

REVIEW PROCESS GUIDE

Responsible Use of Artificial Intelligence in Health Care



Issued June 1, 2026

Joint Commission Mission

Joint Commission's mission is to enable and affirm the highest standards of healthcare quality and safety for all.

© 2026 Joint Commission

Published by Joint Commission Resources

Oakbrook Terrace, Illinois 60181 USA

<https://www.jcrinc.com>

Joint Commission Resources, Inc. (JCR), a not-for-profit affiliate of Joint Commission, has been designated by Joint Commission to publish publications and multimedia products. JCR reproduces and distributes these materials under license from Joint Commission.

JCR educational programs and publications support, but are separate from, the accreditation activities of Joint Commission. Attendees at JCR educational programs and purchasers of JCR publications receive no special consideration or treatment in, or confidential information about, the accreditation process.

All rights reserved. No part of this publication may be reproduced in any form or by any means without written permission from the publisher. Requests for permission to make copies of any part of this work should be sent to permissions@jcrinc.com.

For more information about Joint Commission, please visit

<https://www.jointcommission.org>.

Disclaimer

THIS CERTIFICATION PROVIDES AN ASSESSMENT OF AN ORGANIZATION'S COMMITMENT TO THE RESPONSIBLE USE OF HEALTH AI THROUGH ORGANIZATIONWIDE GOVERNANCE AND FOCUSED POLICIES AND PROCEDURES. AN ORGANIZATION IS FULLY RESPONSIBLE FOR ITS OWN EXPERT ANALYSIS AND CONFIRMATION THAT IT IS PROPERLY FOLLOWING LAWS, RULES, AND REGULATIONS RELATED TO THE DEVELOPMENT, IMPLEMENTATION, AND OVERSIGHT OF HEALTH AI POLICIES AND PROCEDURES, INCLUDING REQUIREMENTS FOR DATA MANAGEMENT, PRIVACY, SECURITY, USE, AND TRANSFER.

THE SERVICES PROVIDED UNDER THIS CERTIFICATION DO NOT SERVE AS A SUBSTITUTE FOR ANY ORGANIZATION RESPONSIBILITIES RELATED TO THE SUBJECT MATTER OF THE CERTIFICATION. NO REPRESENTATIONS OR WARRANTIES ARE MADE BY JOINT COMMISSION CONCERNING THE EFFECT(S), IF ANY, OF THE CERTIFICATION IT PROVIDES UNDER AGREEMENT ON THE QUALITY OF CARE OR TREATMENT, POLICIES, PROCEDURES, PROCESSES, AND DATA USE, OR THE OUTCOMES THEREOF, PROVIDED OR PERFORMED BY THE ORGANIZATION. THE SERVICES TO BE PROVIDED BY JOINT COMMISSION ARE SEPARATE FROM ANY COMPLIANCE WITH LAWS, RULES, OR REGULATIONS APPLICABLE TO THE ORGANIZATION, AND JOINT COMMISSION SPECIFICALLY DISCLAIMS ANY RESPONSIBILITY OR LIABILITY FOR THE ORGANIZATION'S FAILURE TO MEET THE REQUIREMENTS OF ANY APPLICABLE LAWS, RULES, OR REGULATIONS.

THE ORGANIZATION SHALL BE SOLELY RESPONSIBLE FOR MAINTAINING ITS OWN EFFECTIVE PROGRAMS, POLICIES, PROCEDURES, RECORDKEEPING, DECISION MAKING, AND MANAGEMENT FUNCTIONS. AS SUCH, THE ORGANIZATION SHALL BE SOLELY AND FULLY RESPONSIBLE UNDER THE AGREEMENT FOR (a) APPLYING INDEPENDENT JUDGMENT (b) MAKING ALL IMPLEMENTATION DECISIONS AND (c) DETERMINING FURTHER COURSES OF ACTION WITH RESPECT TO ANY MATTERS ADDRESSED BY THE SURVEYORS EITHER ORALLY OR IN WRITING.

Contents

General Guidance and Overview	2
Prereview Outreach	2
Information Evaluated Prior to Certification Review	3
Questions About the Standards	3
Opening Conference and Governance Session.....	4
Discussion Topics.....	4
AI Governance Playbook. Domain 2: Organizational Structures	6
Planning Session and Program Document Review	7
AI Governance Playbook. Domain 1: AI Policy	8
Health AI Tool or System Tracer Activity.....	9
Tracer 1: High-risk clinical use case health AI tool or system tracer	10
Discussion Questions	10
Tracer 2: Third-party vendor clinical or nonclinical use case health AI tool or system tracer.....	13
Discussion Questions	13
AI Governance Playbook. Domain 3: Organizational Resources.....	15
AI Governance Playbook. Domain 4.1: Responsible AI Lifecycle Management and Use	16
AI Governance Playbook. Domain 4.2: Risk and Impact Assessments.....	17
AI Governance Playbook. Domain 4.3: Responsible Data Management and Use	18
AI Governance Playbook. Domain 4.4: Third Party Management	19
Staff Education and Training Session	20
AI Governance Playbook. Domain 3: Organizational Resources.....	20
AI Governance Playbook. Domain 4.5: Education, Training, and Feedback	21
Reviewer Report Preparation.....	22
Exit Conference	23

General Guidance and Overview

The purpose of the Review Process Guide (RPG) is to inform organizations and reviewers about the Responsible Use of Artificial Intelligence in Health Care (RUIH) review process.

Organizations are encouraged to review the following documents prior to their review:

- Agenda (as applicable to their program). The agendas can be obtained on Joint Commission's website: [Review Agenda | Joint Commission](#).
- RUIH requirements listed in the *Comprehensive Certification Manual for Responsible Use of Artificial Intelligence in Health Care*.
- *Joint Commission News* articles about new and/or revised RUIH requirements. *JC News* posts monthly to your organization's *Joint Commission Connect*® extranet site.

Prereview Outreach

A Joint Commission account executive will contact your organization by phone or e-mail shortly after receiving your application for certification or recertification. The purpose of this call or e-mail with the account executive is to do the following:

- Confirm information reported in the application for certification or recertification.
- Confirm access to *Joint Commission Connect* and the certification-related information available there.
- Confirm accuracy of any program-specific eligibility requirements.
- Communicate document submission requirements and due date.

Note 1: Documents are due 7 business days prior to review date.

Note 2: The RUIH program uploads program-specific documents based on the current document list available through the *Joint Commission Connect*, which must be completed by the due date listed on the "What's Due" section. Your account executive will assist with the process in advance of certification review if needed.

- Answer any questions and address any concerns.

Note: For all certification reviews, electronic recordings, including artificial intelligence (AI) or other transcribing platforms, are not allowed per Joint Commission policy.

Information Evaluated Prior to Certification Review

Questions About the Standards

To submit a question:

- Log in to [Joint Commission Connect](#) and click on Resources—Standards Interpretation to submit the question.

OR

- If personnel access is limited, log in to [Joint Commission Connect](#), then go to the [Standards Interpretation Page](#) to submit a question.

For questions about the review process, agenda, scheduling, and so on, please contact your Joint Commission account executive.

Opening Conference and Governance Session

Duration: 60 minutes

Objective

- To gain a better understanding of the RUAIH program and its governance structure, collect background information to inform review tracers, and answer any questions

Organization Participants

- Program executive and individuals (for example, team or committee members) who are responsible for leading the use of health AI across the organization
- Individual(s) who will participate in tracer activities
- Others at the discretion of the organization

Materials Needed

- Introductory overview of program (While not required, many organizations choose to prepare a slide deck as an introductory overview.)
- Supporting evidence on the discussion topics below

Activities

- Reviewer and program staff introduce themselves.
- Reviewer presents the review agenda and objectives.
- Program leaders present an overview of the program, which includes but is not limited to the following:
 - Factors that influence AI technology adoption in the organization (for example, patient safety/quality, workflow efficiency/productivity)
 - Program leadership and reporting structure or established teams/arrangements to provide leadership and oversight for the program
 - Planned, piloted, deployed, scaled, paused, or withdrawn AI tools and systems, such as:
 - Clinical vs. administrative use cases
 - Vendor developed, internally developed, or codeveloped tools and systems
- Reviewer facilitates a guided discussion.

Discussion Topics

Governance Structure

- Describe the organization's governance structure for health AI, including whether required expertise is provided internally, obtained through external sources, or both. Include how the organization ensures sufficient representation from clinical, operational, compliance, information technology (IT), and other relevant domains. (RUAIH.01.01.01 EP 1)

Governance Oversight of Use Cases

- Describe the role of governance in defining the process for health AI tool or system intake (procurement). What information is gathered during intake to establish baseline information on an AI solution's intended use and risk? (RUIH.01.01.01 EP 1)
- What criteria does the organization use to determine which health AI use cases require governance-level oversight? What criteria or conditions would prevent an AI solution from proceeding to deployment? (RUIH.03.01.01 EP 1)
- How does the organization apply a risk-based approach when determining the level of resources (that is, the level of documentation, evaluation, monitoring, and other governance activities needed for different AI systems)? (RUIH.01.01.01 EP 2)
- Describe the process for escalating AI-related risks, biases, and safety concerns to the executive responsible for the program and organization leaders. Describe the process used to inform the governing body about including outcomes, risks, and potential or actual adverse events. (RUIH.01.01.01 EP 3) How do AI-related incidents differ from traditional safety events and how they are investigated and escalated? (RUIH.07.01.01 EPs 1–4)

Stakeholder Engagement in AI Governance

- Describe how relevant stakeholders, including legal, ethics, IT, cybersecurity, operational, and clinical leaders, are engaged in the development and review of health AI policies. (RUIH.03.01.01 EP 3)

Training and Workforce Education

- Describe how the organization trains staff on policies and procedures related to AI tools and systems to promote safe adoption. What additional resources are available to support appropriate and responsible AI use? If applicable, describe how the organization ensures clinicians understand where AI influences clinical decision-making. (RUIH.08.01.01 EP 1)

The following additional resources are intended to support organizations in safe deployment and operations of AI tools and systems.

AI Governance Playbook. Domain 2: Organizational Structures

Standard/EP	CHAI™ Baseline Operational Controls*	CHAI Implementation Guidance (Suggestions Based on Known Practices)
RUIAH.01.01.01 EP 1	Control 1: Ensure your organization has staff assigned to critical roles and responsibilities (as defined by your organization). These can be existing or new staff, and one staff member may hold multiple responsibilities (one-to-many).	Models of Governance Structure
	Control 2: Establish a formal committee structure bringing together all governance stakeholders.	
RUIAH.01.01.01 EP 1	Control 3: Establish an intake, assessment, and monitoring process for thorough investigation of prospective solutions and mechanisms for incident detection, feedback, and follow-up.	Health AI Tools Selection or Intake
RUIAH.01.01.01 EP 3 RUIAH.07.01.01 EPs 1–4	Control 4: Establish protocols for escalating and communicating concerns/incidents for resolution to the governance structure.	Escalation to Governance Triggers

* Excerpt from *AI Governance Playbook. Domain 2: Organizational Structures*. © 2026 by Coalition for Health AI. Used with permission.

Planning Session and Program Document Review

Duration: 30 minutes

Objective

To review program policies and assess processes for policy oversight and dissemination among relevant organization staff

Organization Participants

- Program representative(s) familiar with organization health AI tool and system policies

Materials Needed

- The organization is required to upload required documents **7 business days prior to review date** (see General Guidance and Overview section).

Activities

Reviewer assesses materials provided to verify the following:

- The organization has developed AI policies and procedures for the intake, procurement, implementation (use), and lifecycle management of health AI tools and systems. (RUIH.01.01.01 EP 1)
- Organization AI policies and procedures address the following:
 - Scope, permitted/prohibited AI uses (for example, prohibition of use of protected health information (PHI) in public AI tools and systems) (RUIH.03.01.01 EP 2)
 - Organization's definition of responsible AI principles (RUIH.03.01.01 EP 1)
 - Criteria for which health AI tools and systems require governance, including tools that are internally developed, vendor supplied, and platform embedded (RUIH.03.01.01 EP 1)
 - Direct alignment with or reference to the organization's policies on data safety, including policies on cybersecurity, data governance, and privacy (RUIH.03.01.01 EP 4)
- Health AI policies are reviewed at least annually by relevant stakeholders. (RUIH.03.01.01 EPs 3 and 6)
- Health AI policies are approved by the governing body or executive leaders. (RUIH.03.01.01 EP 5)
- Program representative(s) can demonstrate that relevant staff users of AI solutions have access to health AI policies (for example, through portals, trackers, organization's policy internal webpage). (RUIH.03.01.01 EP 6)

AI Governance Playbook. Domain 1: AI Policy

Standard/EP	CHAI Baseline Operational Controls [†]	CHAI Implementation Guidance (Suggestions Based on Known Practices)
RUAIH.03.01.01 EPs 1–6	Control 1: Develop a formal AI Policy document, approved by organizational leadership, and make accessible to all relevant staff.	AI Policy and Executive Sponsorship
RUAIH.03.01.01 EPs 1–4	Control 2: Define key concepts in the AI Policy (e.g., definition of AI, scope of AI solution use, AI approval process).	Defining Key Concepts and Scope, AI Policy Changes and Maintenance
RUAIH.01.01.01 EP 1	Control 3: Establish an appropriate individual or individuals with designated oversight for policy changes.	

[†] Excerpt from *AI Governance Playbook. Domain 1: AI Policy*. © 2026 by Coalition for Health AI. Used with permission.

Health AI Tool or System Tracer Activity

Duration: 3 hours 30 minutes

Objectives

- Using at least two health AI tools or systems, to trace how the organization governs, deploys, uses, monitors, and responds to risks across the full AI lifecycle (that is, intake/procurement, risk categorization/assessment, pre-deployment, piloting [if applicable], deployment, monitoring, termination [if applicable])
- Ideally, to validate that governance decisions, risk/bias management, data protections, and AI transparency principles are implemented in practice for both clinical and nonclinical AI solutions

Organization Participants

- Program leaders, tool owner(s), and representatives from clinical/operational areas, IT, cybersecurity, privacy, and risk/safety who support the selected tools

Materials Needed

- Virtual meeting link with screensharing enabled
- Electronic access (via secure share) to the AI registry/intake record for the selected tool(s) or system(s), including intended use, owner, risk categorization, and lifecycle traceability records (for example, version history, validation evidence, mitigation controls, review status) (RUIH.04.01.01 EP 5)
- Vendor documentation of known biases, limitations, and risks for the selected tool(s) or system(s) (RUIH.06.01.01 EP 1)
- Data protection agreements applicable to the tool(s) or system(s), such as business associate agreements (BAAs) for PHI and data use agreements (DUAs) or equivalent contractual controls for non-HIPAA data used in health AI tools, as appropriate to the data type and use case (RUIH.02.01.01 EPs 3,4)
- Evidence of monitoring of health AI tool or system performance throughout its lifecycle (for example, performance/bias dashboards, drift alerts, review cadence, revalidation triggers, recent reports) (RUIH.06.01.01 EP 2; RUIH.05.01.01 EP 2)
- Evidence of internal tracking of safety events associated with AI use and investigation(s) (for example, root cause analyses, vendor communications, meeting minutes, presentations on AI-related event trends) (RUIH.07.01.01 EPs 1–4)
- Brief remote demonstration (live or screenshots) of how users access the health AI tool or system output (for example, electronic health record (EHR) view, dashboard, portal), including any warnings/limitations and documentation expectations

Instructions

Reviewer selects *at least* two health AI tools or systems to trace from the following options (selection is based on the AI use cases the organization has deployed):

- **Tracer 1: High-risk clinical use case health AI tool or system tracer** (for example, deterioration prediction/early warning clinical decision support): Assess for risk categorization, bias, mitigation, and system-level impacts.
- **Tracer 2: Third-party vendor clinical or nonclinical use case health AI tool or system tracer** (for example, health AI tool or system for clinical documentation): Follow a vendor-supplied or cloud-hosted AI tool or system from intake to assess deployment, use, and performance monitoring, including PHI protections and governance influence on controls.

Tracer 1: High-risk clinical use case health AI tool or system tracer

Focus: High-risk clinical AI decision support where incorrect, delayed, or overtriggered outputs could contribute to patient harm (for example, sepsis early warning/deterioration prediction). Trace how the organization categorizes risk, identifies biases, implements mitigations and limits on use, monitors performance over time, and ensures transparency and accountability in clinical practice.

Applies to: Clinical health AI tools and systems used to inform diagnosis, triage, escalation, treatment initiation, or other time-sensitive decisions (internally developed, vendor supplied, or platform embedded), including tools and systems that use PHI and require patient transparency/education regarding AI use.

Discussion Questions

- **Use case (intended use and decision influence)**
 - What clinical decision(s) does the tool influence (for example, initiating a sepsis bundle, escalating level of care, activating rapid response) and at what point in the workflow? (RUAIH.06.01.01 EP 1)
 - Is the tool advisory or triage, or does it automatically trigger orders/alerts? What is the required human review step before action is taken? (RUAIH.03.01.01 EP 2; RUAIH.06.01.01 EP 1)
 - Who are the intended users (nurses, physicians, rapid response team), and what training is required before they rely on the output? (RUAIH.08.01.01 EP 1)
- **Risk categorization (why this is “high risk” and how was that determined)**
 - How did you define “high risk” for this use case (for example, potential for delayed treatment, inappropriate treatment)? (RUAIH.05.01.01 EP 1)
 - Was a pre-deployment risk categorization conducted and considered for patient safety, financial, legal, and operational domains? What evidence supported the categorization decision (vendor documentation, local pilot results, clinical leader review)? (RUAIH.04.01.01 EP 1)
 - How do you document risk category? (RUAIH.04.01.01 EP 2, 5)
 - Does this tool meet the criteria for AI tool and system governance? (RUAIH.03.01.01 EP 1)

- What specific governance input (for example, committee recommendations), if any, changed the outcome of this risk categorization (for example, elevating to high risk, requiring a pilot, adding monitoring, narrowing the intended use)? (RUIH.03.01.01 EP 1)
- How are governance decisions regarding this health AI tool or system being tracked (for example, minutes, approval memo, intake record)? (RUIH.03.01.01 EP 1)
- **Hazard-focused risk assessment (identifying specific hazards and harms)**
 - What are the most concerning *failure modes* for this tool or system in practice (for example, false negatives missing sepsis, false positives causing overtreatment, alert fatigue, automation bias)? (RUIH.05.01.01 EP 1)
 - Have you performed pre-implementation validation testing/baseline testing to determine whether the health AI tool or system could lead to patient harm, performs differently across subgroups or settings, or may cause operational disruptions? (RUIH.04.01.01 EP 3)
 - How did you assess bias risk (for example, age, sex, race/ethnicity)? (RUIH.05.01.01 EP 1)
 - How did you determine whether the tool or system was developed for its intended purpose using appropriately representative training datasets? (RUIH.05.01.01 EP 2)
 - How did you verify if the tool or system underwent bias detection assessments during development (for example, vendor documentation or internal development records)? (RUIH.05.01.01 EP 2)
 - What detailed requirements exist for ongoing bias detection (for example, metrics, stratification, thresholds, triggers, documentation expectations)? (RUIH.05.01.01 EP 2)
 - How do you regularly monitor and audit the tool or system to identify bias when appropriate (for example, cadence, responsible parties, reporting, corrective actions)? (RUIH.05.01.01 EP 2)
- **Mitigation controls (how hazards are reduced and how you know that controls work)**
 - What *risk controls* were implemented (for example, workflow guardrails, alert tiering, hard stops, order-set constraints, second-review requirements, downtime plans)? (RUIH.05.01.01 EP 3)
 - How do you monitor whether controls are effective (for example, override rates, alert response time, near-miss reporting, calibration drift, safety event review)? (RUIH.06.01.01 EP 2)
 - What “stop rules” or triggers lead you to pause or withdraw the tool or system (for example, performance drift, safety signals, vendor change notice, adverse events)? (RUIH.06.01.01 EP 2)
 - How would leaders be updated on the status of the tool or system use and decide to continue, modify, scale, pause, or withdraw the tool or system based on evidence? (RUIH.03.01.01 EP 1)

- **Monitoring and continuous risk management (post-deployment)**
 - What key performance and safety metrics are monitored routinely for this health AI tool or system? (RUIH.06.01.01 EP 2)
 - How do you conduct regular security assessments and vulnerability scans for this tool and its supporting infrastructure (including any vendor-hosted components) within the organization's defined time frames, and how are findings tracked to remediation? (RUIH.04.01.01 EP 6)
 - How do you monitor whether *bias mitigation controls remain effective over time* (for example, periodic subgroup performance checks, recalibration by subgroup, monitoring for differential alert burden), and what is the review cadence? (RUIH.05.01.01 EP 2)
 - When bias signals are detected, what is the defined response pathway (for example, investigation, workflow changes, threshold tuning, retraining/revalidation, patient safety review), and how are actions communicated to stakeholders? (RUIH.05.01.01 EP 3; RUIH.08.01.01 EP 1)
- **System-level impact assessment (broader consequences beyond discrete hazards)**
 - What unintended consequences have you looked for (for example, overdiagnosis, treatment inequities, shifts in clinician autonomy, reduced bedside assessment, increased workload)? (RUIH.06.01.01 EP 2)
 - Have there been downstream operational effects created by deployment of this AI tool or system, and how are these monitored? (RUIH.06.01.01 EP 2)
 - What health AI-specific cybersecurity risks and systemwide impacts have been assessed (for example, adversarial manipulation that could systematically shift outputs, large-scale alert disruption, PHI exposure through integrations, compromised model/service availability)? (RUIH.04.01.01 EP 7)
 - Has the tool or system and its supporting infrastructure undergone penetration testing within the defined timeframe (including cloud services, EHR integrations, and identity/access pathways), and how are findings prioritized and tracked to remediation? (RUIH.04.01.01 EP 7)
 - If the tool uses internal or vendor application programming interfaces (APIs), what AI-specific API security reviews are performed (for example, authentication/authorization, least privilege scopes, rate limiting, logging/monitoring, input validation, injection protections, protection against data exfiltration), and how often? (RUIH.04.01.01 EP 7)
 - What protections are in place to reduce model theft or unauthorized extraction? (RUIH.04.01.01 EP 7)
- **Transparency and accountability**
 - What process exists to support patient transparency and/or consent when AI directly affects care? (RUIH.09.01.01 EP 1)
 - When consent is required, who is responsible for obtaining it, and how is consent captured? (RUIH.09.01.01 EP 1)

- For this AI use case, can patients opt out? If yes, what is the process for receiving, documenting, and operationalizing opt-out requests without compromising safety? If no, how is that communicated to patients? (RUAIH.09.01.01 EP 1)
- Describe how the organization's Notice of Privacy Practices (NPP) is updated and provided, in accordance with applicable law and regulation, to explain how PHI may be used or disclosed by AI-enabled systems (RUAIH.09.01.01 EP 3)

Tracer 2: Third-party vendor clinical or nonclinical use case health AI tool or system tracer

Focus: Third-party vendor AI governance across the full lifecycle, including risk/bias controls, PHI protection, and response to safety or privacy incidents

Applies to: Clinical and nonclinical AI solutions (vendor-supplied or cloud-hosted)

Examples of third-party tool scenarios (select one to trace):

- **Clinical:** Examples include vendor AI tools or systems generating patient risk scores, imaging tools flagging urgent scans at the top of the reading list, and tools that warn the care team when a patient may be getting worse.
- **Nonclinical:** Examples include vendor AI tools or systems for clinical documentation, prior authorization automation, coding assistance, and patient scheduling optimization.
- **Shared risk theme:** Examples include vendor AI tools or systems involving access to PHI (directly or via integration), cloud processing, and model updates outside the organization's direct control.

Discussion Questions

- **Intake/selection**
 - How did this tool enter the organization (for example, procurement request, platform-embedded feature, renewal, pilot)? What gate(s) ensured it went through the health AI intake using an established governance process rather than “shadow AI” adoption? (RUAIH.03.01.01 EP 1)
 - What documentation did the vendor provide (for example, model card/solution card, technical documentation, validation reports), and how can users and leaders access it? (RUAIH.06.01.01 EP 1)
 - Does this health AI use case require governance-level oversight? (RUAIH.03.01.01 EP 1)
 - If so, what governance review(s) occurred before selection (for example, AI committee, privacy/security, clinical safety), and what conditions or constraints did governance place on adoption (for example, pilot-first, limited rollout, required mitigations, PHI controls, monitoring plan)? (RUAIH.03.01.01 EP 1)
 - How does the vendor educate and train the organization's staff to ensure effective adoption and ongoing use of the product or service? How do you administer and ensure timeliness and relevance of education and training? (RUAIH.08.01.01 EP 1, 2)
- **Risk, bias, and mitigation planning**

- What risks and potential biases were identified for this use case (for example, workflow-related bias or subgroup performance differences)? (RUIH.05.01.01 EP 1)
- How did bias information affect risk categorization (RUIH.04.01.01 EP 1) or mitigations? (RUIH.05.01.01 EP 3)
- What is your process when bias is detected post-deployment, how is bias identified, what would be done to mitigate, how quickly, and who is notified? (RUIH.05.01.01 EP 1, 3)
- **PHI and data protection (BAA/DUA)**
 - How do you ensure only HIPAA-compliant deidentification methods are applied, and how are they validated? (RUIH.02.01.01 EP 1)
 - For a potential PHI breach involving this tool, system, or vendor, what would be the organization's decision points, roles, and required timelines for investigation, notification, and reporting under HIPAA and applicable state laws, and what evidence is retained (for example, incident log, notifications, post-incident review)? (RUIH.02.01.01 EP 1)
 - Does this tool use or disclose PHI? If yes, is there a BAA that addresses all the required elements? (RUIH.02.01.01 EP 3)
 - For non-HIPAA data used in health AI tools and systems, how do you determine if HIPAA does not apply (for example, limited data set or de-identified data)? What does the DUA prohibit (unauthorized reidentification, secondary use), and what audit rights and penalties exist? (RUIH.02.01.01 EP 4)
 - Describe how the organization aligns its health AI security infrastructure, policies, and procedures with nationally recognized cybersecurity frameworks and provide evidence of that alignment. (RUIH.02.01.01 EP 2)
- **Deployment/implementation controls**
 - If this health AI use case requires governance-level oversight, which implementation decisions required governance approval (for example, go-live criteria, threshold settings, user eligibility, documentation requirements)? (RUIH.03.01.01 EP 1)
 - Was pre-deployment testing or piloting performed (technical integration, workflow simulation) prior to full deployment? What criteria or factors determined the need for pre-deployment testing? (RUIH.04.01.01 EPs 3, 4)
 - What training was provided to staff who directly use or are affected by this particular health AI tool, system, or workflow? (RUIH.08.01.01 EP 1)
- **Use in practice**
 - What safeguards prevent inappropriate use outside intended scope? (RUIH.03.01.01 EP 2; RUIH.06.01.01 EP 2)
 - When AI directly affects a patient's care (for example, triage, risk scoring, imaging prioritization, clinical documentation used for decision-making), what is your process for informing the patient, including how data may be used, when consent is required, whether opt-out is available, and where this process is documented? (RUIH.09.01.01 EP 1)
 - What information is provided to patients about how their PHI is used by this AI tool? Does the NPP reflect this information? (RUIH.09.01.01 EP 2)
- **Ongoing monitoring and evaluation**

- What metrics are monitored for this tool (for example, safety outcomes, accuracy/performance, alert burden, overrides)? Who reviews them, and how often? (RUIH.06.01.01 EP 2)
- What monitoring is performed by the vendor vs. the organization, and how do you validate vendor-reported performance? (RUIH.06.01.01 EP 2)
- **Incident response**
 - How do you coordinate with the vendor on root cause analysis? What is the vendor's required response time? (RUIH.07.01.01 EP 3)
 - How are lessons learned incorporated (for example, policy updates, training updates, contract amendments at renewal, monitoring threshold changes)? (RUIH.07.01.01 EP 4)

AI Governance Playbook. Domain 3: Organizational Resources

Standard/EP	CHAI Baseline Operational Controls [†]	CHAI Implementation Guidance (Suggestions Based on Known Practices)
RUIH.02.01.01 EP 2	Control 1: Identify and document security infrastructure and methods (e.g. HITRUST, SOC 2, NIST CSF, CISA) available and needed to protect data; including methods for encrypting data at rest and in transit.	Establishing a Security Baseline Aligned with Recognized Frameworks. Encryption Standards, Addressing Data Security Risks
RUIH.04.01.01 EP 6	Control 2: Identify and document the tooling and data resources available and needed to conduct regular security assessments and vulnerability scans to identify and address risks.	Inventorying Existing Security Assessment Tools and Data Access and Identifying Gaps
RUIH.04.01.01 EP 7	Control 3: Identify and document tools, resources, and methods available and needed to implement AI cybersecurity evaluation (penetration testing, adversarial robustness, etc.).	AI Cybersecurity Evaluation, Vendor Evaluation
RUIH.04.01.01 EP 5	Control 4: Maintain comprehensive records of AI-related assets including datasets, models, and tools to ensure traceability.	Governance of Documentation for All AI Assets
	Control 5: Identify and document tools and resources available and needed for standard documentation of all AI systems and for integrating them into an AI inventory, such as adopting a Model Card.	Capturing Critical Information about AI Systems: An Applied Model Card (AMC)

[†] Excerpt from *AI Governance Playbook. Domain 3: Organizational Resources*. © 2026 by Coalition for Health AI. Used with permission.

	Control 6: Identify and document the tools and resources available and needed to implement and maintain an AI inventory registry to track internal and third-party models.	AI inventory
RUAIH.01.01.01 EP 2	Control 7: Identify and document the tools and resources available and needed to carry out validation testing and monitoring for relevant AI models, including responsible AI baseline tests.	Resources for Validation Testing, Including Definitions of Responsible AI Principles (that is, fairness)
RUAIH.01.01.01 EP 2	Control 8: Identify and document the computing resources available and needed to conduct recurring cybersecurity audits of AI infrastructure; enforce access controls and HIPAA compliance.	Infrastructure for Cybersecurity Audits of AI Infrastructure, Enforcement of HIPAA Compliance

AI Governance Playbook. Domain 4.1: Responsible AI Lifecycle Management and Use

- Intake/Procurement
- Risk
- Pre-deployment
- Piloting
- Deployment
- Monitoring
- Termination

Standard/EP	CHAI Baseline Operational Controls[§]	CHAI Implementation Guidance (Suggestions Based on Known Practices)
RUAIH.06.01.01 EP 1	Control 1: Develop and maintain a process that appropriately assesses and documents intended use of each AI system.	Template for Control #1
RUAIH.03.01.01 EPs 1, 2	Control 2: Define responsible AI principles, as aligned with the organization's mission and goal (e.g., usefulness, fairness, safety, transparency, security, privacy); document the objectives and processes that the organization will use to align with these principles across relevant lifecycle stages.	Operationalizing controls #2 and #3

[§] Excerpt from *AI Governance Playbook. Domain 4.1: Responsible AI Lifecycle Management and Use*. © 2026 by Coalition for Health AI. Used with permission.

RUAIH.01.01.01 EP 1 RUAIH.03.01.01 EPs 1, 2	Control 3: Operationalize a process to evaluate defined responsible AI principles (e.g., usefulness, fairness, safety, transparency, security, privacy) and reference industry recommended evaluation frameworks where available.	
RUAIH.04.01.01 EP 4 RUAIH.05.01.01 EPs 1–3 RUAIH.06.01.01 EP 2	Control 4: Define a process to monitor the safety, performance, and responsible use of AI-enabled solutions.	Operationalizing controls #4 and #5
RUAIH.06.01.01 EP 2 RUAIH.07.01.01 EPs 1–3	Control 5: Establish a monitoring mechanism or process for performance reporting via a dashboard or similar interface. Monitoring mechanisms or processes should flag unexpected patterns for review by responsible parties.	
RUAIH.01.01.01 EP 3 RUAIH.03.01.01 EP 3 RUAIH.07.01.01 EP 4	Control 6: Establish a process to inform relevant stakeholders about Responsible AI principles and processes (e.g., definitions, evaluation, monitoring).	Operationalizing control #6

AI Governance Playbook. Domain 4.2: Risk and Impact Assessments

Standard/EP	CHAI Baseline Operational Controls**	CHAI Implementation Guidance
RUAIH.04.01.01 EP 1	Control 1: Conduct a Risk Categorization assessment (pre-deployment) to categorize risk in the context of the organization's AI use case scope.	CHAI Risk Categorization Tool
RUAIH.04.01.01 EP 2	Control 2: Document how Risk Categorization is evaluated, recorded, retained, and reviewed.	
RUAIH.05.01.01 EPs 1, 2	Control 3: Leverage a rigorous Risk Assessment to evaluate AI solutions that are categorized as higher risk (as defined by the organization).	Risk Assessment Tools
RUAIH.05.01.01 EPs 1, 2	Control 4: Document how Risk Assessment is evaluated, recorded, retained, and reviewed.	

** Excerpt from *AI Governance Playbook. Domain 4.2: Risk and Impact Assessments*. © 2026 by Coalition for Health AI. Used with permission.

AI Governance Playbook. Domain 4.3: Responsible Data Management and Use

Standard/EP	CHAI Baseline Operational Controls ^{††}	CHAI Implementation Guidance (Suggestions Based on Known Practices)
RUAIH.04.01.01 EP 5	Control 1: Create and maintain a data acquisition register tracking origin, handling, and intended use of data used in AI systems.	Data Acquisition Register
RUAIH.02.01.01 EPs 3, 4	Control 2: Establish comprehensive Data Use Agreements and/or Business Associate Agreements that includes information on permitted and prohibited uses, compliance with organization's security and privacy requirements, rights to audit, consequences of non-compliance, and data return/destruction terms at end of use.	Key DUA Provisions for AI
RUAIH.02.01.01 EP 1	Control 3: Establish written HIPAA-compliant de-identification policies (Safe Harbor or Expert Determination) considering applicable state privacy laws; evaluate each PHI-containing dataset to select the method that minimizes re-identification risk; validate de-identification before any dataset is used in AI training or model development; and maintain continuous oversight of de-identified datasets, reassessing re-identification risk whenever datasets are linked or new identifiers emerge.	HIPAA Deidentification Methods, AI-Specific Deidentification Considerations
RUAIH.05.01.01 EP 1	Control 4: Establish a process for recurring AI data quality and bias evaluation to help identify quality gaps and known sources of bias.	Sources of Bias in Healthcare AI Data, Data Quality for AI
RUAIH.05.01.01 EP 1	Control 5: Establish a standard operating procedure (SOP) for AI data preparation.	Key Elements of an AI Data Preparation SOP

^{††} Excerpt from *AI Governance Playbook. Domain 4.3: Responsible Data Management and Use*. © 2026 by Coalition for Health AI. Used with permission.

AI Governance Playbook. Domain 4.4: Third Party Management

Standard/EP	CHAI Baseline Operational Controls ^{††}	CHAI Implementation Guidance (Suggestions Based on Known Practices)
RUAIH.02.01.01 EPs 3, 4 RUAIH.03.01.01 EP 1 RUAIH.05.01.01 EP 1 RUAIH.06.01.01 EP 1	Control 1: Include clauses in all AI vendor contracts that specify clinical, operational, and regulatory responsibilities; outline requirements for disclosure of known model limitations and risks; define liability for harm or failure resulting from the AI system.	Defining Clinical, Operational, Regulatory Responsibilities for Vendors

^{††} Excerpt from *AI Governance Playbook. Domain 4.4: Third Party Management*. © 2026 by Coalition for Health AI. Used with permission.

Staff Education and Training Session

Duration: 30 minutes

Organization Participants

- Program representative(s) familiar with staff education and training on health AI tools and systems

Objective

To verify that the organization provides education and training on health AI tools and systems used in the organization

Activities

- From the health AI tool or system tracers, identify at least two primary users (for example, nurses, physicians, coders, schedulers, case managers).
- Review files for evidence of training materials and completion records for initial training, ongoing training at least every two years, and retraining after health AI tool, system, and/or policy and procedures changes. (RUIH.08.01.01 EP 2)
- Verify education and training are tailored to staff roles, responsibilities, and level of interaction with health AI tools and systems. (RUIH.08.01.01 EP 1)
- Verify education and training include AI literacy and change management to support safe, informed adoption of health AI tools and systems, and provide case-specific training for staff who directly use or are affected by a particular tool, system, or workflow. (RUIH.08.01.01 EP 1)

AI Governance Playbook. Domain 3: Organizational Resources

Standard/EP	CHAI Baseline Operational Controls ^{ss}	CHAI Implementation Guidance (Suggestions Based on Known Practices)
RUIH.01.01.01 EP 2 RUIH.08.01.01 EPs 1, 2	Control 9: Establish an AI workforce competency framework (or related document) that defines roles and responsibilities of AI governance personnel using AI minimum qualifications and/or certification. Include ongoing training programs to update personnel on governance concepts such as AI safety and bias mitigation.	AI Governance Roles and Responsibilities, Qualification

^{ss} Excerpt from *AI Governance Playbook. Domain 3: Organizational Resources*. © 2026 by Coalition for Health AI. Used with permission.

	Control 10: Identify when clinicians and staff need to be trained on specific AI solutions prior to implementation; also, determine if certain AI solutions require regular training/competency assessments.	AI Solutions and Staff Training/Competency
--	--	--

AI Governance Playbook. Domain 4.5: Education, Training, and Feedback

Standard/EP	CHAI Baseline Operational Controls ^{***}	CHAI Implementation Guidance (Suggestions Based on Known Practices)
RUAIH.08.01.01 EPs 1, 2	Control 1: Training: Develop a process to ensure all relevant staff receive training on AI systems, including their purpose, limitations, and related information. Reinforce training via recurring briefings and optional seminars for deeper engagement.	Illustrative Example: Piloting to Inform Scaling and Training
RUAIH.09.01.01 EP 3	Control 2: Education: Provide all patients, no later than the date of first service delivery, with a comprehensive Notice of Privacy Practices (NPP), including how protected health information (PHI) may be used by AI systems, in compliance with HIPAA.	HIPAA Notice of Privacy Practices (NPP) Template
RUAIH.09.01.01 EP 1	Control 3: Education: Develop a process for patient transparency and/or consent where appropriate for relevant AI solutions.	Illustrative Example: Patient Intake Packet
RUAIH.07.01.01 EPs 1–4	Control 4: Feedback: Develop a process to document, escalate, and notify relevant parties about AI incidents. Ensure it is clearly communicated that all parties involved in an AI incident share responsibility for reporting any voluntary or mandatory incidents.	Incident Communication
RUAIH.02.01.01 EP 1	Control 5: Feedback: Ensure information included in AI incident communication falls under relevant federal and state laws and protections.	Implementation Guiding Questions on Regulatory Requirements and Mandatory Reporting
RUAIH.07.01.01 EP 2	Control 6: Feedback: Provide whistleblower protections for both internal and external reporting, including anonymity, confidentiality, non-retaliation assurances, and clear disclosure of data retention policies.	Building AI Incident Reporting into Existing Infrastructure

^{***} Excerpt from *AI Governance Playbook. Domain 4.5: Education, Training, and Feedback*. © 2026 by Coalition for Health AI. Used with permission.

Reviewer Report Preparation

Duration: 30 minutes

Objective

To compile, analyze, and organize data the reviewer has collected into a summary report of observations made throughout the review

Organization Participants

- None required, unless specifically requested by the reviewer

Materials Needed

- None

Activities

The reviewer uses this time to enter their observations related to standards compliance and plan for the Exit Conference.

Exit Conference

Duration: 30 minutes

Objective

To provide the Preliminary Certification Report of findings from the reviewer

Organization Participants

- Program executive and individuals (for example, team or committee members) who are responsible for leading the use of health AI across the organization
- Individual(s) who participated in tracer activities
- Others at the discretion of the organization

Materials Needed

- None

Activities

- Review the Preliminary Certification Report, including the *Survey Analysis for Evaluating Risk® SAFER®* Matrix.
- Discuss any standards compliance issues that resulted in Requirements for Improvement (RFIs).
- Allow the organization a final opportunity to question the review findings and provide additional material regarding standards' compliance.
- Mention the post-review clarification process.
- Review required follow-up actions as applicable.

During the Exit Conference or at the close of day, the reviewer will post the Preliminary Certification Report to the organization's *Joint Commission Connect®* extranet site.

The Final Certification Report and certification decision are made by Joint Commission's Central Office within 10 days of the review and will be posted on *Joint Commission Connect*.