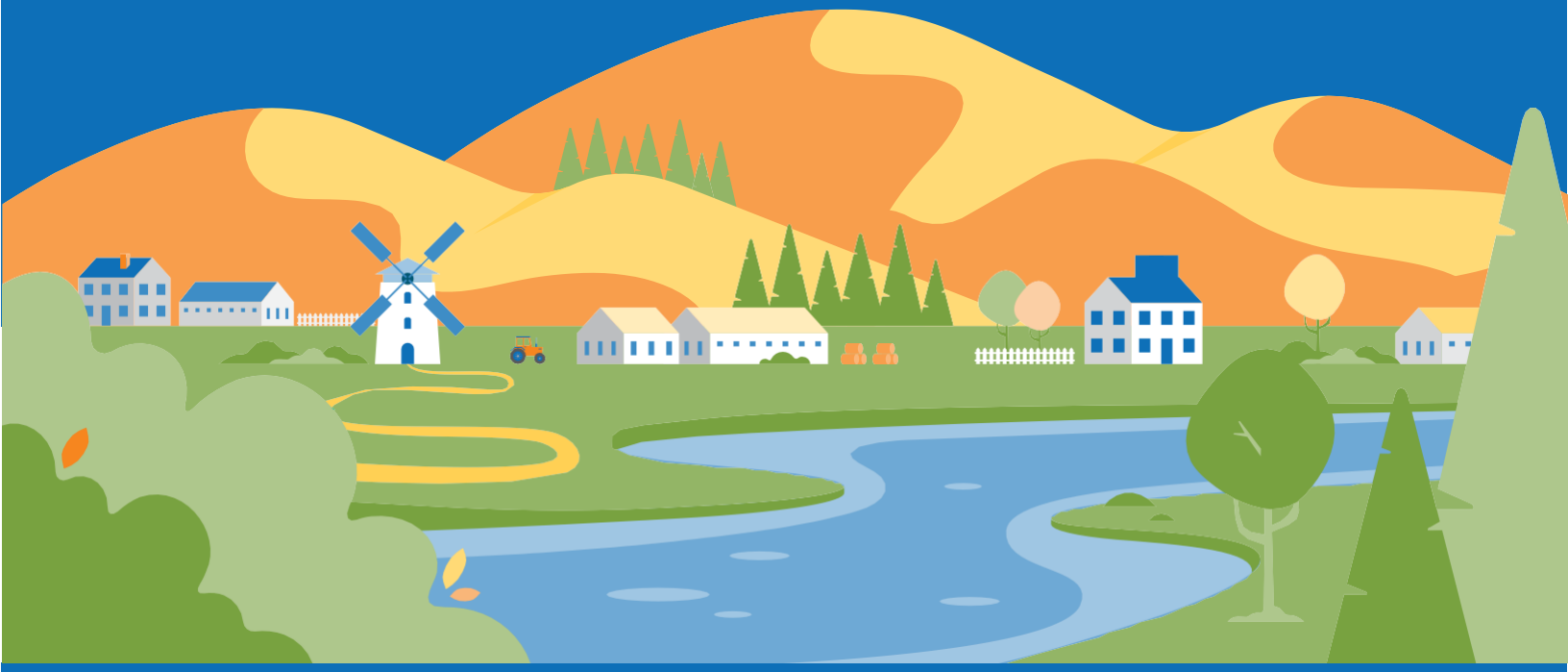
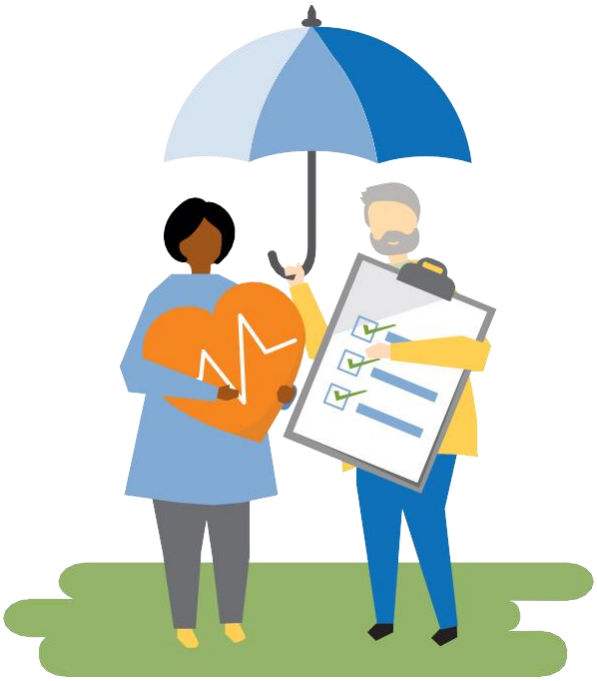
Health Care Artificial Intelligence Governance Guide



CALIFORNIA TELEHEALTH RESOURCE CENTER

Part of OCHIN

2025



The California Telehealth Resource Center (CTRC) and all resources and activities produced or supported by the CTRC are made possible by grant number U1UTH42520-01-01 from the Office for the Advancement of Telehealth, Health Resources and Services Administration, DHHS, and the California State Office of Rural Health (CalSORH). This information or content and conclusions are those of the CTRC and should not be construed as the official position or policy of, nor should any endorsements be inferred by HRSA, HHS, the U.S. Government, CalSORH or the State of California.

CTRC does not provide legal advice. CTRC has no relevant financial interest, arrangement, or affiliation with any organizations related to commercial products or services mentioned in this toolkit. It is for informational purposes only.

GOVERNANCE FOR AI APPLICATIONS

Strong AI governance policies enable health care providers to use AI in an ethical, responsible, and secure manner, leveraging the benefits while minimizing risks.

Policy Framework

Objective: Establish clear guidelines and principles for the use of AI in healthcare to ensure safety, effectiveness, and ethical standards are met.

- **AI Ethics Policy**: Outline principles related to transparency, fairness, accountability, and patient consent, including information how AI is being used, what data is being collected, and how decisions will be made.
- **Data Privacy and Security Policy:** Define standards for data protection, including access controls, encryption, and patient privacy.
- **AI Usage Policy**: Specify permissible uses of AI, the level of autonomy, and who is authorized to utilize it for things like diagnostic support, project planning, task management, drafting communications, predictive analytics, and administrative automation as well as uses of generative AI. Provide specific guidance on the use of generative AI in patient-facing communications.
- **Risk Management Policy**: Establish procedures for identifying, assessing, and mitigating risks associated with AI applications, including any copyrighted material, hallucinations, or algorithmic bias.

Procedures

Objective: Develop standard operating procedures (SOPs) to ensure consistent and safe deployment and management of AI systems.

AI System Deployment Procedure:

- Evaluation: Assess the AI tool for clinical effectiveness, reliability, adverse bias, and alignment with organizational goals.

- Implementation: Detailed steps for integrating AI systems into existing workflows.
- Training: Ensure all relevant personnel are adequately trained in using the AI tool

Data Management Procedure:

- Data Collection: Guidelines for collecting high-quality, relevant data while ensuring patient privacy.
- Data Processing: Steps for preprocessing data to be used by AI systems, including cleaning and normalization.
- Data Storage: Secure storage solutions to protect sensitive health information.

Monitoring and Evaluation Procedure:

- Performance Monitoring: Regular monitoring of AI system performance, including accuracy, efficiency, and user satisfaction.
- Issue Reporting: Mechanisms for reporting and addressing any issues or malfunctions.
- Continuous Improvement: Procedures for incorporating feedback and making iterative improvements to AI systems.

Personnel

Objective: Train and assign clear roles and responsibilities to ensure proper governance and management of AI systems.

Training:

- Initial Foundational Training: General education on AI basics needed along with specialized training based on function and responsibilities for all staff.
- Ongoing Upskilling: As AI evolves and more tools become available, staff and leadership will need specialized upskilling based on function and role to understand both benefits and risks of AI systems.

Organizational Leadership

- Ultimately responsible for the safe, ethical, and effective use of AI within the organization.
- Operational duties are delegated to functional roles (e.g. AI System Administrator, AI Ethics Officer, and Clinical AI Champions).
- When these functional roles flag an issue with an AI system, leadership is responsible for coordinating incident response, initiating remediation, engaging with legal entities, and ensuring transparent communication with patients and staff.
- A member of leadership should chair the AI Governance Committee.

AI Governance Committee:

- Composition: Build a cross-functional team, including representatives from clinical staff, IT, legal, and administrative departments, chaired by organizational leadership.
- Responsibilities: Review and approve vendors, oversee the implementation of AI policies, review AI system performance, and make decisions as well as recommendations to leadership on AI usage.

AI Ethics Officer

- Role: Ensure that AI applications comply with ethical standards and patient consent requirements.
- Duties: Conduct regular ethical reviews and address any ethical concerns related to AI usage.

AI System Administrator:

- Role: Manage the technical aspects of AI systems.
- Duties: Oversee system integration and implementation, perform routine maintenance, and ensure data integrity.
- Data Processing (where applicable): Steps for preprocessing data to be used by AI systems, including cleaning and normalization.

Clinical AI Champions:

- Role: Act as liaison between clinical staff and the AI governance committee.
- Duties: Provide feedback on AI tool performance, assist in training, and promote best practices and ensure clear accountability and reporting.

Testing

Objective: Regularly test and verify that AI systems comply with established policies and procedures.

Initial Validation:

- Clinical Validation: Test AI systems for clinical accuracy and relevance before deployment. Include real-world testing environments and simulations.
- Technical Validation: Ensure the AI system is technically sound and integrates well with existing IT infrastructure.

Ongoing Compliance Testing:

- Routine Audits: Conduct periodic audits to check for compliance with AI usage policies, data privacy, and security standards.
- Performance Reviews: Regularly review AI system performance against predefined metrics (e.g., accuracy, reliability, user satisfaction, mitigating adverse bias).
- Security Testing: Perform vulnerability assessments and penetration testing to identify and address security gaps

Incident Response:

- Incident Management Procedure: Establish clear steps for responding to AI system failures or breaches.
- Root Cause Analysis: Investigate incidents to determine the root cause and implement corrective actions.
- Reporting and Documentation: Maintain detailed records of incidents, responses, and outcomes for accountability and learning.

Regulatory Compliance

See Appendix B for more information on these laws.

Objective: Ensure AI systems meet all relevant regulatory requirements, including but not limited to:

- The Health Information Portability and Accountability Act (HIPAA)
- The U.S. Department of Health & Human Services (HHS) Office of Civil Right's Non-Discrimination prohibition, and other local health data regulations
- The Food and Drug Administration requirements for medical devices
- The HHS Office of the National Coordinator for Health Information Technology requirements for certified health IT
- California Privacy laws and AI laws

Conclusion

Implementing robust governance for AI applications in a community clinic or critical access hospital requires a comprehensive approach that includes clear policies, detailed procedures, well-defined personnel roles, and rigorous compliance testing. By adhering to these components, healthcare providers can ensure that AI tools are used safely, effectively, and ethically, even with limited resources.

Appendix A: Sample Policy

Below is a sample policy that should be used as a starting point to build out your organization's AI governance policy. This sample governance policy is intended as a foundational template to support healthcare organizations in developing their own AI governance framework. However, it should not be adopted as-is. Each organization should conduct an internal stakeholder review process—including input from clinical, IT, legal, compliance, administrative, and patient-facing staff—to ensure the policy reflects the organization's specific mission, values, culture, and operational realities. Final policies should be vetted through appropriate internal governance channels (e.g., compliance, risk management, executive leadership) and tailored to comply with applicable laws, accreditation standards, and local community needs.

Organizational Policy on the Ethical and Responsible Use of Artificial Intelligence (AI) in Clinical and Operational Settings

I. Purpose

This policy establishes the principles, procedures, and responsibilities for the use of artificial intelligence (AI) technologies across clinical and administrative functions within [Provider Name]. The goal is to ensure AI is used safely, ethically, and in full compliance with applicable laws and organizational standards, particularly in high-risk scenarios involving sensitive patient data and healthcare outcomes.

II. Scope

This policy applies to all staff members, contractors, vendors, and partners who interact with or rely on AI-powered tools in their roles, including but not limited to clinical decision support, diagnostics, patient communications, documentation, communication drafting, operational automation, and predictive analytics.

III. Governance Structure

To manage AI responsibly, our organization has created a structured oversight framework:

A. AI Governance Committee

- A cross-functional leadership group that:

- Reviews and approves all AI tools before deployment.
- Conducts risk assessments and performance audits.
- Updates this policy as needed and leads incident investigations.
- Approves vendor updates and monitors model drift.

If you are implementing or using a new AI tool, the Governance Committee must approve it first. If you observe an issue with an AI tool, report it to this committee through your department lead or Clinical AI Champion.

B. AI System Administrator:

A technical expert who:

- Installs, configures, and maintains AI tools.
- Ensures system reliability, data security, and log auditing.
- Works with vendors and IT staff to fix issues.

If your AI tool isn't working correctly, or if you encounter access or system issues, notify your Clinical AI Champion, who will escalate to the System Administrator.

C. AI Ethics Officer

A compliance and ethics lead who:

- Evaluates tools for fairness, bias, and patient consent.
- Monitors legal and ethical compliance with AI regulations.
- Leads investigations if ethical or discriminatory concerns arise.

If you have concerns about an AI tool giving biased results or causing patient confusion, you can report them confidentially through the Ethics Officer.

D. Clinical AI Champions

Designated frontline staff (e.g., a nurse, physician, MA, or telehealth coordinator) who:

- Help train staff on AI tools and serve as your first point of contact.
- Gather feedback and report usability issues.
- Represent clinical voices in governance decisions.

If you're unsure how to use an AI tool, need help interpreting its results, or have concerns, your Clinical AI Champion is your go-to resource.

IV. Policy Statements

A. AI Ethics and Transparency

- AI systems must uphold transparency, explainability, and fairness.
- Patients must be informed when AI is part of their care or diagnosis, including a plain-language explanation of the tool's purpose.

- No AI system may replace human clinical judgment in high-risk scenarios without FDA authorization/clearance.
- Any written or verbal communications to patients pertaining to patient clinical information that uses generative artificial intelligence must include a disclaimer that indicates to the patient that the communication was generated by artificial intelligence along with clear instructions describing how the patient may contact a human health care provider (per AB 3030 of 2024).

B. Data Privacy and Security

- All AI systems must meet all relevant federal and state security standards, including end-to-end encryption, audit trails, and role-based access.
- Only de-identified or consented data may be used for training, testing, or external benchmarking.
- No personally identifiable information or patient health information (PHI) may be used for generative AI model fine-tuning or external analytics.

C. Authorized Uses and Prohibited Uses

- Permissible: Diagnostic decision support (if FDA-cleared or authorized), risk scoring, care coordination alerts, summarization of documentation, predictive analytics, administrative efficiency (e.g., billing).
- Prohibited: Using generative AI to synthesize clinical advice, using non-vetted consumer-grade tools for patient data processing.
- Employees may submit requests regarding additional permissible uses of AI to the AI Governance Committee.

V. AI Use Policy for All Staff

A. Permissible Uses

The following uses have been approved by the AI Governance Committee:

- Clinical decision support (e.g., triage, diagnosis, alerts) if FDA-cleared or authorized.
- Drafting clinical documentation (with human review).
- Administrative support (e.g., billing, scheduling, referrals).
- Generating communications (with AI disclaimers, where required).

AI may not be used as the sole basis for medical decisions unless specifically authorized. Always double-check AI-generated output.

B. Prohibited Uses

- Using non-approved or consumer-grade AI tools with patient data.
- Making diagnoses or treatment plans based solely on AI suggestions.
- Using generative AI tools to simulate conversations or write clinical messages without final human review or proper disclosures.

VI. Staff Responsibilities

A. General Staff

- Complete required AI training before using AI tools.
- Always verify AI output before sharing with patients or adding to records.
- Report any system malfunctions or unexpected AI behavior.
- Notify a designated AI position (your Clinical AI Champion, AI System Administrator, or AI Ethics Officer) if you have concerns about safety, accuracy, or bias.

B. Managers & Team Leads

- Ensure staff are trained before granting access to clinical AI tools.
- Support the collection of feedback and issue reporting.
- Serve as communication bridges between staff and governance roles.

VII. Training & Support

Purpose

To ensure that all staff—clinical, administrative, and technical—have the knowledge, skills, and confidence to safely and appropriately use AI tools in their work. Training helps reduce errors, supports patient safety, and ensures that AI is used as a tool to assist, not replace, human judgment.

All staff using AI tools must complete a structured training program tailored to their role.

Foundational Training for All Staff:

- Basics of how AI works
- Benefits and risks of using AI in healthcare
- The organization's policy on AI use and data protection
- How to recognize bias or errors in AI-generated content

Role-Based Training:

- Clinical staff: How to interpret AI outputs, when to override suggestions, and how to document decisions.
- Administrative staff: How to use AI to improve workflows (e.g., summarizing patient

messages or generating forms), and limits of AI output.
- IT staff: How to maintain AI systems and manage data inputs and outputs securely.

Annual Refresher:

- All users must complete a yearly update, including changes in regulations, tools, and internal policy.

VIII. Risk Management & Incident Reporting

AI tools are powerful but can introduce serious risks—such as incorrect recommendations, biased outputs, or security breaches. Promptly identifying and addressing these risks helps protect patients, staff, and the organization from harm or liability.

If an AI tool:

- Provides incorrect or biased recommendations,
- Fails to operate as intended,
- Results in a near-miss or actual patient safety event,

You must report this immediately through the incident reporting system or directly to your Clinical AI Champion or supervisor. These incidents will be reviewed by the AI Governance Committee and, if necessary, the Ethics Officer and Risk Manager.

Examples of Reportable Incidents:

- AI system gives a clearly incorrect clinical suggestion
- Patient information is accidentally exposed via an AI tool
- A staff member relies on an AI recommendation in an unapproved manner
- The system is behaving inconsistently (e.g., giving different outputs for similar cases)
- AI-generated documents are sent to the wrong patient or provider

IX. Regulatory Compliance

Because AI is used in healthcare decision-making and handles sensitive patient data, there are many legal rules and regulatory standards that must be followed. This ensures patient safety, avoids legal penalties, and protects the organization's reputation. All AI tools used by this organization must comply with all relevant state and federal requirements. The Compliance Officer will ensure that tools meet these requirements. This includes, but is not limited to:

- HIPAA/HITECH
- FDA regulations
- OCR nondiscrimination laws
- ONC certification standards (for EHR-integrated AI tools)
- California privacy laws, including CCPA, CPRA, and AI-specific laws (AB 3030, etc.)

Appendix B: Laws & Regulations

Health care providers must ensure that any use of AI is compliant with relevant federal and state laws. This is provided for educational purposes and does not constitute legal advice. Please review all of these materials with your legal counsel.

Below is a non-exhaustive list that providers should observe.

California State Laws & Regulations

For more information about laws that may impact the use of AI in California, see Attorney General Bonta's January 2025 guidance:

- California Attorney General's Legal Advisory on the Application of Existing California Laws to Artificial Intelligence
- California Attorney General's Legal Advisory on the Application of Existing California Law to Artificial Intelligence in Healthcare

1. **California Medical Information Act (CMIA)**
   - Safeguards individually identifiable medical information maintained by healthcare providers, health plans, and contractors in California, imposing strict confidentiality and disclosure requirements beyond those of HIPAA.
   - Any AI tool that stores, processes, or generates predictions using identifiable health data must comply with CMIA protections, including rules around patient authorization, access, and disclosure.
2. **California Consumer Privacy Act (CCPA)**
   - Overview: Grants California residents rights over their personal information held by businesses, including the right to know, delete, and opt-out of the sale of personal data.
   - Applies to businesses that collect personal data of California residents and meet certain thresholds.
   - Provides Californians with the right to know about the personal information that a

business collects about them, the right to opt out of the sale or sharing of their personal information, and the right to limit the disclosure of their sensitive personal information.

2. California Privacy Rights Act (CPRA)

- Amends and expands the CCPA, introducing new rights and establishing the California Privacy Protection Agency to enforce privacy laws.
- Introduces the concept of "sensitive personal information."
- Provides consumers with the right to correct inaccurate personal information.

3. AB 3030 – Generative AI in Healthcare Communications

- Overview: Mandates that healthcare providers disclose when generative AI is used to generate patient communications concerning clinical information.
- Requires providers to include a disclaimer indicating the communication was generated by AI.
- Requires providers to provide clear instructions for patients to contact a human healthcare provider.

4. Unfair Competition Law

- Applies to developers of AI tools
- Protects Californians against unlawful, unfair, or fraudulent business acts or practices

5. Unruh Civil Rights Act

- Prohibits discrimination based on sex, race, color, religion, ancestry, national origin, disability, medical condition, genetic information, marital status, sexual orientation, citizenship, primary language, or immigration status.
- Can impact the types of discriminatory practices likely to be caused by AI, including denial of full and equal access.

Federal Laws & Regulations

1. Health Insurance Portability and Accountability Act (HIPAA)

- Overview: Establishes national standards to protect individuals' medical records and other personal health information.
- Privacy Rule: Sets standards for the protection of health information.
- Security Rule: Specifies safeguards to ensure the confidentiality, integrity, and security of electronic protected health information (ePHI).

2. Health Information Technology for Economic and Clinical Health (HITECH) Act

- Overview: Promotes the adoption and meaningful use of health information technology, enhancing privacy and security protections under HIPAA.
- Strengthens enforcement of HIPAA rules.

- Introduces breach notification requirements.

3. Food and Drug Administration (FDA) Regulations on AI/ML-Based Software as a Medical Device (SaMD)

- Overview: Provides a regulatory framework for AI and machine learning-based software intended for medical purposes.
- AI/ML-Based SaMD Action Plan: Outlines the FDA's approach to regulating AI/ML-based medical software.

4. Assistant Secretary for Technology Policy, Office of the National Coordinator for Health Information Technology (ASTP/ONC) Regulations

- Overview: Sets standards and certification criteria for electronic health record (EHR) systems to ensure interoperability and secure data exchange.
- Certification of health IT products.
- Promotion of nationwide health information exchange.