

AI Tooling Inventory: The Manual Workflow

This document outlines the step-by-step manual process for identifying and classifying generative AI systems within a healthcare organization. It specifically targets the five ways AI enters an environment, including the four paths that evade standard procurement controls.

Phase 1: Zero-Ticket Discovery (The First Pass)

Run this entirely on your own authority, without requesting elevated IT access.

1. The Interview (The Primary Instrument)

Do not start with IT reports. Start by asking staff, framing questions as fixing a control gap, not investigating misconduct.

- **Workflow Pressure:** Ask functions with high document volume (intake, prior authorization, billing) if anyone has automated parts of the work.
- **The Capable Individual:** Ask who is known for building their own shortcuts. In-house tooling clusters around one or two people.
- **Shared Prompts:** Ask if anyone maintains custom instructions or shared prompts that colleagues use. A shared prompt is a system.
- **Authoring Disclosure:** Ask if any policies, compliance reports, or patient-facing letters were drafted with generative AI assistance.

2. Self-Inspection Checks

Walk through these checks with the staff during the interview:

- **Own-account Connected Apps:** Have them

check their Microsoft My Apps portal or Google linked-apps page. Record what they find.

- **Browser Extensions:** Have them check `chrome://extensions` or `edge://extensions` for anything that reads page content or the clipboard.
- **Inbox Search (Crucial):** Have them search their work email for "verify your email", "welcome to", or "confirm your account". This catches email/password signups that OAuth logs structurally miss.

3. Vendor Coverage Gap Identification

For every product already approved that was not acquired for its AI (EHR, practice management, transcription, phone systems), ask yourself this coverage question:

- Do we know exactly which AI features are enabled on this tenant, what data they process, and which subprocessors are involved?
 - If you cannot confidently answer this, you have identified a gap. Write to the vendor to secure written confirmation.
-

Phase 2: Artifact Harvesting

Use these to corroborate the interview, not replace it.

- **Vendor or BAA Register:** Confirms recognized relationships.
 - **Software Spend Export:** Identifies licensed and expensed tools, but misses free tiers.
 - **Platform App Directories:** Identifies integrations attached to approved platforms.
-

Phase 3: Classification & Evaluation

For every tool discovered, perform the following evaluations:

1. Classify the Entry Path

- **Licensed purchase:** Acquired through standard procurement.

- **Built in-house:** Built on a model subscription already held.
- **Feature activated:** Shipped inside an approved product.
- **Integration attached:** Connected to an approved platform (often without an agreement).
- **Free third-party tool:** Signed up for with a work email or free tier.

2. Evaluate ePHI Contact

Evaluate what the tool actually processes, not what it is licensed to do.

- **Confirmed:** Documented processing of identifiable health info.
- **Likely:** Processes a document class (or holds scopes) that routinely reaches ePHI.
- **Unlikely:** Operates only on material with no path to identifiable health info.

3. Assess Defensibility (The 4 Dimensions)

For each tool, verify:

1. Is an **agreement** (BAA) in place with the actual operator?
 2. Is there a **named owner**?
 3. Has it been **verified** against a graded set?
 4. Is it in the organization's current **risk analysis scope**?
-

Phase 4: Producing Findings

- **Critical Findings:** Apply when ePHI contact is confirmed/likely AND no agreement is in place, OR the tool is missing from the risk analysis.
- **High Findings:** Apply when ePHI contact is confirmed/likely but there is no named owner or verification.
- **Authoring-Disclosure Findings:** Apply retrospectively if documents were drafted with AI on a consumer tier.

Note: If at any point you discover ePHI was transmitted to an external system without an agreement, pause the assessment. This is an incident tripwire that requires legal counsel review.

