OMH-HealthEdge Holdings, Inc.[1] *dba* Omega Healthcare Management Services® Global Integrated Artificial Intelligence ("AI") Policy

Doc ID: POL-GIAI
Version: 2.0
Effective: 01/28/2026

[1] This document applies to OMH-HealthEdge Holdings, Inc. dba Omega Healthcare Management Services® and its controlled subsidiaries and affiliates.

Contents

1. Purpose

Omega Healthcare is committed to using artificial intelligence ("AI") responsibly, legally, and in accordance with its organizational values.[2] This policy establishes standards for both the development of AI systems and the use of AI tools with the key considerations of confidentiality, fairness, transparency, accountability, and compliance with applicable laws and regulations.

2. Scope

This policy applies to:

- The development and deployment of AI systems within and by Omega Healthcare.
- The use of AI tools (whether enterprise-licensed or public) by Omega Healthcare personnel.
- All Omega Healthcare employees, contractors, subcontractors, vendors, and third-party partners involved in AI activity.

3. Definitions

For purposes of this policy:

- **AI Activity**: Any development, deployment, or use of AI systems or tools in Omega Healthcare's operations.
- **AI Governance Committee**: The cross-functional group designated by Omega Healthcare to oversee AI activity, including policy enforcement, platform approvals, risk reviews, and incident response. Membership includes representatives from Legal, Compliance, Technology, and other functions as designated by senior leadership.
- **AI Platform**: Any software, system, or service that provides access to AI functionality. For business use, only Omega Healthcare-approved, enterprise-licensed AI platforms (e.g., Microsoft Copilot) or Omega Healthcare's internal AI environments may be used ("Omega AI Platform(s)"). **Public or unlicensed AI tools are prohibited unless expressly authorized by the AI Governance Committee.**
- **AI System**: A machine-based system that, for explicit or implicit objectives, infers, predicts, recommends, or generates outputs (such as content, decisions, or forecasts) that can influence physical or virtual environments. *Examples: a model that predicts claims denials, a chatbot trained on Omega Healthcare policies, a risk-scoring algorithm*.
- **AI**: Systems that perform tasks normally requiring human cognition, such as learning, reasoning, or decision-making.
- **Confidential Information:** Any Omega Healthcare proprietary business information or

[2] For purposes of this Policy, "Omega Healthcare" refers to OMH-HealthEdge Holdings, Inc. dba Omega Healthcare Management Services® and its subsidiaries.

client data, including Protected Health Information ("PHI") and Personally Identifiable Information ("PII"). This includes technical and non-technical information related to Omega Healthcare's operations, products, services, research, development, financials, procurement, customers, pricing sales, marketing, and any information received from third parties that Omega Healthcare is obligated to treat as confidential.

- **Covered Individuals**: All Omega Healthcare employees, contractors, subcontractors, vendors, and third-party partners who develop, deploy, or use AI systems or tools in connection with Omega Healthcare's business.

- **Developers**: Omega Healthcare employees and contractors whose role includes designing, training, testing, or deploying AI systems.

- **Generative AI (GenAI)**: AI tools that produce new content, such as text, images, or code.

4. Principles

The following principles guide all AI activity by Covered Individuals, with additional obligations for Developers established in Section 5.

4.1 Confidentiality

All Confidential Information, including but not limited to PHI and PII, may only be used within Omega Healthcare's approved internal systems or enterprise-licensed AI Platforms that are designated as compliant with applicable security, privacy, and regulatory requirements. Any exception requires approval by the AI Governance Committee in consultation with Legal and Compliance. Covered Individuals must not place Confidential Information, including PHI or PII, into public or unlicensed AI Platforms. As set forth in Section 7, the restrictions of this section are in addition to, and not replacing, all applicable Omega Healthcare and client policies, and applicable law, regarding Confidential Information, PHI, and PII.

4.2 Client Data Use and Approval Requirements

All AI use involving client data, including any information classified as Confidential Information (including but not limited to PHI and PII), must strictly adhere to the permissions, data-handling, security, and privacy requirements defined in each client's contract with Omega Healthcare.

Non-PII corporate data may be accessed, processed, or analyzed by Omega Healthcare so long as the platform has been expressly approved by the AI Governance Committee and Legal for the relevant use case; the purpose of use is limited to fulfilling the contracted service or a documented business need; and the use complies with all applicable privacy laws (e.g., HIPAA, GDPR) and Omega's information-security standards. Any proposed AI use of client data outside the agreed scope or within new functionality (such as model training, retraining, or cross-client analytics) requires case-by-case approval from the AI Governance Committee in consultation with Legal and Compliance.

4.3 Approved Platforms Only

Covered Individuals may only use AI Platforms that have been reviewed and approved by Omega

Healthcare. Enterprise AI tools may only be used through Omega Healthcare -issued accounts, not personal accounts.

All AI use must occur within enterprise-licensed and managed IT environments (e.g., Omega-issued devices, secure networks, or VPNs) that have been approved by Omega Healthcare for compliance with security, privacy, and contractual requirements. Use of Confidential Information is permitted only within those enterprise-licensed Omega AI Platforms specifically approved for that data classification under Section 4.1.

Permitted non-confidential uses include non-confidential tasks such as drafting, summarizing, and brainstorming, provided that the material does not contain Confidential Information and that all AI-generated outputs are subject to human review before use.

In addition to assisted use, Omega Healthcare may automate certain repetitive or rules-based tasks through AI-enabled systems where controls, audit trails, and human override mechanisms are in place. Such automation must still comply with oversight, risk-assessment, and accountability requirements established under this Policy.

4.3.1 Sales Proposals and Account Plans and AI Use

Sales proposals and account plans routinely contain Confidential Information (including corporate data). All AI Activity involving such information must comply with applicable contractual data-handling, privacy, and security requirements and may occur only within Omega's enterprise-licensed, AIGC-approved AI Platforms.

AI may be used to assist with sales proposals and account-plan drafting only when:

- the platform is expressly approved by the AI Governance Committee and Legal for the relevant use case
- use is limited to the contracted service or a documented business need, and
- all applicable privacy laws and Omega information security standards are met.

Any proposed AI use outside the agreed scope or introducing new functionality (e.g., model training/retraining or cross-client analytics) requires case-by-case approval by the AIGC in consultation with Legal and Compliance.

Permitted Uses (approved platforms only)

- Structure or outline creation (e.g., suggesting a table of contents for a payer-segment account plan).
- Style or tone edits on sanitized text (all client names, identifiers, or specifics removed).
- Drafting of generic talk tracks or value propositions that do not include client identifiers or proprietary data.

Prohibited Uses (without prior written approval)

- Entering client names, unique identifiers, financials, PHI / PII, or proprietary strategies into any unapproved or public AI tool.
- Using client data for model training, retraining, or cross-client analytics without documented authorization and AI Governance Committee approval.
- Using any vendor AI tool that does not meet Omega's contractual data-use and security requirements.

Required Workflow

- **Check the Tool** – Confirm the AI Platform appears on Omega's approved list of AI tools maintained by the AI Governance Committee. If not, stop and route the request through the Committee's intake process for review.
- **Sanitize** – Remove client identifiers and other sensitive information before using the tool; replace with generic placeholders (e.g., "[Payer]," "[2026 forecast]").
- **Human Review** – Treat all AI-generated output as a draft. Validate facts, remove assumptions, and re-insert client-specific information offline (do not re-upload client data).

Prompt Examples

- Good Prompt (allowed): "Create a concise outline for a payer-segment account plan. Include: Overview, Client Profile, Stakeholder Map, Strategy & Opportunities, Action Plan & Timeline, KPIs & Risk. Keep it generic for later customization."
- Bad Prompt (disallowed): "Draft a plan for [ClientName] (Medicare Advantage) including their claims error rate, premium targets, and named executives."

4.4 Human Oversight

AI is intended to support, not replace, human judgment. All AI-generated outputs, including text, data, recommendations, or other results, must be reviewed, fact-checked, and validated by a responsible human before its use in decision-making or client-facing materials. AI-generated outputs used in client-facing materials must also comply with Omega Healthcare's legal and brand review procedures. The level of review must be proportionate to the audience and potential impact, with more rigorous verification required for external or client-facing use.

4.5 Transparency

Transparency requires open communication about the role of AI. When an AI Platform or AI System materially assists in creating or shaping content, Covered Individuals should disclose this in client-facing, regulatory, or external communications. Internally, transparency supports trust and accountability in AI use.

4.6 Accountability

Each Covered Individual is responsible for the accuracy, legality, and appropriateness of any AI-generated output they use. Final accountability always rests with the human user, consistent with Omega Healthcare's standards of professional and legal responsibility.

4.7 No Misuse

Intentional misuse of AI Platforms or AI Systems is strictly prohibited. Misuse includes, but is not limited to, fraud, harassment, discrimination, spreading misinformation, malicious activity, or attempts to bypass security controls. All AI Activity must also be consistent with Omega Healthcare's existing policies on confidentiality, security, intellectual property, anti-discrimination, and professional conduct. Violations may result in disciplinary action up to and including termination.

5. Development and Deployment

This section applies only to Developers and establishes additional requirements for the development and deployment of AI Systems that build on the general principles in Section 4.

5.1 Governance Alignment

Developers must follow the directives of the AI Governance Committee and document compliance with Omega Healthcare's AI Policy in all development activities.

5.2 Risk and Bias Assessment

Before deployment and periodically thereafter, Developers must perform risk assessments[3] and evaluations for potential bias in all AI Systems. Assessments must address data quality, model fairness, potential harms, and privacy impacts. Particular attention must be paid to potential biases in healthcare data. Assessments must also consider specific AI risk scenarios, including risks of data leakage, copyright violations in generative outputs, and other harms identified by the Committee. Developers must follow the principle of data minimization, collecting and using only the minimum necessary data for training and deploying AI systems. Where required, a privacy impact assessment must be conducted to document compliance with Omega Healthcare's privacy obligations. Procedures and templates approved by the AI Governance Committee must be used to complete and document these assessments.

5.3 Bias Treatment

Where unwanted bias is identified, Developers must apply treatment methods in accordance with procedures approved by the AI Governance Committee. Bias mitigation techniques may include pre- and post-processing methods, prompt design, and dataset diversity strategies, as set out in procedures approved by the Committee. Documentation must demonstrate that mitigation steps were effective and did not undermine the reliability, accuracy, or intended function of the AI System.

[3] *See* Omega Healthcare AI Risk & Bias Assessment Template.

5.4 Lifecycle Documentation

Developers must maintain records throughout the lifecycle of each AI System. Documentation must explain how the AI System produces outputs, how those outputs should be interpreted, and the limitations of the System. Developers must also record design decisions, data sources, and points where human oversight is required. Developers must also define mechanisms for human intervention in case of errors, biases, or unexpected outcomes. All documentation must be created and retained in accordance with procedures established by the AI Governance Committee.

5.5 Vendor and Third-Party AI

AI Systems or components provided by vendors must meet Omega Healthcare's governance standards. Vendors must complete risk assessments and evaluations for potential bias and provide documentation as required by Omega Healthcare's vendor management procedures and Supplier Code of Conduct. All vendors providing AI-related products or services are subject to the Supplier Code of Conduct, which establishes requirements for AI governance, data privacy, and security. The Committee will oversee vendor risk assessments and may require regular audits to confirm compliance with these standards.

Customer data may be used only for the purpose for which it was provided, unless otherwise authorized in a written agreement in compliance with applicable law and Omega Healthcare's privacy obligations. Where authorized, customer data may be used to train or retrain AI Systems, provided that appropriate notice, risk assessments, and privacy safeguards are in place. Customer data must never be used in any open source or unlicensed AI Platforms.

The AI Governance Committee may review vendor submissions for compliance.

5.6 Cooperation with Investigations

Developers must cooperate fully with any internal or external investigations related to the design, deployment, or operation of AI Systems. This includes providing documentation, responding to inquiries, and supporting the Committee in addressing suspected violations, incidents, or regulatory reviews. Developers must also notify and coordinate with Omega Healthcare's Legal and Compliance teams when responding to external inquiries.

5.7 Security Evaluation

Developers must confirm that AI Systems are tested for security and reliability before release. Evaluations must identify known limitations, potential failure modes, and vulnerabilities. The AI Governance Committee may require specialized testing methods as appropriate.

6. Education and Awareness

This section applies to all Covered Individuals and establishes training and awareness requirements for the responsible use of AI, with additional requirements for Developers.

6.1 Training Requirement

Covered Individuals must complete training on Omega Healthcare's AI Policy and the responsible use of AI Platforms before being granted access to enterprise-licensed AI Platforms or AI

development environments. Completion of required training is a condition of access.

6.2 Ongoing Awareness

Covered Individuals must participate in refresher training as determined by the AI Governance Committee to reflect changes in laws, regulations, approved AI Platforms, or Omega Healthcare's internal procedures. Developers, as well as managers and senior leaders who oversee the use of AI in their areas of responsibility, must also maintain awareness of AI security risks, relevant threats, and mitigation responsibilities as part of Omega Healthcare's ongoing compliance training.

6.3 Developer Education

Developers must also complete specialized training on AI System lifecycle management, risk assessment, and bias treatment in accordance with procedures established by the AI Governance Committee. Developers are also required to maintain awareness of evolving standards and practices for the responsible and secure design, testing, and deployment of AI Systems.

6.4 AI Literacy and Stakeholder Education

With guidance and direction from the AI Governance Committee, Omega Healthcare will provide regular training programs to improve AI literacy and promote ethical AI practices for all Covered Individuals. Omega Healthcare may also provide educational resources to clients and partners to increase awareness of AI in healthcare services.

7. Compliance and Governance

This section establishes Omega Healthcare's compliance obligations and governance structure for AI activity.

7.1 Regulatory Alignment

Omega Healthcare will comply with all applicable laws and regulations governing the use of AI, including healthcare, privacy, civil rights, and consumer protection requirements. Examples may include, as applicable, HIPAA, HITECH, GDPR, and state AI laws. All Omega Healthcare policies, including those on confidentiality, intellectual property, anti-discrimination, and professional conduct, also apply to AI Activity. Omega Healthcare applies infrastructure security, access controls, and environment segregation to AI development and deployment in accordance with industry standards.

7.2 Monitoring and Auditing

AI Platforms and AI Systems may be subject to monitoring and audit to verify compliance with this policy, applicable procedures, and regulatory requirements. Audits and assessments will include reviews of AI System performance, fairness, data privacy, security, and compliance with Omega Healthcare's ethical standards. Enterprise AI usage will be logged and monitored in accordance with Omega Healthcare's information security policies. Logs and audit records must be maintained in accordance with procedures approved by the Committee. Monitoring will also account for sudden or gradual changes in AI System behavior (data drift), potential anomalies affecting security or reliability, and error-handling mechanisms to support timely human intervention.

7.3 Governance Oversight

The AI Governance Committee is responsible for overseeing this policy, reviewing compliance findings, and coordinating incident responses for AI-related issues. Its responsibilities are summarized below, but are set forth in and subject to AI Governance Committee Charter:

- Maintaining a responsibility matrix to provide clear lines of accountability throughout the AI lifecycle.
- Overseeing AI initiatives and managing third-party vendor compliance (including the Supplier Code of Conduct and vendor risk assessments).
- Coordinating with Omega Healthcare's information security and incident response teams to verify AI-related incidents are addressed
- Maintaining a risk registry for enterprise AI tools
- Recommending updates to procedures or training based on audit results, risk assessments, or changes in law.

8. Reporting and Enforcement

This section establishes reporting channels, protections, and enforcement measures for AI-related concerns.

8.1 Reporting

Covered Individuals shall promptly report any suspected misuse of AI Platforms or AI Systems through Omega Healthcare's Ethics Hotline, designated Compliance contacts, or other channels provided in Omega Healthcare's Code of Conduct. Reports may be made confidentially and will be investigated promptly, thoroughly, and as confidentially as possible, under the same standards and protections set out in the Code of Conduct and compliance procedures. Anonymous reporting is also available through Omega Healthcare's designated whistleblower platform. Covered Individuals shall cooperate fully with investigations into suspected violations or incidents involving AI use.

8.2 Non-Retaliation

Omega Healthcare prohibits retaliation against any Covered Individual who makes a good faith report of AI misuse or other compliance concerns, in accordance with Omega Healthcare's non-retaliation policy.

8.3 Enforcement

Violations of this policy may result in disciplinary action up to and including termination of employment or contract. Contractors, subcontractors, vendors, and partners may also be subject to contract termination or other remedies under applicable agreements.

8.4 Monitoring of AI Use

Omega Healthcare reserves the right to review communications, prompts, attachments, and files transmitted through AI Platforms or AI Systems for purposes of investigating suspected violations or incidents, consistent with Omega Healthcare's existing monitoring and investigation policies. Covered Individuals should not expect personal privacy when using Omega Healthcare -issued accounts or systems to access AI Platforms.

9. Review and Revision

This Policy will be reviewed periodically to confirm it remains aligned with legal requirements, industry standards, and Omega Healthcare's evolving needs. Reviews will be initiated by the AI Governance Committee in coordination with other relevant leadership, and proposed updates will be submitted for approval through Omega Healthcare's policy governance process.

10. Implementation and Acknowledgement

All Covered Individuals are required to read, understand, and comply with this Policy. Use of AI Platforms or participation in AI development at Omega Healthcare constitutes acknowledgment of this requirement. Failure to comply may result in disciplinary action, up to and including termination of employment or contract. Committee-approved procedures, checklists, and forms are maintained separately from this Policy by the AI Governance Committee.

11. References and Governing Standards

This Policy is informed by the following laws, regulations, and standards, among others:

Healthcare and Privacy Regulations

- Health Insurance Portability and Accountability Act ("HIPAA"), including the Privacy, Security, and Breach Notification Rules.
- Health Information Technology for Economic and Clinical Health Act ("HITECH").
- General Data Protection Regulation ("GDPR"), particularly Articles 5 and 25 (data minimization and Privacy by Design).
- Emerging state and national laws regulating artificial intelligence and data privacy.

Information Security Standards

- ISO/IEC 27001 – Information Security Management Systems.
- ISO/IEC 27701 – Privacy Information Management (if relevant to your environment).

Artificial Intelligence Standards

- ISO/IEC 42001:2023 – AI Management Systems.
- ISO/IEC 23894:2023 – AI Risk Management.
- ISO/IEC TR 24027:2021 – Bias in AI systems and decision making.
- ISO/IEC TS 12791:2024 – Bias treatment methods for classification and regression.
- ISO/IEC TR 24028:2020 – Trustworthiness of AI.
- ISO/IEC 5338:2023 – Guidance on AI system lifecycle processes.
- ISO/IEC TR 24368:2023 – Ethical and societal concerns related to AI.
- ISO/IEC 38507:2022 – Governance implications of AI for organizations.