# AI Use Policy for Medical Practices: Free Template Guide

Published July 4, 2026 45 min read


AI Use Policy for Medical Practices: Free Template Guide

# AI Use Policy for Medical Practices: Free Template Guide

## Executive Summary

Medical practices in the United States are adopting artificial intelligence (AI) faster than most of them are governing it, and that gap is now the central compliance risk in outpatient medicine. As of the American Medical Association's (AMA) 2026 Physician Survey on Augmented Intelligence, **81% of physicians report using AI professionally**, more than double the rate recorded when the AMA first asked the question in 2023 (Source: www.ama-assn.org). Yet a January 2026 poll by the Medical Group Management Association (MGMA) found that only **42% of medical group leaders** say their organization has a formal AI governance policy in place or is actively building one, while a majority, 56%, still have nothing written down (Source: www.mgma.com). That governance lag, layered onto a healthcare data breach environment where the average incident already costs **$10.93 million**, the highest of any industry IBM and the Ponemon Institute track, is why an **AI use policy**, a written document that defines what staff may and may not do with AI tools, who approves new tools, and how patient data is protected, has become a baseline compliance artifact rather than an optional nicety (Source: www.ibm.com).

This report explains what a defensible AI use policy for a medical practice must contain, how the regulatory landscape now forces specific provisions into that document, and how a practice builds and rolls one out. At minimum, an effective policy defines AI and generative AI in plain terms, names an accountable governance owner or committee, sets explicit rules for what can and cannot be entered into consumer AI tools such as ChatGPT, requires a signed HIPAA Business Associate Agreement (BAA) before any vendor touches protected health information (PHI), mandates human review of AI-generated clinical content before it is relied upon or filed in the record, and establishes a channel for staff to report AI errors or "hallucinations." The Health Insurance Portability and Accountability Act (HIPAA) does not create new rules for AI, but its existing Privacy and Security Rules apply in full: any AI vendor that creates, receives, maintains, or transmits PHI on a practice's behalf is a business associate and must sign a BAA before that data ever reaches the tool (Source: www.hhs.gov.

State law has moved even faster than federal guidance. Texas requires AI-using health care practitioners to disclose that use to patients and to review every AI-generated medical record for accuracy under Senate Bill 1188, effective **September 1, 2025**, and its companion Texas Responsible AI Governance Act notably "also requires that HCPs notify patients when using AI tools for treatment" (Source: www.sheppard.com). California's Assembly Bill 3030 has required AI-generated clinical communications to carry a disclaimer and human-contact instructions since **January 1, 2025** (Source: leginfo.legislature.ca.gov), and by 2027 Illinois, Colorado, and additional states will have layered on their own disclosure and behavioral-health-specific restrictions, detailed in Table 2 below. Enforcement is real: Texas's 2024 settlement with Pieces Technologies, over an advertised "severe hallucination rate" of fewer than one in 100,000, shows regulators are already testing AI accuracy claims against consumer protection law, not waiting for AI-specific statutes (Source: www.texasattorneygeneral.gov).

Health systems that have governed AI deployment carefully report strong results: Kaiser Permanente's ambient documentation rollout reached **8 regions, 600 medical offices, and 40 hospitals**, supporting more than **4 million** patient encounters with structured quality assurance built in from the start (Source: permanente.org), and Mass General Brigham's phased "clinical trial" approach to its ambient scribe program grew from 20 pilot physicians to roughly **800 clinicians** without a reported hallucination in the reviewed workflows (Source: www.beckershospitalreview.com). By contrast, an Associated Press investigation found that OpenAI's Whisper transcription tool, used by some medical centers, occasionally fabricates racial commentary and clinically consequential text that was never spoken (Source: www.pbs.org), a cautionary case for why human review provisions are not optional in any policy. This report walks through the policy's required components, the regulatory drivers behind each one, a step-by-step build process, the freely available templates a practice can adapt (from bodies such as the Community Health Care Association of New York State, the Arizona Healthcare Financial Management Association, the Mississippi Artificial Intelligence Network, and the Joint Commission with the Coalition for Health AI), and the data and case evidence that should inform a practice's risk posture going into 2027.

## Introduction and Background

Generative AI arrived in outpatient medicine faster than almost any prior health information technology. Ambient listening tools now draft clinical notes in real time, chatbots triage patient portal messages, and revenue cycle software predicts claim denials before they happen. The AMA's most recent survey found physicians are using health AI to summarize medical research (39%), draft discharge instructions and progress notes (30%), document billing codes (28%), and draft responses to patient portal messages (19%) (Source: www.ama-assn.org). At the same time, an MGMA poll from August 2025 found **71% of practice leaders report some use of AI for patient visits**, though nearly half of those confine it to a quarter or less of encounters (Source: www.mgma.com). This is not a niche experiment; it is the working reality of a majority of American medical practices in mid-2026.

Governance has not kept pace with adoption. A joint MGMA and Humana study conducted in late 2024 found that **73% of surveyed organizations did not have a formal governance structure for AI use**, even as adoption accelerated (Source: www.mgma.com). More recent data suggests the picture is improving only slowly: as of January 2026, that gap had narrowed to 56% of practices with no policy and no plan to build one (Source: www.mgma.com. Similarly, healthcare compliance vendor Polygraf AI, drawing on adoption survey data, states that **46% of US healthcare organizations are now implementing AI, but most have no written policy governing what staff can and cannot enter into AI tools** (Source: polygraf.ai).

The stakes of that gap are concrete. A single staff member pasting a patient's name and diagnosis into a consumer chatbot to "clean up" a message is, in most circumstances, an impermissible disclosure of PHI under HIPAA, because most consumer-facing AI products will not sign a BAA and may retain user inputs to improve their models (Source: www.hipaajournal.com). Beyond privacy exposure, AI-generated clinical content can simply be wrong. A modified Physician Documentation Quality Instrument survey embedded in Kaiser Permanente's rollout found that even a largely successful ambient-notes program produced errors that required physician correction, underscoring why review requirements matter regardless of how well a tool performs on average (Source: permanente.org). This report treats an **AI use policy** as the primary control instrument a medical practice has to close that gap: a single governing document (sometimes paired with shorter procedures and a living tool registry) that translates HIPAA, state disclosure law, and clinical safety practice into rules staff can actually follow. IntuitionLabs, a life sciences and AI consultancy that works alongside regulated healthcare and pharmaceutical organizations on AI governance and Veeva-adjacent data infrastructure, frames this challenge the same way regulators increasingly do: as a compliance and change management problem first, and a technology procurement problem second (Source: intuitionlabs.ai).

## What an AI Use Policy Is and Why Medical Practices Need One

An **AI use policy**, sometimes called an AI acceptable use policy or an AI governance policy, is a written organizational document that defines the scope of AI covered, states who may use which tools for which purposes, sets data handling and privacy rules, assigns approval authority, and establishes consequences for violations. It differs from a generic technology use policy because AI introduces failure modes that ordinary software does not: models can "hallucinate" plausible-sounding but false content, they can absorb and later resurface sensitive inputs, and they can encode bias that is difficult to detect from a single output. A widely circulated model policy from the Community Health Center Association of New York State (CHCANYS) captures this succinctly, warning that AI tools "generally provide confident-appearing output, making it difficult to assess when the output may be inaccurate" (Source: www.chcanys.org). This opacity is closely related to what the Joint Commission and CHAI's guidance calls "the lack of transparency in AI decision-making processes, often referred to as the 'black box' problem," which the guidance identifies as a central obstacle to accountability in health AI deployments of any size (Source: digitalassets.jointcommission.org).

A useful taxonomy separates the AI a practice will actually encounter into five categories, each of which needs its own policy language rather than a single blanket rule:

- **Ambient clinical documentation ("AI scribes")**: tools that listen to or transcribe a patient encounter and draft a note. These tools were the single most uniformly adopted AI use case among the health systems surveyed by researchers publishing in the Journal of the American Medical Informatics Association, with **100% of the 43 responding health systems reporting at least piloting activity** (Source: pmc.ncbi.nlm.nih.gov).
- **Clinical decision support and diagnostic AI**: software that suggests diagnoses, flags risk, or assists interpretation of images or labs. Much of this category is regulated directly by the Food and Drug Administration (FDA) as Software as a Medical Device (SaMD); the agency's public list of authorized AI-enabled medical devices carried **1,524 entries** as of the researched period, and FDA states the list "can also provide transparency for healthcare providers and patients to clearly identify when medical devices use AI technologies" (Source: www.fda.gov) (Source: www.fda.gov).
- **Administrative and revenue cycle AI**: prior authorization drafting, denial prediction, coding assistance, and scheduling. MGMA identifies this as one of the three most common uses among practices experimenting without formal governance (Source: www.mgma.com.
- **Patient-facing AI**: chatbots, symptom checkers, and automated portal-message drafting, which carry distinct transparency obligations because the patient, not just the clinician, is interacting with the system.
- **General-purpose consumer generative AI**: tools such as ChatGPT, Claude, or Gemini used through their public consumer interfaces for tasks unrelated to a specific vetted workflow. This is the category with the highest PHI exposure risk and the one most model policies restrict most

tightly.

The rationale for writing a policy rather than relying on informal norms is threefold. First, HIPAA liability does not wait for a formal breach: entering PHI into an unapproved AI tool is itself a use or disclosure that must be authorized, and CHCANYS's model policy states plainly that doing so "likely violates HIPAA and potentially other state privacy laws" (Source: www.chcanys.org). Second, state disclosure and review laws (detailed below) now impose duties directly on the "health care practitioner" and the "health facility, clinic, physician's office," not on the AI vendor, so a practice cannot outsource compliance by contract alone. Third, in the absence of written rules, staff will improvise: MGMA's governance analysis warns that "if your policy doesn't create a safe, approved path, staff will create their own," citing a cybersecurity practitioner's observation that "when using tools like ChatGPT or other generative AI platforms, you don't always know where the data is going" (Source: www.mgma.com).

# Core Components of a Medical Practice AI Use Policy

A defensible policy is not a single paragraph banning AI, nor is it a permissive memo that simply encourages "responsible use." Reviewing the model policies published by CHCANYS, the Arizona chapter of the Healthcare Financial Management Association (HFMA), the Mississippi Artificial Intelligence Network (MAIN), and the Joint Commission's guidance developed with the Coalition for Health AI (CHAI), a consistent structure of eight core components emerges.

## Governance Structure and Accountability

Every model reviewed calls for a named, cross-functional governance owner. HFMA's template calls for "an AI Governance Committee... comprising representatives from clinical leadership, IT, legal, compliance, data science, and patient advocacy," with responsibility for "AI strategy, policy enforcement, risk management, and continuous evaluation" (Source: www.hfma.org). The Joint Commission and CHAI's Responsible Use of AI in Healthcare (RUAIH) guidance makes the same point for smaller organizations, noting the governance function "does not need to be its own standalone team" but must include "a designated individual(s) with appropriate technology expertise" and a mechanism to keep the practice's leadership "updated on uses, outcomes, and potential adverse events" (Source: digitalassets.jointcommission.org). For a solo or small group practice, this may be a single physician-owner paired with an office manager and outside compliance counsel; for a larger group, MGMA recommends a formal working group that functions "like a formulary committee meets change-management committee" (Source: www.mgma.com). Whatever its size, the governance function should maintain a "central inventory of AI tools in use, including AI features embedded in the electronic health record and other software, with their data flows, intended use, validation status, and owners," so the committee is never governing blind (Source: mainms.org).

## Permitted and Prohibited Uses

The policy must draw an explicit line between low-risk drafting tasks and prohibited PHI exposure. CHCANYS's model language permits publicly available AI tools for tasks such as "internal presentations," "grant or other applications," and "patient educational materials that summarize complex general medical or medication information," provided no Personal Information or Confidential Information is entered, while flatly prohibiting entry of "Personal Information, including PHI, into any publicly available AI tools, such as ChatGPT, or publicly available chatbots" (Source: www.chcanys.org). MGMA advises practices to define at least five distinct categories that will be governed differently: consumer generative AI, enterprise generative AI with contracted data terms, AI embedded in the electronic health record (EHR) or revenue cycle platform, predictive and machine-learning risk models, and patient-facing AI (Source: www.mgma.com. A policy that treats "AI" as one undifferentiated category will either be too restrictive to be usable or too permissive to be safe. Any category involving diagnosis, treatment, or bias-sensitive triage should also carry an explicit fairness check, since HFMA's governance template requires that "models must be tested for demographic fairness and adjusted to prevent disparate impacts" before deployment (Source: www.hfma.org).

## Protecting Patient Data and PHI (HIPAA and Business Associate Agreements)

This is the section auditors and regulators will scrutinize first. HIPAA's Privacy Rule requires covered entities to enter into a business associate contract with any vendor that creates, receives, maintains, or transmits PHI on their behalf, including AI vendors and the cloud service providers that host them (Source: www.hhs.gov. The Department of Health and Human Services' Office for Civil Rights (OCR) is explicit that using a cloud service to store or process electronic PHI without first executing a BAA is itself a Rules violation (Source: www.hhs.gov. OpenAI offers BAAs for eligible API configurations and certain products, including sales-managed ChatGPT Enterprise or Edu accounts, ChatGPT for Healthcare, ChatGPT for Clinicians, and Enterprise regulated workspaces; ChatGPT Business is not eligible. A BAA covers only eligible products and functionality and does not, by itself, make every feature or configuration HIPAA compliant ( OpenAI BAA eligibility; HIPAA-eligible products and functionality. This supersedes older secondary summaries such as (Source: www.hipaajournal.com). CHCANYS's model policy adds an important operational control beyond the BAA

itself: unless a governance committee specifically approves otherwise, "all AI tools must be configured in 'incognito' mode or a similar setting so the AI tool or vendor cannot track Company data inputs and outputs or ingest them into the AI tool's learning model" (Source: www.chcanys.org). Notably, HHS guidance also confirms that a software vendor is not automatically a business associate: "the mere selling or providing of software to a covered entity does not give rise to a business associate relationship if the vendor does not have access to the protected health information," a distinction that matters when classifying locally hosted or air-gapped AI tools (Source: www.hhs.gov).

## Clinical Use, Generative AI for Clinicians, and Mandatory Human Review

Every model reviewed requires that a licensed clinician remain the final decision-maker. MAIN's template phrases the standard directly: "AI may support, but not replace, the professional judgment of licensed clinicians acting within their scope of practice. A qualified clinician remains responsible for clinical decisions and for reviewing AI-generated output, including ambient documentation, before it is relied upon or entered into the record" (Source: mainms.org). CHCANYS's policy adds a specific clause for diagnostic use: "If an AI tool is being used to support clinical decision-making, a clinician may not rely solely on the output of the AI tool but may consider the output as part of the factors and circumstances taken into account when making a clinical decision" (Source: www.chcanys.org). This provision is not theoretical: Texas SB 1188 now makes it a statutory requirement that a practitioner using AI for diagnosis or treatment "review all medical records created by AI to ensure they conform to records standards established by the Texas Medical Board" (Source: www.sheppard.com).

## Patient Transparency and Disclosure

A policy must decide, in advance, when and how a patient learns AI was involved in their care, because several states now require this by law. CHCANYS's model language states that "if AI is used in connection with an online or telephone chatbot, the chatbot must clearly and conspicuously disclose, prior to beginning a chat session, that responses are not generated by a human" (Source: www.chcanys.org). MGMA recommends that practices "figure out patient transparency" deliberately rather than by default, deciding which uses (diagnostic support, triage, patient messaging) require disclosure and which internal drafting tasks do not (Source: www.mgma.com).

## Vendor Management and Procurement

A policy that stops at internal staff behavior is incomplete, because most AI risk originates with vendors. MGMA recommends embedding vendor requirements directly into policy, not only into contracts, covering "data ownership and reuse," "security controls and breach notification expectations," and "update/change controls" (Source: www.mgma.com). CHCANYS's contract checklist adds confidentiality requirements, indemnification for third-party intellectual property claims, and "representations and warranties that the AI tool has been tested for its intended purpose and implicit bias" (Source: www.chcanys.org).

## Staff Training and AI Literacy

Every model calls for role-based training before staff use any approved tool, covering both what the tool can do and its known failure modes such as hallucination and bias. MAIN specifically recommends training that helps staff "recognize risks such as hallucination and bias, and know what is prohibited" (Source: mainms.org). HFMA's template requires that "training programs should include: AI literacy and basic principles. System functionality and limitations. Ethical use and patient communication" (Source: www.hfma.org).

## Incident Reporting, Monitoring, and Review Cadence

Finally, a policy needs a living feedback loop. The Joint Commission and CHAI's RUAIH guidance recommends "voluntary, blinded reporting of AI safety-related events" comparable to existing patient safety incident systems (Source: digitalassets.jointcommission.org). This mirrors an obligation that already exists for any AI vendor handling PHI: the HIPAA Security Rule "requires business associates to identify and respond to suspected or known security incidents... and document security incidents and their outcomes," so an AI-specific reporting channel should route directly into that existing compliance process rather than duplicate it (Source: www.hhs.gov. MGMA suggests a concrete reporting channel covering "hallucinated content in a note," "suspected bias in risk scoring," and "workflows where staff are bypassing safeguards" (Source: www.mgma.com). Among practices with formal policies today, MGMA reports "annual reviews being the most common," followed by quarterly or biannual cycles (Source: www.mgma.com), while HFMA's template calls for review "annually or upon significant changes in AI technology, regulations, or organizational strategy" (Source: www.hfma.org).

*Table 1* below summarizes these eight components alongside the primary regulatory or governance driver behind each, so a practice can trace every clause in its policy back to a specific requirement rather than writing from a blank page.

**Table 1. Core Components of a Medical Practice AI Use Policy**

| POLICY COMPONENT | WHAT IT MUST SPECIFY | PRIMARY DRIVER |
|---|---|---|
| **Governance structure** | Named accountable owner or committee; cross-functional representation; reporting to leadership | Joint Commission/CHAI RUAIH; HFMA template (Source: digitalassets.jointcommission.org) |
| **Permitted and prohibited uses** | Category-by-category rules (consumer AI, enterprise AI, embedded EHR AI, predictive models, patient-facing AI) | MGMA governance guidance (Source: www.mgma.com) |
| **PHI and HIPAA protections** | BAA requirement before PHI enters any tool; incognito or non-training mode by default | HIPAA Privacy and Security Rules; HHS OCR guidance (Source: www.hhs.gov |
| **Clinical use and human review** | Mandatory clinician review before AI content informs a diagnosis, treatment, or record entry | Texas SB 1188; state medical board record standards (Source: www.sheppard.com) |
| **Patient transparency** | Disclosure triggers, script language, and opt-out mechanics for AI-assisted communications | California AB 3030; Texas TRAIGA (Source: leginfo.legislature.ca.gov) |
| **Vendor management** | Data ownership, training-data prohibition, breach notification, and audit rights in contracts | MGMA and CHCANYS procurement checklists (Source: www.mgma.com) |
| **Staff training** | Role-based AI literacy covering hallucination, bias, and prohibited uses before tool access is granted | MAIN and HFMA templates (Source: mainms.org) |
| **Incident reporting and review** | Defined channel for AI errors; annual or more frequent policy review cycle | Joint Commission/CHAI RUAIH; MGMA polling of current practice (Source: digitalassets.jointcommission.org) |

Read across the eight rows, the pattern is that no single component stands alone: a governance committee with no defined permitted-use categories cannot make consistent decisions, and a strong HIPAA clause is undermined if there is no training requirement to ensure staff actually know it exists. Practices building a policy from scratch should treat this table as a coverage checklist, confirming each row is addressed in the final document even where the specific language is adapted to the practice's size and specialty mix.

## The Regulatory Landscape Shaping Healthcare AI Policy

No AI use policy for a medical practice can be written in a regulatory vacuum, because several distinct legal regimes now touch the same underlying activity: a clinician or staff member entering patient information into, or relying on output from, an AI tool.

**HIPAA remains the floor.** OCR has not issued AI-specific rules, and existing guidance from bodies summarizing the primer literature confirms the framework's core position: AI does not change the traditional HIPAA rules on how PHI may be accessed, used, or disclosed; it simply creates a new channel through which those rules can be violated. The proposed HIPAA Security Rule update, published for comment in January 2025 and not yet finalized as of the current reporting period, would further tighten cybersecurity expectations relevant to AI infrastructure, and practices should track its progress (Source: mainms.org).

**State disclosure and oversight law is now the fastest-moving layer.** *Table 2* summarizes the state statutes most directly relevant to medical practices as of the July 2026 research period.

**Table 2. State AI Disclosure and Oversight Laws Affecting Medical Practices**

| STATE / LAW | EFFECTIVE DATE | CORE REQUIREMENT FOR PRACTICES |
|---|---|---|
| **Texas SB 1188** | September 1, 2025 | Practitioner must act within license scope, ensure use is not otherwise restricted by law, review all AI-generated records for accuracy, and disclose AI use to patients (Source: www.sheppard.com) |
| **Texas HB 149 (TRAIGA)** | January 1, 2026 | "Clear and conspicuous" patient disclosure whenever AI is used in care, with an emergency-care exception (Source: mosaiclifetech.com) |
| **California AB 3030** | January 1, 2025 | AI-generated clinical communications must carry a disclaimer and instructions to reach a human provider, unless a licensed clinician reviewed the content first (Source: leginfo.legislature.ca.gov |
| **California AB 489** | January 1, 2026 | AI may not use professional credentials (MD, DO, RN, etc.) implying licensed human oversight where none exists (Source: mosaiclifetech.com) |
| **California SB 243** | January 2026 | AI companion and mental health chatbots must disclose they are not human, with added minor-protection safeguards (Source: mosaiclifetech.com) |
| **Illinois HB 1806** | August 2025 | Bars AI from independently making psychotherapy or treatment-plan decisions without licensed review; requires disclosure of AI use in behavioral health care (Source: mosaiclifetech.com) |
| **Colorado SB 26-189** | January 1, 2027 | Replaces the original Colorado AI Act's risk-management mandate with a disclosure-based framework and limited consumer rights (Source: mosaiclifetech.com) |

The pattern across these seven statutes is consistent even though the mechanics differ: disclosure to the patient, review by a licensed human, and record-keeping of that review are the three obligations that recur in nearly every state framework. A national practice's simplest compliance strategy is to build a single policy that meets the most stringent applicable state standard and apply it everywhere, rather than maintaining separate state-by-state tracks. Colorado's reversal is instructive on its own: the state's original AI Act would have required formal risk management programs and documented impact assessments for high-risk systems, but the legislature ultimately replaced that heavier mandate with a lighter, disclosure-based model, suggesting future state laws may converge on transparency requirements rather than additional process mandates.

**Federal device and coverage regulation adds a second layer for specific tools.** Any AI functioning as a medical device, most commonly in radiology, cardiology, and diagnostic imaging, falls under FDA's Software as a Medical Device framework, and a policy must track which tools in active use are FDA-authorized versus non-device administrative software so staff do not use a cleared tool outside its authorized indication (Source: mainms.org). Separately, Centers for Medicare and Medicaid Services (CMS) rules governing Medicare Advantage coverage determinations require that medical necessity decisions reflect the individual enrollee's circumstances rather than a blanket output, and CMS's 2024 final rule reinforces this by requiring that internal coverage criteria be based on current evidence and made publicly available, a standard industry guidance extends explicitly to any algorithm or AI used in utilization review (Source: www.cms.gov) (Source: mainms.org).

**The Federal Trade Commission (FTC) provides a fourth backstop.** Even where no AI-specific law applies, deceptive claims about an AI tool's accuracy or capabilities remain actionable consumer protection violations, and the agency has stated publicly that there is no AI exemption from existing law. Texas's enforcement action against Pieces Technologies, discussed in the case studies section below, was itself built on this consumer protection theory before any AI-specific Texas statute took effect.

**Voluntary frameworks round out the landscape.** The National Institute of Standards and Technology's (NIST) AI Risk Management Framework, released January 26, 2023, is voluntary but has become the de facto reference architecture nearly every model healthcare policy cites; it is "intended for voluntary use and to improve the ability to incorporate trustworthiness considerations into the design, development, use, and evaluation of AI products, services, and systems" (Source: www.nist.gov), and NIST supplemented it on July 26, 2024 with a Generative AI Profile addressing risks specific to large language models (Source: www.nist.gov). Section 1557 of the Affordable Care Act adds a nondiscrimination duty specific to "patient care decision support tools," which has applied since May 1, 2025 and survived a 2026 partial vacatur that removed only its gender-identity provisions while leaving the decision-support requirements intact (Source: mainms.org).

## Building and Implementing Your AI Use Policy: A Step-by-Step Guide

Practices asking how to create an AI acceptable use policy for healthcare, rather than simply what to include in one, typically follow a sequence close to the one the AMA's own "Governance for Augmented Intelligence" toolkit lays out: an eight-step path beginning with executive accountability and governance structure, then moving through working group formation, assessment of current state, policy development, vendor evaluation, implementation processes, oversight and monitoring, and organizational readiness (Source: www.mgma.com). A practice-sized adaptation of that sequence follows.

**Step 1: Assign an accountable owner and, where staffing allows, a small governance group.** For a solo or small group practice this may be the physician-owner plus the practice manager; for larger groups, MGMA recommends including "one physician champion, nursing/clinical operations, compliance/privacy, security/IT, revenue cycle, patient experience, and HR" (Source: www.mgma.com).

**Step 2: Inventory current AI use, including "shadow AI."** Before writing rules, find out what staff are already doing. MGMA's survey data shows the most common ungoverned uses are documentation efficiency (scribing, dictation, charting support), revenue cycle tasks (prior authorizations), and general administrative support such as meeting notes and scheduling (Source: www.mgma.com. This inventory should also capture AI features embedded in the practice's EHR and practice management software, since MAIN's template warns these are the most commonly overlooked source of "ungoverned EHR AI features" (Source: mainms.org).

**Step 3: Start from a free template rather than a blank page.** Several organizations publish adaptable, no-cost AI policy templates specifically for healthcare, summarized in *Table 3* below. Adapting an existing template, rather than drafting from scratch, is both faster and reduces the risk of missing a required clause.

**Step 4: Draft one umbrella policy, not a patchwork of tool-specific memos.** MGMA recommends starting with "one umbrella policy that defines 'AI' in your office," with clearly separated categories for consumer, enterprise, embedded, predictive, and patient-facing AI, so new tools can be classified quickly rather than triggering a fresh policy debate every time (Source: www.mgma.com).

**Step 5: Build a lightweight intake and approval process for new tools.** MGMA's minimum standard requires that any new AI tool trigger "a short use-case description; a data flow description (what goes in, what comes out, where it's stored); a pilot plan and success metrics; and an owner for monitoring and issue escalation" before adoption (Source: www.mgma.com). CHCANYS's model policy operationalizes this with a formal AI Request and Impact Assessment Form reviewed against the NIST AI Risk Management Framework before approval (Source: www.chcanys.org).

**Step 6: Pilot before scaling.** MGMA's suggested ambulatory-care timeline runs a 0-to-6-month phase piloting ambient scribes in select exam rooms and integrating patient-facing chatbots into portals, followed by a 6-to-12-month expansion phase with standardized templates and "AI super-users" leading peer training (Source: www.mgma.com). This mirrors the "clinical trial" approach used successfully at scale by Mass General Brigham, discussed in the case studies section.

**Step 7: Train before granting access, and require attestation.** Training should be role-based and completed before, not after, a staff member is granted access to an approved tool, covering both intended use and known failure modes.

**Step 8: Set a review cadence and a defined incident-reporting channel, then repeat.** Given how quickly both the tools and the state legal landscape are changing, most model policies recommend at minimum an annual review, with an interim review triggered by any new state law, a material vendor change, or a reported safety event (Source: www.hfma.org).

*Table 3* below compares the major free templates and frameworks a practice can draw on when executing Step 3, since this is one of the most commonly searched needs among practices starting this process from scratch.

**Table 3. Free AI Policy Templates and Governance Frameworks for Healthcare Organizations**

| RESOURCE | PUBLISHER | BEST SUITED FOR | NOTABLE FEATURE |
|---|---|---|---|
| **CHC Model Policy on the Use of AI** | Community Health Care Association of New York State (CHCANYS) | Community health centers and small to mid-size practices needing full contract and approval-process language | Includes a detailed prohibited/permitted use matrix and an AI Request and Impact Assessment Form (Source: www.chcanys.org) |
| **AI Governance Policy Template** | Arizona chapter, Healthcare Financial Management Association (HFMA) | Larger practices and health systems wanting a concise, board-ready governance skeleton | Explicitly aligns with the NIST AI Risk Management Framework and ISO standards (Source: www.hfma.org) |
| **AI Policy and Guidance Template for Healthcare** | Mississippi Artificial Intelligence Network (MAIN) | Practices wanting section-by-section sample language plus common pitfalls for each topic | Twenty-two sections spanning governance, HIPAA, FDA device status, coverage, HR uses, and training (Source: mainms.org) |
| **Responsible Use of AI in Healthcare (RUAIH)** | Joint Commission and Coalition for Health AI (CHAI) | Hospitals and practices preparing for accreditation-linked AI expectations | Defines seven elements of responsible use, from governance to voluntary safety-event reporting (Source: digitalassets.jointcommission.org) |
| **AI Risk Management Framework (AI RMF 1.0) and Generative AI Profile** | National Institute of Standards and Technology (NIST) | Any organization wanting the underlying risk taxonomy referenced by nearly every other template on this list | Voluntary, sector-agnostic, and the explicit foundation cited by CHCANYS, HFMA, and MGMA templates alike (Source: www.nist.gov) |

None of these five resources is a finished, ready-to-sign policy for any individual practice; each publisher explicitly says so, and MAIN's template states directly that its content "is not a final policy, not legal advice, and not a mandatory model" (Source: mainms.org). A practice should select the template whose structure best matches its size and specialty, then have compliance, privacy, and clinical leadership revise it against the practice's actual tool inventory and state law obligations, ideally with input from outside legal counsel before adoption. IntuitionLabs, in its work advising regulated life sciences and healthcare organizations on AI governance, similarly frames adaptation, not template selection alone, as the step that determines whether a policy is defensible in practice, since a generic document that is never mapped to a practice's specific vendor contracts and workflows offers limited protection in an actual OCR or state AG inquiry (Source: intuitionlabs.ai).

## Data Analysis and Evidence

The quantitative picture confirms both the urgency and the direction of AI policy adoption in medicine. On the adoption side, the AMA's 2026 survey of nearly 1,700 physicians found **81% now use AI professionally**, and among specific use cases, summarizing medical research and standards of care rose 33 percentage points from the 2023 survey to be cited by 39% of respondents, with translation services and assistive diagnosis following at 18% and 17% respectively (Source: www.ama-assn.org) (Source: www.ama-assn.org). Confidence is rising alongside use: in 2026, more than three-quarters of physicians believe AI improves their ability to care for patients, up from 65% in 2023 (Source: www.ama-assn.org). Yet the same survey found 88% of doctors report at least some concern about AI-related skill loss and 86% emphasize the importance of data privacy for broader adoption (Source: www.ama-assn.org, underscoring that enthusiasm and risk awareness are rising together, not in place of one another.

On the governance side, the gap between use and policy remains the defining statistic of this topic. MGMA's fall 2024 research with Humana found 73% of health systems lacked a formal AI governance structure (Source: www.mgma.com), a figure that had improved only to 56% still lacking any policy or plan as of MGMA's January 2026 poll of 328 practice leaders (Source: www.mgma.com). A separate survey of 43 Scottsdale Institute member health systems, published in the Journal of the American Medical Informatics Association, found that "immature AI tools" were the most frequently cited barrier to adoption, flagged by 77% of respondents, ahead of financial concerns at 47% and regulatory uncertainty at 40% (Source: pmc.ncbi.nlm.nih.gov. That same study found imaging and radiology AI was deployed in at least limited areas by 90% of responding systems, though ambient clinical documentation was the only use case with universal piloting activity across all 43 respondents (Source: pmc.ncbi.nlm.nih.gov.

Financial exposure gives the governance gap its urgency. Healthcare has recorded the highest average data breach cost of any industry that IBM and the Ponemon Institute track: **$10.93 million** per incident in the most recent comparative analysis available, against a global cross-industry average of $4.45 million (Source: www.ibm.com) (Source: www.ibm.com). Healthcare breaches also took longer to detect, an average of 213 days versus 194 days across other industries, extending the window in which unauthorized PHI exposure, including exposure through an ungoverned AI tool, can go unnoticed (Source: www.ibm.com). The inverse relationship is equally instructive: organizations making serious, well-governed use of automation and AI in their own security operations "enjoyed an average cost reduction of 1.76 million USD compared to those without such technologies," suggesting that the same discipline a practice applies to AI governance in clinical workflows pays off in cybersecurity outcomes as well (Source: www.ibm.com). IBM's 2025 edition of the same research, subtitled "The AI Oversight Gap," reframed this dynamic explicitly around governance: organizations that skip security and governance steps in favor of rapid AI adoption are, in the report's own framing, "more likely to be breached, and more costly when they are" (Source: www.bakerdonelson.com).

On the regulatory front, the FDA's public tally of authorized AI-enabled medical devices, which has grown to **1,524 entries** predominantly in radiology, cardiovascular, and neurology applications as of the current research period, illustrates how much of a practice's diagnostic AI exposure is already under a distinct, device-specific compliance regime that a policy must reference rather than duplicate (Source: www.fda.gov). Taken together, these figures describe a field where adoption, patient risk, financial exposure, and regulatory density are all rising simultaneously, which is precisely the condition under which a written, specific, and actively maintained AI use policy moves from best practice to necessity.

# Case Studies and Real-World Examples

## Pieces Technologies and the Texas Attorney General's 2024 Settlement

In September 2024, Texas Attorney General Ken Paxton announced what his office called the first-of-its-kind healthcare generative AI settlement, following an investigation into Pieces Technologies, a Dallas-based AI vendor whose product summarized patient condition and treatment information for hospital staff at, according to the settlement announcement, "at least four major Texas hospitals" in real time (Source: www.texasattorneygeneral.gov). The investigation found that Pieces had marketed an error rate, or "severe hallucination rate," of "<1 per 100,000" that the Attorney General's office determined "were likely inaccurate and may have deceived hospitals about the accuracy and safety of the company's products" (Source: www.texasattorneygeneral.gov). Under the settlement, Pieces agreed to accurately disclose the extent of its products' accuracy and to ensure hospital staff "understand the extent to which they should or should not rely on its products" (Source: www.texasattorneygeneral.gov). Paxton's public statement carries a direct message for practices building vendor-management policy language: "AI companies offering products used in high-risk settings owe it to the public and to their clients to be transparent about their risks, limitations, and appropriate use. Anything short of that is irresponsible... Hospitals and other healthcare entities must consider whether AI products are appropriate and train their employees accordingly" (Source: www.texasattorneygeneral.gov). The case is important precisely because it predates Texas's AI-specific statutes: it was built on ordinary consumer protection law, confirming that a practice's exposure exists whether or not an AI-specific statute is yet in force in its state.

## Kaiser Permanente's Governed, Large-Scale Ambient Documentation Rollout

Kaiser Permanente offers the clearest public example of governance scaling alongside adoption. Before its national rollout, the organization ran a 10-week pilot in early 2024, recruiting more than 1,000 physician users before expanding the tool system-wide across **8 regions, 600 medical offices, and 40 hospitals** (Source: permanente.org). A dedicated quality assurance team, including physicians, administrators, informaticists, and safety officers, tracked 63,000 patient encounters and reviewed more than 3,600 free-text clinician comments during the pilot (Source: permanente.org). The tool's use has remained voluntary for clinicians, who must obtain patient approval before recording a visit, and the underlying audio is not retained (Source: permanente.org). Results were largely positive but not uniform: 47% of rated encounters received five stars and 31% received four stars, while 7% received one or two stars, and a minority of users reported the tool had difficulty tracking multiple speakers or made erroneous assumptions later corrected by physicians (Source: permanente.org). Governance did not stop at deployment: the quality assurance team "communicated frequently with the software vendor during the QA evaluation, and the vendor made rapid improvements in response to user feedback," illustrating how a live feedback loop between practice and vendor is itself a governance control, not just a courtesy (Source: permanente.org). Kaiser Permanente's chief medical officer, Dr. Andrew Bindman, summarized the governance philosophy directly relevant to any practice-level policy: "Like any technology we adopt in the care setting, we thoroughly evaluate all AI-based tools and systems before use and regularly monitor their performance... our clinicians and care teams are the medical decision-makers, not AI" (Source: permanente.org). By the time of reporting, the tool had supported more than **4 million** patient encounters system-wide (Source: permanente.org).

### Mass General Brigham's Phased "Clinical Trial" Approach

Mass General Brigham took a deliberately incremental path with its own ambient documentation program, providing the technology first to just 20 physicians and evaluating workflow safety and technical stability before wider release (Source: www.beckershospitalreview.com). Reported results from that pilot, that the technology "ran without hallucinations" and drove enthusiasm that expanded adoption to roughly 800 physicians and advanced practice providers, led the health system to measure outcomes directly: around 60% of providers said they were more likely to extend their clinical careers because of the tool, 20% reported reduced burnout symptoms, and 80% said they spent more time looking at patients rather than the screen (Source: www.beckershospitalreview.com). The health system's chief medical information officer, Dr. Rebecca Mishuris, described the underlying governance question that any practice, regardless of size, must answer for each new AI use case: "Do we continue to use... our clinical trials-informed approach and how robust should that change be based on the risk of the application?" (Source: www.beckershospitalreview.com).

### The Whisper Transcription Hallucination Investigation

Not every deployment has gone as smoothly as Kaiser Permanente's or Mass General Brigham's, and the contrast is instructive for why human review provisions belong in every policy regardless of vendor reputation. This is a reported investigative finding, not a hypothetical scenario. An Associated Press investigation, reported on PBS NewsHour in January 2025, found that OpenAI's Whisper transcription tool, used by some medical centers to transcribe patient interactions, sometimes fabricates content, including in one documented example replacing a simple description of prayer with an invented and disturbing passage about violence (Source: www.pbs.org). The investigating reporter, Garance Burke of the Associated Press, found the tool "makes things up that can include racial commentary, sometimes even violent rhetoric," and specifically "incorrect words regarding medical diagnoses," raising direct concern for use "in really sensitive settings like in hospitals" (Source: www.pbs.org). Critically, the investigation found that not every healthcare adopter had built in the safeguard a strong policy would require: while some organizations fine-tuned the model and retained original audio for fact-checking against the AI transcript, "we did find one company that just threw out the original audio," removing the only means of verifying what a patient actually said (Source: www.pbs.org). OpenAI's own response acknowledged the limitation, stating its "usage policies prohibit use in certain high stakes decision making contexts" and that its model card for open-source use "includes recommendations against use in high risk domains" (Source: www.pbs.org), underscoring that vendor-provided guardrails only work if a practice's own policy actually reads and enforces them.

## Implications and Future Directions

The trajectory across adoption data, state legislation, and enforcement activity points toward three near-term shifts a medical practice's AI use policy should anticipate rather than react to. First, disclosure requirements are converging even as broad risk-management mandates recede: Colorado's replacement of its original AI Act with a disclosure-based framework mirrors the approach Texas and California already took, and this pattern, transparency obligations rather than heavier process requirements, appears likely to be the more common model as additional states legislate. A practice's disclosure and consent language, once drafted to meet the most stringent current state standard, should therefore be built to extend easily to new jurisdictions rather than rewritten from scratch each time a new law passes.

Second, accreditation is likely to formalize AI governance expectations that are currently voluntary. The Joint Commission's development of its Responsible Use of AI in Healthcare (RUAIH) guidance with CHAI, alongside a forthcoming voluntary certification program built on that guidance, signals that AI governance maturity may become a factor in accreditation and payer contracting discussions even for practices that never treat AI as a distinct regulatory category today (Source: digitalassets.jointcommission.org). Practices that build a governance structure now, even a lightweight one, are positioned to adopt that certification path incrementally rather than build a program from nothing under time pressure later.

Third, the compliance burden of ungoverned "shadow AI" is likely to grow faster than the direct cost of governed adoption. MGMA's own analysis frames this precisely: automation bias, where confident-sounding AI outputs go unchecked because staff simply stop double-checking, applies equally to clinical suggestions and to administrative decisions such as prioritizing insurance denials or flagging high-risk patients (Source: www.mgma.com). As AI becomes embedded by default inside EHRs and revenue cycle platforms rather than adopted as a distinct, deliberate purchase, a practice's policy will increasingly need to govern features it did not choose to buy, which raises the importance of the vendor-management and tool-inventory provisions discussed earlier over the historical model of approving discrete, named software products one at a time.

For practices seeking outside support in navigating this shift, particularly those operating in regulated life sciences and pharmaceutical-adjacent environments where AI governance intersects with Good Practice (GxP) quality systems, IntuitionLabs' advisory work illustrates the complementary role a specialized consultancy can play: translating frameworks such as the NIST AI Risk Management Framework and emerging state disclosure law into implementation plans mapped to an organization's actual systems and vendor contracts, rather than treating policy adoption as a document exercise disconnected from operations (Source: intuitionlabs.ai).

## Frequently Asked Questions (FAQs)

**What is an AI use policy template for healthcare, and where can a practice get one for free?** A template is a pre-drafted policy document covering governance, permitted and prohibited uses, HIPAA and data protections, clinical review requirements, patient disclosure, vendor management, training, and incident reporting, which a practice edits to match its own size, specialty, and tool inventory. Free healthcare-specific templates are published by CHCANYS, the Arizona chapter of HFMA, the Mississippi Artificial Intelligence Network, and the Joint Commission with CHAI, as summarized in Table 3 above (Source: www.chcanys.org).

**Does HIPAA require a specific AI policy, or does general HIPAA compliance cover AI use?** HIPAA has no AI-specific rule, but its existing Privacy and Security Rules apply fully to AI, meaning any vendor with access to PHI must sign a BAA, and PHI entered into a tool without one is a Rules violation (Source: www.hhs.gov. A written AI-specific policy is not itself a HIPAA mandate, but it is the practical mechanism most compliance professionals use to ensure staff actually follow HIPAA when using new AI tools, since a general HIPAA policy written before generative AI existed rarely anticipates chatbot prompts or ambient scribes as disclosure vectors.

**How do you create an AI acceptable use policy for a healthcare organization step by step?** Follow the eight-step sequence detailed above: assign an accountable owner, inventory current AI use including shadow AI, adapt a free template, draft one umbrella policy with clear tool categories, build a lightweight approval intake process, pilot before scaling, train staff before granting access, and set an annual (or more frequent) review cadence with a defined incident-reporting channel.

**What should a generative AI policy for clinicians specifically cover?** Beyond the general components above, clinician-facing provisions should require human review of every AI-generated note, diagnosis suggestion, or treatment recommendation before it is relied upon or filed in the record, consistent with Texas SB 1188's requirement that practitioners review all AI-generated records for accuracy (Source: www.sheppard.com), and should clarify that AI output may inform but never solely determine a clinical decision (Source: www.chcanys.org).

**What counts as an AI governance policy versus an AI use policy?** In practice, the terms are often used interchangeably, but "governance policy" more often emphasizes the committee, approval process, and oversight structure (who decides), while "use policy" or "acceptable use policy" more often emphasizes staff-facing rules (what staff may do). Most effective single documents, including the CHCANYS and MAIN templates reviewed here, combine both elements rather than separating them into two documents.

**What specific rules should govern AI and patient data or PHI?** At minimum: no PHI may be entered into any AI tool without an executed BAA; approved tools should be configured to prevent the vendor from using practice data to train its models unless the governance committee specifically approves otherwise (Source: www.chcanys.org); only the minimum necessary PHI should be entered for the tool to function; and any de-identification claimed must meet the HIPAA Privacy Rule's Safe Harbor or Expert Determination standard rather than an informal judgment that a record "looks anonymous" (Source: www.hipaajournal.com).

**What staff guidelines should apply to everyday AI use in a medical practice, beyond clinical documentation?** Front-desk, billing, and administrative staff need the same core prohibition on entering PHI into unapproved tools, plus specific guidance on de-identifying scenarios before using AI for tasks like drafting appeal letters or summarizing internal reports, and a clear escalation path if they are unsure whether a task is permitted (Source: www.mgma.com.

## Conclusion

The evidence assembled in this report points to a single, consistent conclusion: the question facing medical practices in 2026 is no longer whether to adopt AI, since 81% of physicians already have, but whether to govern that adoption deliberately or let it happen by default. The 42% of practices with a formal policy or one under active development are ahead of a regulatory curve that is tightening quickly, from Texas's disclosure and record-review mandates to California's three overlapping AI statutes to Illinois's behavioral health restrictions, while the majority still operating without any written policy carry real and quantifiable exposure, both to the HIPAA violations that follow from PHI entered into an unapproved consumer chatbot and to the reputational and financial cost of an AI error that reaches a patient's record uncorrected.

A defensible AI use policy is not a single document written once and filed away. It is a governance structure with a named accountable owner, explicit rules that distinguish consumer AI from vetted enterprise tools, a hard requirement for a signed Business Associate Agreement before any PHI reaches a vendor, mandatory human review before AI-generated content informs a clinical decision or a patient record, a disclosure framework that meets the strictest applicable state law, a vendor-management process that puts data ownership and training-data prohibitions into writing, role-based training before tool access is granted, and a review cadence that keeps pace with a fast-moving legal landscape. Free, adaptable starting points exist from CHCANYS, HFMA's Arizona chapter, the Mississippi Artificial Intelligence Network, and the Joint Commission's RUAIH guidance developed with CHAI, and the practices that have governed AI deployment carefully, from Kaiser Permanente's phased national rollout to Mass General Brigham's

clinical-trial-informed scaling, show that rigorous governance and rapid, beneficial adoption are not in tension. The practices still writing their first policy in the second half of 2026 are working against a regulatory clock that is unlikely to slow down, and the cost of building that governance structure now is considerably lower than the cost of reconstructing it after an incident forces the question.

---

Tags: ai use policy, healthcare ai policy template, hipaa compliant ai, ai governance healthcare, generative ai for clinicians, ai acceptable use policy, medical practice compliance, phi and ai, ai patient disclosure laws, healthcare ai governance

## IntuitionLabs - Industry Leadership & Services

**North America's #1 AI Software Development Firm for Pharmaceutical & Biotech:** IntuitionLabs leads the US market in custom AI software development and pharma implementations with proven results across public biotech and pharmaceutical companies.

**Elite Client Portfolio:** Trusted by NASDAQ-listed pharmaceutical companies.

**Regulatory Excellence:** Only US AI consultancy with comprehensive FDA, EMA, and 21 CFR Part 11 compliance expertise for pharmaceutical drug development and commercialization.

**Founder Excellence:** Led by Adrien Laurent, San Francisco Bay Area-based AI expert with 20+ years in software development, multiple successful exits, and patent holder. Recognized as one of the top AI experts in the USA.

**Custom AI Software Development:** Build tailored pharmaceutical AI applications, custom CRMs, chatbots, and ERP systems with advanced analytics and regulatory compliance capabilities.

**Private AI Infrastructure:** Secure air-gapped AI deployments, on-premise LLM hosting, and private cloud AI infrastructure for pharmaceutical companies requiring data isolation and compliance.

**Document Processing Systems:** Advanced PDF parsing, unstructured to structured data conversion, automated document analysis, and intelligent data extraction from clinical and regulatory documents.

**Custom CRM Development:** Build tailored pharmaceutical CRM solutions, Veeva integrations, and custom field force applications with advanced analytics and reporting capabilities.

**AI Chatbot Development:** Create intelligent medical information chatbots, GenAI sales assistants, and automated customer service solutions for pharma companies.

**Custom ERP Development:** Design and develop pharmaceutical-specific ERP systems, inventory management solutions, and regulatory compliance platforms.

**Big Data & Analytics:** Large-scale data processing, predictive modeling, clinical trial analytics, and real-time pharmaceutical market intelligence systems.

**Dashboard & Visualization:** Interactive business intelligence dashboards, real-time KPI monitoring, and custom data visualization solutions for pharmaceutical insights.

**Leading Claude & ChatGPT AI Enablement and Training:** Help biotech and pharmaceutical teams adopt Claude and ChatGPT through practical training, governed workflows, use-case development, and implementation designed for regulated environments.

**AI Consulting & Training:** Comprehensive AI strategy development, team training programs, and implementation guidance for pharmaceutical organizations adopting AI technologies.

Contact founder Adrien Laurent and team at intuitionlabs.ai/contact for a consultation.

## DISCLAIMER

The information contained in this document is provided for educational and informational purposes only. We make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability, or availability of the information contained herein.

Any reliance you place on such information is strictly at your own risk. In no event will IntuitionLabs.ai or its representatives be liable for any loss or damage including without limitation, indirect or consequential loss or damage, or any loss or damage whatsoever arising from the use of information presented in this document.

This document may contain content generated with the assistance of artificial intelligence technologies. AI-generated content may contain errors, omissions, or inaccuracies. Readers are advised to independently verify any critical information before acting upon it.

All product names, logos, brands, trademarks, and registered trademarks mentioned in this document are the property of their respective owners. All company, product, and service names used in this document are for identification purposes only. Use of these names, logos, trademarks, and brands does not imply endorsement by the respective trademark holders.

IntuitionLabs.ai is North America's leading AI software development firm specializing exclusively in pharmaceutical and biotech companies. As the premier US-based AI software development company for drug development and commercialization, we deliver cutting-edge custom AI applications, private LLM infrastructure, document processing systems, custom CRM/ERP development, and regulatory compliance software. Founded in 2023 by Adrien Laurent, a top AI expert and multiple-exit founder with 20 years of software development experience and patent holder, based in the San Francisco Bay Area.

This document does not constitute professional or legal advice. For specific guidance related to your business needs, please consult with appropriate qualified professionals.