it with an invention — enforced product-wide.

Automated quality gates. Each output is validated against a locked set of gates enforcing structural completeness, presence of every required element, and temporal anchoring consistent with the input. An output that fails a gate is not returned as a final artifact.

Human-in-the-loop. Every artifact is labeled DRAFT and carries a standing notice that it requires independent human judgment. The case manager remains author of record; Norris Codex is a drafting and completeness-checking instrument, not an autonomous decision-maker.

Statutory traceability. Each required element in an audit-readiness output maps to its governing subdivision of the § 245D.095 record-requirements statute, so a reviewer can trace any finding to the law it rests on rather than to a checklist form.

> **Why it matters:** case-management documentation is the basis for Medicaid billing and federal financial-participation claims, so a fabricated detail would be a fabricated billing record. The anti-fabrication design means an artifact never asserts a service fact the worker did not record.

4 Inference & data-privacy posture (Phase 3 pilot)

Inference runs through the **Logic Socket** provider-abstraction layer, routing **exclusively to AWS Bedrock**. Anthropic Claude is the current primary model; the Logic Socket selects the model within Bedrock. No inference is routed outside AWS Bedrock — there is no third-party fallback path.

- **U.S. regions only.** All inference routes through U.S. regions of AWS Bedrock; none leaves the U.S. Enforced at the AWS account level via IAM region restrictions on the dedicated Norris Codex pilot account.
- **Non-training.** Inference runs under enterprise non-training terms; inputs are not used to train, fine-tune, or improve the models (AWS Bedrock enterprise terms; Anthropic non-training terms).
- **Minimal retention.** Request/response bodies are treated as sensitive and are not written to application logs, analytics, monitoring, or any database. Only non-sensitive aggregate metrics (token counts, average completion time) are retained.
- **No fine-tuning on user inputs.** No fine-tuning, embedding generation, or model-customization on user inputs. The RAG corpus is built exclusively from public regulatory documents and licensed references; no customer data enters it.
- **Cryptographic session clearing.** At session end the application cryptographically clears in-memory session data. No persistent local storage of inputs, outputs, or session metadata beyond what the browser preserves under user control.

5 Business Associate Agreement posture

The architecture is designed to operate without ingesting PHI. Even where that posture removes most of the HIPAA risk surface, Norris Codex maintains a Business Associate posture as **defense-in-depth** for any customer that determines a BAA is required.

The BAA is prepared by Norris Codex's **outside legal counsel**, consistent with the standard 45 CFR Part 164 Subpart E provisions, modified to reflect the no-PHI architecture and the minimal-retention configuration in Section 4. It is finalized and executed alongside the Phase 3 Pilot Agreement in the August 2026 activation window; county/provider counsel may register interest in advance (Section 10).

Customers retain responsibility to ensure case managers do not paste PHI into the extension. The user-facing Safety Notice explicitly instructs users not to enter PHI, highly sensitive personal data, or anything they are legally prohibited from sharing.

6 SOC 2 Type II roadmap

Norris Codex is on a SOC 2 Type II readiness track — **a roadmap, not a current attestation** — targeting attestation in Q2–Q3 2027. Interim posture:

Q2 2026	Documented information-security policy stack: access control, change management, incident response, data handling (current).
Q3 2026	AWS CloudTrail audit logging on the Bedrock account with quarterly review documentation.
Q4 2026	HIPAA Security Risk Analysis (45 CFR 164.308(a)(1)(ii)(A)); one-page Incident Response Plan; workforce HIPAA awareness training; engage a CPA firm with SOC 2 capability.
Jan 1 2027	SOC 2 Type II observation window opens (proposed Jan 1–Jun 30, 2027). Trust Services Criteria: Security; Confidentiality & Availability under review.
Q2–Q3 2027	SOC 2 Type II audit & attestation report; published on request to procurement gates.

7 Architectural footprint on the county network

Norris Codex deploys **exclusively as a Chrome browser extension**, supported through Google Chrome Enterprise central policy management the county IT team already uses. It requires **no new servers, network access, firewall rules, VPN configuration, Active Directory integration, database tables in SSIS or MnCHOICES, or backend integration**.

Extension traffic egresses over standard HTTPS on port 443 to the Norris Codex endpoint, which then communicates with AWS Bedrock (Section 4). **No inbound network access to county systems is required.**

8 Data sovereignty & cryptographic clearing

Session data is held only in volatile memory during a session and is cryptographically cleared at termination. The application maintains no persistent storage of inputs, outputs, or session metadata. The RAG corpus contains only public regulatory and reference documents — no customer data, no PHI, no personally identifiable information.

9 Minnesota Government Data Practices Act posture

Data handled by county lead agencies under Minn. Stat. § 256B.0911 and adjacent waiver authorities may be classified under the Minnesota Government Data Practices Act (Minn. Stat. ch. 13). A Phase 2 legal memorandum by outside counsel — on a **July 31, 2026** delivery target, ahead of the August 2026 pilot — addresses classification of MnCHOICES support-plan data elements and confirms that the stateless, zero-retention architecture satisfies the handling requirements for the applicable classification. Available on request to county counsel under confidentiality.

10 Single point of contact

JR Fuller — Founder & Chairman, Norris Codex LLC

612-405-0117 · jrfuller@norriscodex.com · Minneapolis, MN 55407

IP status: Patent Pending. Non-provisional patent filing in preparation ahead of the hard November 13, 2026 deadline; specific application details available to counsel/procurement under NDA.

This brief is a Chairman-authored description of the Norris Codex technical posture as of the document date. It is informational; it does not modify the Business Associate Agreement, Master Services Agreement, Pilot Agreement, or any contract instrument. Specific procurement, contract, and indemnification language is delivered through Norris Codex's outside counsel of record.