AI-Trust™ Certified Organization

Certification Policies, Standards, & Survey Process

Effective March 2026

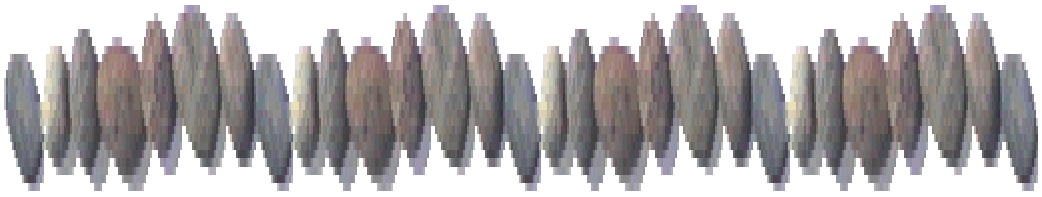

Table of Contents

INTRODUCTION

Healthcare organizations worldwide are rapidly deploying artificial intelligence (AI) across clinical, operational, and administrative workflows. While current oversight initiatives rigorously evaluate traditional quality, safety, and compliance, AI introduces new categories of operational, ethical, and governance risk that are not systematically assessed today – including model governance, data integrity, bias, drift, human override capabilities, and post-deployment monitoring.

The Center for Improvement in Healthcare Quality (CIHQ) and AnalytAIX have partnered to bring forth the healthcare industry's first formal certification program in AI. The overall goal of this certification is to provide assurance to healthcare institutions, providers, patients, and other key stakeholders that your AI programs and systems are AI-Trust™ Certified!

AI-Trust™ Certified is not a descriptor. It is a determination / conclusion that the structures and processes your organization develops will ensure that AI is used in a safe, reliable, and effective manner.

This certification program systematically assesses the key domains of AI trustworthiness:

- AI governance and accountability structures – how oversight of AI is organized (e.g. committees, leadership responsibility).
- Data provenance, privacy, and PHI handling – how data used by AI is sourced, managed, and protected.
- Model lifecycle management and change control – how AI models are developed, validated, updated, and retired.
- Human-in-the-loop safeguards and escalation pathways – how human oversight is implemented and how issues with AI are escalated.
- Transparency, explainability, and disclosure practices – how AI use and limitations are communicated internally and externally.
- Bias detection, drift monitoring, and post-deployment controls – how the AI's performance is monitored for bias or degradation over time and controlled.
- Incident response and continuous oversight mechanisms – how AI-related incidents are handled and how ongoing compliance is maintained.
- Third party AI and vendor governance - how externally developed or hosted AI systems are evaluated, monitored, and contractually governed.
- Research and advanced analytics governance - how AI systems used in research, advanced analytics, and model driven insight generation are governed, documented, and protected.

The certification approach is designed to be globally adaptable across regulated industries. It aligns with emerging AI risk management frameworks and emphasizes compliance with international data protection standards by upholding core principles of data minimization, transparency, lawful basis for processing (consent), purpose limitation, and secure cross-border data handling

Certification assessment methods ensure that all client data remains within the healthcare organization's own cloud environment whenever possible, under robust security and privacy controls, so that no sensitive data leaves the client's domain.

The certification standards contained herein are based on the following:

- National Institute of Standards & Technology's (NIST) "Artificial Intelligence Risk Management Framework"
- Organization for Economic Co-operation and Development (OECD)
- General Data Protection Regulation (GDPR)
- IS International Organization for Standardization O/IEC 42001
- Health Insurance Portability and Accountability Act (HIPAA)
- PDPL

ROLE OF CIHQ

CIHQ is a leading accreditor for hospitals and other healthcare organizations across the United States. CIHQ is the certifier of record and is responsible for:

- Governance and administration of the certification program
- Approval of standards, and certification policies
- Issuance of certifications and final decisions regarding said issuance

ROLE OF ANALYTAIX

AnalytAIX is internationally recognized as a leader in AI-powered analytics solutions for businesses. AnalytAIX delivers AI solutions that integrate fragmented data into actionable insights, support organizations in achieving smarter, faster, and more ethical decisions, and foster knowledge transfer, workforce development, and innovation. AnalytAIX:

- Provides technical expertise in the development of certification standards and the assessment process
- Conducts all technical and operational AI readiness assessments on behalf of the program.

STATEMENT OF SCOPE

AI-Trust™ Certified is an organization-level governance certification evaluating conformity to the AI-Trust™ Standards (AI-1 through AI-15).

Certification evaluates governance structures and operational oversight mechanisms governing the development, deployment, monitoring, and management of artificial intelligence systems.

Certification does not:

- Certify individual AI products or algorithms
- Validate clinical, technical, or operational efficacy
- Constitute regulatory authorization or approval
- Serve as legal compliance determination
- Transfer liability from the certified organization

Certification affirms that, at the time of evaluation, the organization demonstrated governance structures consistent with AI-Trust™ Standards.

In a manner analogous to a licensing authority verifying competency at a point in time, AI-Trust™ Certified attests to governance maturity but does not guarantee future outcomes or assume responsibility for operational performance.

The AI-Trust™ framework aligns with recognized international AI governance principles. Alignment does not constitute certification of compliance under external statutory or regulatory law, regulation, or requirements..

CERTIFICATION POLICIES

ELIGIBILITY REQUIREMENTS

To obtain/maintain certification, an organization must:

- Be in full compliance with CIHQ certification policies
- Be in full compliance with CIHQ certification standards or have developed and implemented an acceptable plan of correction to come into compliance in areas of deficient practice.
- Pay certification fees in a timely manner
- Permit access by AnalytAIX staff to policies, procedures, AI systems, and other sources of information necessary to perform the certification assessment.
- Submit an annual attestation, signed by the organization's Chief Executive Officer, confirming continued adherence to AI-Trust™ Standards.

CIHQ reserves the right to withdraw/deny certification to an organization that does not meet/maintain eligibility requirements.

APPLICATION FOR CERTIFICATION

An organization must submit a formal application to CIHQ requesting certification. The application must be completed and accepted by CIHQ before the certification can occur. Once designated, the organization is responsible for assuring that information contained in the application is current. Organizations must notify CIHQ of any substantive changes to information contained in their application in a timely manner.

BUSINESS ASSOCIATE / CONFIDENTIALITY AGREEMENT
If an organization requires CIHQ and AnalytAIX to sign a business associate agreement / confidentiality agreement for HIPAA or other regulatory compliance, the agreement must be provided to CIHQ at the time the application is filed.

DURATION OF CERTIFICATION AWARD
Certification is awarded to an organization for a maximum of 36 months. Prior to the 36-month expiration, the organization must undergo another full assessment to maintain its status. For initial surveys, the date of certification will be the date that a submitted plan of correction has been accepted by CIHQ to address any identified deficiencies.

RELATIONSHIP BETWEEN CIHQ / ANALYTAIX STAFF & APPLICANT ORGANIZATIONS
CIHQ and AnalytAIX staff may not assess an organization in which the individual has a professional or financial interest. An individual is considered to have a professional or financial interest in an organization under any of the following conditions:

- The individual is currently employed or has been employed within the past five years by the organization
- The individual has an ownership interest in, or receives monies or other compensation from, the organization
- The individual serves on the Board of the organization or in another professional capacity.

CERTIFICATION STANDARDS / REQUIREMENTS
Each certification standard contains one or more requirements. Each requirement is classified under one of the following categories:

- Core – These requirements are designed to establish the minimum structures and processes necessary for an AI trustworthy organization.
- Level I – These requirements represent advanced structures and processes necessary for an AI trustworthy organization.
- Level II – These requirements address optimal structures and processes for an AI trustworthy organization.

CERTIFICATION DECISIONS
Provisional Certification
Provisional certification is granted when an organization meets all Core requirements either at the time of the validation survey or submits / implements an acceptable plan of correction for identified deficiencies within 30 days following the survey.

Full Certification
Full certification is granted when an organization meets all Level I and Level II requirements either at the time of the validation survey or submits / implements an acceptable plan of correction for identified deficiencies within the following timeframes:

- Level I Requirements – within 90 days following survey
- Level II Requirements – within 180 days following survey

SUSPENSION OF CERTIFICATION

Suspension

Certification may be immediately suspended for:

- Failure to report Level 3 or Level 4 severity incidents to CIHQ within 10 calendar days
- Material falsification or misrepresentation
- Systemic governance collapse
- Severe Level 4 incident indicating material risk to patients and/or the care environment

Conditional Suspension

Certification may be conditionally suspended for:

- Failure to submit an annual attestation
- Failure to implement a corrective action plan when required to do so
- Repeated Level 2 incidents indicating systemic weakness
- Non-payment of certification fees

Administrative Non-Payment

Failure to pay certification fees within thirty (30) calendar days of invoice date.

During suspension, the organization must immediately cease representation as an AI-Trust™ Certified Organization and suspend use of the AI-Trust™ mark.

REVOCATION OF CERTIFICATION

Revocation may occur for:

- Deliberate falsification
- Repeated severe governance failure
- Obstruction of review / refusal to allow AnalytAIX staff access to information and/or perform an on-site survey.
- Non-payment certification fees beyond 60 calendar days from invoice date.

FALSIFICATION & MISREPRESENTATION

Honesty and the provision of truthful and accurate information is at the heart of the certification process. Organizations are expected to engage in all activities in an honest and truthful manner. Information presented in any manner, for any reason, at any time must be accurate. If an organization's leadership or staff intentionally misrepresents their compliance to certification standards and/or policies, lies, falsifies documents or is otherwise dishonest or untruthful, CIHQ reserves the right to immediately withdraw/deny certification.

NOTIFYING ORGANIZATIONS OF CHANGES TO CERTIFICATION STANDARDS, REQUIREMENTS, & POLICIES

All changes to certification standards, requirements, and policies will be communicated to organizations in writing. The notification will include the effective date of implementation. In addition, all notifications will be posted on the CIHQ website and permanently archived for review.

CIHQ may from time-to-time issue official interpretation of existing certification standards, requirements, and policies. These interpretations will be posted on the CIHQ website and are accessible to organizations. It is the organization's responsibility to access this information.

Organizations may request official interpretation of an existing certification standard, requirement, or policy. Requests must be made in writing. Information on submitting a written request is available on the CIHQ website. CIHQ will provide a written response to each request within five business days of submittal.

INFORMATION THAT IS PUBLICLY SHARED BY CIHQ

CIHQ may, at its discretion, make the following information available to the public:

- Verification that the organization is certified or is seeking certification
- The organization's current certification status
- The dates of the organization's initial or last assessment
- The expiration date of the organization's current certification

RECORDS RETENTION AND LITIGATION HOLD

Certification records shall be retained for:

- The three (3) year certification term; and
- One (1) year following certification expiration.

If certification is subject to investigation, appeal, regulatory inquiry, or legal dispute, records shall be preserved under litigation hold until final resolution, regardless of standard retention timelines.

RISK FINANCING CONSIDERATIONS (Advisory)

AI-Trust™ Certified does not require organizations to maintain specific insurance coverage as a condition of certification. Organizations are encouraged to evaluate whether appropriate cyber liability, technology errors and omissions, or AI-related risk coverage is maintained consistent with their AI deployment profile.

Insurance coverage is not evaluated as part of certification and does not substitute for governance conformity.

CERTIFICATION FEES

Certification fees are billed annually. The fee is determined by the scope and degree of AI integration into an organization's structures and practices, as well as the scope and complexity of the organization services. Fees are non-refundable and due within 30 days of invoice.

The higher the level of AI integration and scope the more time and resources are necessary to adequately perform the assessment. Hence, fees are adjusted based on this fact. It is anticipated that most assessments will be performed virtually. However, if an on-site survey is required, the organization will be billed for usual and customary travel expenses.

INDEMNIFICATION

By applying, the organization agrees to release from liability and hold harmless CIHQ and AnalytAIX, its commissioners, officers, agents, employees, and member organizations from any and all liability claims arising from its certification designation program, process, policies, and survey activities, including all judgments, settlements, costs, expenses, and reasonable attorneys' fees, unless and until any such judgments, settlements, costs, expenses and attorneys' fees are found by a final judgment of a court of competent jurisdiction to have resulted solely from negligence or wrongdoing on the part of the CIHQ and AnalytAIX.

The organization agrees that in the event of any error or omission in connection with or because of CIHQ and AnalytAIX performance of certification services including, but not limited to, the performance of any assessments, processing of the results of any assessments, and the disclosure of assessment results, liability to the organization for any loss or damage arising therefrom, shall be limited to one year's annual fee.

This limitation of liability shall apply to the fullest extent permitted by law regardless of whether the organization's claim for loss or damage is based upon contract, tort, strict liability, or otherwise, and shall constitute CIHQ and AnalytAIX sole liability to the organization and the organization's exclusive remedy against CIHQ and AnalytAIX in the event of any such error or omission.

CERTIFICATION ASSESSMENT PROCESS

ASSESSMENT PROCESS

The program follows a three-stage readiness and validation model, ensuring organizations progress through preparation, self-evaluation, and external validation:

- Stage 1: Education & Awareness: Prior to the AI Readiness Self-Assessment participating organizations complete a structured AI education and awareness curriculum delivered through AnalytAIX's educational arm. This stage ensures that the organization has a baseline understanding of AI risks and program expectations.
- Stage 2: AI Readiness Self-Assessment: The organization completes a structured self-survey (self-assessment) focused on AI readiness and safety. The organization provides responses to criteria questions and uploads supporting evidence (policies, procedures, operational documents) for review. In addition to the core technical self-assessment, organizations must also include a workforce readiness and change management assessment to enable safe and effective AI adoption.
- Stage 3: Validation Survey: After the self-assessment is completed and reviewed a virtual or on-site validation survey (inspection) is conducted by AnalytAIX's technical reviewers. This serves to verify the self-assessment findings and observe actual practices. Key activities in the validation survey include:
    - Documentation review: The surveyors thoroughly review the policies, procedures, and evidence submitted in the self-assessment to ensure completeness and accuracy.
    - Leadership and staff interviews: Interviews are conducted with organizational leadership and operational staff to assess understanding, verify that stated processes are truly in place, and gauge the culture and oversight practices around AI.
    - Traceability testing: The surveyors perform traceability checks, linking policies to operational practice – for example, taking a stated policy and tracing how it's implemented on the ground with a specific AI system.
    - Verification of controls: Specific checks are done to verify that monitoring tools, escalation pathways, and human oversight controls are functioning as described.

ISSUANCE OF A CERTIFICATION REPORT

Following conclusion of the assessment, a detailed findings and recommendations report authored by AnalytAIX, which outlines strengths observed, any gaps, and recommendations for improvement will be issued. If any gaps are identified that preclude immediate designation, a required action plan will be provided. The organization can address these actions and undergo focused re-evaluation as needed.

APPEAL PROCESS

CIHQ has established an appeals process for organizations wishing to contest a deficiency and/or certification decision.
If an organization wishes to appeal a finding, it must notify CIHQ in writing within 10 business days following receipt of the report. There is no specific format for the appeal. The content must specifically address the following:

- The basis for appealing a deficiency and/or certification decision.
- Submission of evidence to support the appeal

The written request must be submitted to:

Center for Improvement in Healthcare Quality
ATTN: Chief Executive Officer
P.O. Box 1540, Mexia, TX 76667
rcurtis@cihq.org

AnalytAIX staff will review the appeal and forward a recommendation to CIHQ. The decision by CIHQ to accept or deny the appeal is final.

CERTIFICATION STANDARDS

CIHQ Standards & Requirements
AI-1: Establishment of an AI Oversight Structure The organization establishes a structure to oversee the use of AI in its operations and services A. The organization's governing body formally approves an organization-wide AI strategy defining the program's scope, risk tolerance, and expected business value. The organization's AI strategy shall include defined data governance standards addressing data provenance, dataset representativeness, data quality controls, retention policies, data minimization, and cross-border data considerations consistent with applicable law. B. The organization's governing body formally establishes a committee to oversee the use of all AI in its operations and services. This establishment is codified in writing. C. The committee is multi-disciplinary in nature. At a minimum, the committee is comprised of permanent representatives from senior leadership, information management, and risk management. Ad-hoc committee members shall include key stakeholders and end-users of the specific AI program(s) used in the organization. D. An "AI Lead" shall be designated as chair of the oversight committee and shall be appointed by the governing body. This individual shall have the requisite education, training, and/or experience to provide effective leadership of the program. The specific responsibilities of the "AI Lead" shall be codified in writing. E. The committee shall meet at a frequency necessary to effectively oversee the AI program. F. On an at least an annual basis, the committee shall report a summary of its actions to the governing body.

CIHQ Standards & Requirements
AI-2: Compliance to Law & Regulation The organization assures that its use of AI systems complies with law and regulation A. The organization assures that it complies with applicable laws and regulations, including those related to data privacy, copyright and intellectual property. B. The organization shall identify and maintain a documented process for determining which laws, regulations, contractual obligations, and regulatory guidance apply to its AI systems based on use case, geography, data type, and risk profile.

CIHQ Standards & Requirements
AI-3: Adherence to Industry Standards The organization plans, develops, implements, and evaluates its AI structures and processes in accordance with accepted industry standards. A. The organization considers the following industry standards in the use of AI: a. National Institute of Standards & Technology's (NIST) "Artificial Intelligence Risk Management Framework" b. Organization for Economic Co-operation and Development (OECD) c. General Data Protection Regulation d. EU AI Act (EU) 2024/1689 e. IS International Organization for Standardization O/IEC 42001 f. Health Insurance Portability and Accountability Act (HIPAA) g. Personal Data Protection Law (PDPL)

CIHQ Standards & Requirements

AI-4: AI Needs Assessment

The organization assesses its AI needs in relation to its scope of services, operations, and clinical care

A. At least once every three years, the organization conducts a formal assessment of AI needs in all departments and services – including the medical staff, senior leadership, and the governing body.
B. The assessment is designed to identify areas where the use of AI can improve the quality, safety, efficiency, and / or outcomes of care, treatment, and service.
C. The results of the needs assessment are reviewed by the AI Oversight Committee and prioritized for further action. The organization is not expected to act on all needs identified. Rather prioritization is used to identify those specific needs for which action would garner the greatest return on investment.
D. The AI Oversight Committee makes a recommendation to the governing body on the prioritized need(s). The governing body acts upon the recommendations consistent with capital, operational, and labor constraints as well as other appropriate considerations.

CIHQ Standards & Requirements

AI-5: Workforce AI Readiness Assessment

The organization assesses the readiness of its workforce (including the medical staff) to embrace and use AI systems in their job function and attendant duties and responsibilities. Representative sampling sufficient to ensure meaningful participation.

A. The organization uses a written tool to gauge a respondents knowledge and understanding of AI, trust in using AI in their job function, readiness to use AI, and perceived barriers to the use of AI. The organization is encouraged, but not required, to use the AnalytAIX's survey instrument for this purpose.
B. The readiness assessment tool is administered to a statistically valid sampling size of employees, medical staff, and management in each affected department / service.
C. The results of the assessment are aggregated, analyzed, and presented to the AI Committee. The AI Committee recommends or acts on the results of the assessment.
D. The assessment is completed at least once every three years.

CIHQ Standards & Requirements

AI-6: Staff Training in AI

The organization assures that end-users of AI systems are appropriately trained and educated on their use.

A. The organization conducts an education needs assessment at least annually in all departments and services that utilize AI systems.
B. Education and training is provided to end-users of AI systems based on identified needs. Training is provided upon hire, as needed, and at least every three years thereafter.
C. At a minimum, the content of education and training addresses at least the following:
    a. The purpose and use of AI systems in the end-users work environment
    b. How to access the AI systems – including any security requirements
    c. Any limitations or restrictions on the use of AI systems in the performance of duties and responsibilities
    d. End-user education and training shall also address reporting responsibilities for AI incidents, appropriate escalation pathways, and the circumstances under which human review, override, or non-use is required.
D. Education and training of end-users is documented.

CIHQ Standards & Requirements

AI-7: AI Incident Response / Reporting

The organization develops and implements processes to identify, report, and respond to incidents involving the use of AI systems.

A. The organization defines what constitutes an incident involving AI systems. Such incidents include, but are not necessarily limited to:
   a. Compromise of data integrity
   b. Breach of security mechanisms
   c. Breach of patient confidentiality
   d. Ethical concerns
   e. Performance outside intended parameters
   f. Patient safety impact

B. There is a defined reporting pathway for incidents involving AI systems. Reporting does not rely solely on one individual and includes escalation to appropriate leadership and the AI Oversight Committee.

C. The organization establishes a reasonable timeframe for review and response to reported incidents.

D. When appropriate, the organization conducts a documented review to determine cause and corrective action.

E. Corrective actions are implemented and monitored. Incidents associated with Clinical High Impact Risk systems shall be escalated to the AI Oversight Committee within a defined timeframe.

F. The organization shall maintain an AI Incident Response Protocol that defines incident identification, containment, escalation, investigation, mitigation, communication, remediation, and lessons learned activities.

G. The organization shall classify AI incidents using a four-level incident severity framework as follows:
   a. Level 1 – Minor AI Incident (an incident that results in minimal adverse impact and no patient harm)
   b. Level 2 – Moderate AI Incident (an incident that results in measurable negative operational impact, potential adverse patient impact, or significant control failure)
   c. Level 3 – Severe AI Incident (an incident resulting in confirmed patient harm, significant data breach, systemic bias, regulatory exposure, or materially adverse safety event)
   d. Level 4 – Critical AI Incident (an incident that results in catastrophic or widespread harm, systemic governance failure, large-scale data compromise, mission-critical operational collapse, or multi-jurisdictional impact requiring executive-level intervention)

   The organization is encouraged – but not required – to use the AnalytAIX "AI Incident Classification Framework" tool for this purpose.

H. Certified organizations must report Level 3 and Level 4 incidents to CIHQ within ten (10) calendar days of identification. Level 1 and Level 2 incidents are managed internally and are not subject to immediate reporting but must be documented and included in an annual attestation in aggregate form.
   Each Level 3 or Level 4 report must include:
   a. Incident description
   b. Severity classification
   c. Systems affected
   d. Immediate mitigation actions
   e. Corrective action plan with milestones
   f. Current operational status of the affected system

I. A Level 4 incident requires:
   - Immediate executive notification
   - Formal review initiation within five (5) business days of identification
   - Containment and mitigation actions
   - Consideration of system suspension
   - CIHQ notification within 10 calendar days

J. For Level 3 or Level 4 incidents, the organization shall conduct a documented root cause analysis and incorporate lessons learned into governance updates, process improvement, retraining, technical safeguards, or system retirement decisions as appropriate.

CIHQ Standards & Requirements

AI-8: Use of AI in Patient Care

The organization assures that AI systems are used safely and appropriately in the provision of patient care. Oversight requirements for AI used in patient care shall be proportional to the system's assigned risk classification

A. The organization develops and implements policies addressing the appropriate use of AI systems in the provision of patient care. This includes identifying specific situations where the use of AI is both permitted and prohibited. End users are educated on these policies.
B. The use of non-approved AI systems is prohibited
C. Prior to deployment, the organization assures that AI systems used in patient care have been thoroughly vetted and validated – including assuring that AI content is derived only from authoritative sources and evidence-based standards of care.
D. The use of AI is disclosed to patients when used in diagnosis, treatment, and care planning consistent with applicable law and organizational policy. This includes a description of what and how AI was used.
E. Clinicians remain ultimately responsible for clinical decision making. The use of AI does not replace clinician judgment. Clinicians review (and if necessary correct) AI generated information and any corresponding entries into a patient's medical record.
F. The use of AI does not replace human interaction between clinicians and patients
G. The organization shall document the boundaries of human oversight for AI systems used in patient care, including when human review is mandatory, when override is permitted or required, and when AI output shall not be used without additional validation.
H. AI systems used in patient care are HIPAA compliant and address other privacy regulations. This includes data encryption, limited access controls, and de-identification of patient records
I. The organization shall document known system limitations relevant to patient care use and make such limitations available to appropriate end-users.
J. For patient care AI systems that materially influence decisions, the organization shall maintain a mechanism for stakeholder inquiry, challenge, escalation, or review consistent with applicable law and organizational policy.
K. There is a safety mechanism ("kill switch") designed to immediately stop, disable, or contain an AI system if it behaves dangerously, unpredictably, or attempts to violate established safety boundaries

CIHQ Standards & Requirements

AI-9: Onboarding & Deployment of AI Systems & Programs

The organization assures that AI systems are appropriately evaluated prior to use.

A. The organization establishes and implements a process to evaluate the use of AI systems prior to deployment.
B. The evaluation is performed by a multi-disciplinary body including representative from Information Management, Risk Management, Leadership, and affected end-users.
C. The evaluation addresses – at a minimum – the following:
    a. Transparency and explainability
    b. Description of end-to-end data lineage (the comprehensive, visual tracking of data's entire journey from its origin (source system) to its destination (reports, dashboards, applications, etc.)
    c. Fairness and equity - including how bias is recognized and managed. This includes defining the minimum acceptable thresholds for error rate, drift tolerance, and retraining triggers
    d. Reliability – including how drift is recognized and managed
    e. Privacy and data protection – including end-to-end encryption, access control, and protection of proprietary and/or patient health information
    f. Ethical considerations
    g. Accountability and human responsibility including adequacy of "human in the loop" features (human intelligence is integrated into the AI system / program to improve accuracy, safety, and decision-making
    h. Security – including mechanisms to protect against cyberattack, and unauthorized access
    i. Safety – including measures that mitigate an unsafe outcome
    j. Cost and return on investment
    k. The results of the evaluation and subsequent recommendation are presented to the AI oversight committee for approval.
D. The organization shall apply an AI Risk Classification Framework tool and associated AI Risk Register to ensure proportional oversight based on risk to each AI system in its inventory. There are three risk classifications
    a. Level 1 = Foundational Risk
    b. Level 2 = Operational Risk
    c. Level 3 – Clinical High Impact Risk

    The organization is encouraged – but not required – to use the AnalytAIX "Governance & Risk Classification" tool for this purpose.

    AI systems classified as Level 2 or Level 3 shall be documented in the organization's AI Risk Register.
E. If material disparities or unacceptable performance differentials are detected across defined population groups, deployment shall require documented review and approval by the AI Oversight Committee prior to production use.
F. The AI system / program is piloted prior to full deployment. Any issues or actions needed are addressed / resolved prior to full deployment.
G. For internally developed or materially customized AI systems, the organization maintains a documented model development checklist that includes training dataset review, validation metrics, defined performance thresholds, fairness indicators, and approval signatures prior to deployment.'
H. For externally developed AI systems, the organization shall obtain and review vendor documentation regarding model limitations, validation methodology, data sources where available, and known bias considerations.
I. The organization maintains version control documentation for each AI system or model iteration, including change logs, update rationale, validation results, and defined rollback procedures in the event of performance degradation or safety concern.

CIHQ Standards & Requirements
AI-10: Inventory of AI Systems The organization establishes and maintains a current and accurate inventory of AI systems used in its operations and services. A. The organization determines the specific AI systems used in each department and setting. For each system/program, the inventory identifies: a. Name of the system / program b. Creator / maker of the program c. Departments / settings where the system / program is used d. The purpose and scope for which the system / program is used e. The operational characteristics of the system / program f. The end-users of the system / program B. A brief written description of the system / program intended purpose, limitations, human oversight requirements, and known constraints shall be maintained and accessible to relevant stakeholders. C. The organization has a defined and implemented process to review its inventory of AI systems on at least an annual basis to assure it remains current and accurate.

CIHQ Standards & Requirements

AI-11 – Ongoing Monitoring of AI Systems

The organization develops and implements processes to monitor the ongoing trustworthiness of its AI systems

A. The organization establishes a scheduled review frequency of each AI system and program. The frequency of review is determined by:
   a. The risk to patient safety and quality of care
   b. The impact on operational effectiveness
   c. History of any adverse events
   d. Historical changes to standards or regulations
   e. The likelihood of bias or drift issues

B. As determined by AI-9 / Requirement D, Level 3 systems used in patient care shall undergo formal performance review at least quarterly. The review is conducted by a team consisting of Information Management, Risk Management, end-users, and other key stakeholders.

C. As determined by AI-9 / Requirement D, Level 1 and Level 2 systems, shall undergo formal performance review at least annually and semi annually respectively. The review is conducted by a team consisting of Information Management, Risk Management, end-users, and other key stakeholders.

D. The review is an assessment of the following:
   a. Use of the system / program by affected departments / services
   b. Satisfaction with the system / program by end-users
   c. Continued adequacy of encryption, access control, and protection of confidential information
   d. Continued adequacy of "human in the loop" features
   e. Presence of bias and/or drift – including structured fairness reviews on model inputs and outputs conducted at least annually and following any major model modification
   f. Incidence of adverse events
   g. Incidence of ethical issues / concerns
   h. Operational effectiveness

E. Ongoing monitoring shall include defined performance metrics measured against documented baselines, with documented thresholds for acceptable variance, alert triggers, escalation pathways, and required review actions.
   Monitoring shall address statistical drift, operational drift, contextual drift, and unintended behavioral change to the extent applicable to the AI system.
   Where protected or risk-sensitive attributes are relevant, the organization shall monitor bias thresholds across such attributes in a manner proportionate to system purpose, data availability, and applicable law.
   Corrective actions, retraining events, version changes, temporary restrictions, suspensions, and rollback decisions arising from monitoring activities shall be documented and maintained under version control.

F. The results of the assessment along with any recommendations are presented to the AI Oversight Committee. The AI Oversight Committee acts on said recommendations. Documentation of review findings, decisions made, corrective actions initiated, and follow-up status shall be maintained.

CIHQ Standards & Requirements
AI-12: Retirement of AI Systems The organization develops and implements a process to remove AI systems when no longer in use. A. The AI oversight committee determines when an AI system or program will be removed from use. The determination is done in consultation with end-users of the system / program. B. A criteria-based approach is used to determine the removal of an AI system program. The criteria include, but are not necessarily limited to: a. Evidence that the AI system has caused harm or performed outside of its intended parameters b. End users no longer use the AI systems c. The vendor no longer supports the AI program / system d. The vendor is unable to adequately address operational issues such a drift, bias, encryption performance, confidentiality, etc. e. There is no longer an acceptable cost / benefit equation f. The potential impact on the organization g. The availability of alternate approaches to meet the organization's needs C. The organization communicates the intent to remove the AI system / program to key stakeholders and end-users. A removal date is determined and communicated D. The organization assures that the AI system / program has been successfully removed. E. The organization monitors affected processes following removal of an AI system / program to identify and address any unforeseen circumstances.

CIHQ Standards & Requirements
AI-13: Performance Improvement The organization incorporates the use of AI into its quality assessment / performance improvement (QAPI) program. *Note: AI-13 is intended to address organizational quality assessment and performance improvement and does not replace the technical monitoring, drift management, and model performance oversight requirements set forth in AI-11.* A. The organization establishes, implements, and maintains an ongoing performance monitoring and improvement program to meet the AI needs of the organization B. The organization identifies at least one key performance indicator from each of the following areas: a. Clinical and diagnostic accuracy b. Operational efficiency c. Patient and clinician impact d. Safety, ethics, and compliance C. Performance indicators are displayed in a dashboard format with acceptable levels or performance and alert thresholds D. The organization collects, aggregates, and analyzes data on each indicator at a determined frequency. The results of data analysis and subsequent recommendations (if any) are reported to the AI Oversight Committee. The committee acts on the recommendations On at least an annual basis, the AI Oversight Committee submits a report on its performance monitoring of its AI systems / programs to the organization's quality improvement program and to the governing body.

CIHQ Standards & Requirements

AI-14: Third Party AI and Vendor Governance

The organization establishes and implements structured oversight of third-party AI systems and vendors.

A. The organization conducts risk assessments and transparency reviews for third party AI systems prior to adoption, deployment, or material expansion of use.
B. The organization requires vendors to provide documentation, as available and appropriate, to the use case and risk level, including but not limited to the following:
    a. Training data sources or data provenance descriptions
    b. Validation methodology and performance information
    c. Known limitations and intended use constraints
    d. Bias testing results or fairness controls where available
    e. Security controls and hosting arrangements
    f. Regulatory, privacy, and compliance statements relevant to the intended use
    g. The organization includes contractual or procurement controls, as appropriate, addressing the following:
    h. Audit rights or review rights proportionate to risk
    i. Breach or security incident notification obligations
    j. Ongoing performance reporting or cooperation in monitoring activities
C. Vendor cooperation in corrective action, investigation, mitigation, or system restriction occurs where necessary.
D. Change notification for material model, functionality, data source, or hosting changes occurs where applicable.
E. High-risk third-party AI systems shall be subject to enhanced monitoring and, where appropriate, independent review.
F. Third party AI system onboarding, monitoring, and retirement shall align with the organization's AI governance and lifecycle controls.

CIHQ Standards & Requirements

AI-15: AI in Research and Advanced Analytics Governance

The organization establishes governance structures for the use of AI systems in research, quality improvement analytics, advanced data analytics, and model-driven insight generation activities.

A. AI systems used for research or advanced analytics are subject to documented review processes prior to implementation, with oversight proportionate to data sensitivity, intended use, and risk.
B. Where applicable, Institutional Review Board approval or other required internal review and approval is obtained for research involving human subjects or other regulated activity.
C. The organization ensures that research and analytics related AI systems:
    a. Utilize data that is appropriately de-identified, anonymized, or otherwise lawfully processed
    b. Comply with applicable privacy, confidentiality, and data protection requirements
    c. Maintain documentation sufficient to support reproducibility, traceability, and review of model development and analytical methods
    d. Include safeguards against bias, inappropriate inferencing, and use beyond authorized scope
    e. Do not repurpose clinical or operational data beyond authorized scope without appropriate review and approval
D. Results derived from AI-enabled research or advanced analytics are transparently documented and subject to governance oversight before being used to inform policy, operations, or care where applicable.
E. The AI Oversight Committee receives periodic updates regarding significant AI research or advanced analytics initiatives and associated risk assessments.

--- END ---

Glossary

Adverse Events
An event where the development, use, or malfunction of one or more AI systems directly or indirectly results in harm. This harm can include injury or health issues, disruption of critical infrastructure, violations of human rights, and damage to property or the environment.

AI System
Refers broadly to an artificial intelligence capability, tool, model, application, platform, service, workflow component, or other technology enabled function used by the organization. For purposes of these standards, the term AI system includes what some organizations may separately refer to as systems, programs, applications, models, tools, platforms, or similar terminology.

AI Registry
An AI registry is a centralized, organized inventory of all artificial intelligence systems, models, and agents used within an organization. It acts as a comprehensive "phone book" or catalog for tracking AI projects, enabling governance, risk management, and visibility into who owns and uses AI systems

Artificial Intelligence (AI)
The application of computer systems able to perform tasks or produce output normally requiring human intelligence, especially by applying machine learning techniques to large collections of data.

Bias
AI bias is when an artificial intelligence system produces systematic, unfair outcomes that favor or disadvantage certain groups, often by reflecting and amplifying human prejudices or historical inequalities present in its training data.

Confidentiality of Information
AI confidentiality of information is the practice of ensuring that sensitive data—including user prompts, PII, and intellectual property - is protected from unauthorized access, leakage, or unintended use for training throughout an AI model's lifecycle. It involves securing data in transit, at rest, and while in use via technical, legal, and operational safeguards.

Data
AI data refers to the vast datasets used to train, test, and operate artificial intelligence systems, enabling them to learn patterns, make predictions, and generate insights, essentially acting as the "building blocks" for AI to mimic human intelligence, from recognizing images (computer vision) to understanding language (NLP) and automating complex analysis.

Data Integrity
Refers to the accuracy, consistency, and reliability of data throughout its entire lifecycle—from creation and storage to processing and transmission. It ensures that data remains unaltered by unauthorized, accidental, or malicious changes, making it a critical component of information security and operational quality.

Drift
AI drift, or model drift, is the gradual decline in an AI model's accuracy and performance over time because the real-world data it encounters changes from the data it was trained on, making its initial assumptions outdated and leading to less reliable predictions.

Encryption
Encryption is the process of converting information (plaintext) into an unreadable, scrambled format (ciphertext) using algorithms and keys to ensure data confidentiality, integrity, and authenticity. It secures data both at rest (in storage) and in transit (over networks). Only authorized parties with the correct decryption key can revert the data to its original, readable form.

Ethics
AI ethics is a field of moral principles guiding the responsible design, development, and use of artificial intelligence to ensure it benefits humanity while minimizing harm, focusing on fairness, transparency, accountability, privacy, safety, and alignment with human values to prevent bias, misuse, and negative societal impacts.

Explainability
The ability to understand why an AI model made a specific decision or prediction, moving beyond "black box" results to provide transparent, understandable justifications for its behavior, which builds trust, ensures fairness, helps debug models, and allows for human oversight, especially in high-stakes areas like healthcare or finance. It involves techniques that reveal the logic, factors, and data influencing an outcome, making complex algorithms interpretable for users and stakeholders.

Kill Switch
An AI kill switch is a safety mechanism designed to instantly disable, pause, or contain an artificial intelligence system if it behaves unexpectedly, dangerously, or outside of its intended parameters

Patient Health Information
Patient Health Information (PHI)—or Protected Health Information—is any identifiable, recorded information relating to a person's past, present, or future physical/mental health, provision of care, or payment, created or maintained by a covered entity.

Reliability
The ability of an AI system to consistently deliver accurate, expected, and safe results over time and under specific, varied conditions. It ensures the system functions as designed without failure, forming a foundation for user trust, safety, and operational performance.

Transparency
The practice of making artificial intelligence systems' inner workings, decisions, and data usage understandable, traceable, and clear to users and stakeholders, acting like a "window" into the "black box" to build trust, ensure fairness, and enable accountability for how these systems operate and impact people. It involves being open about an AI's purpose, its training data, its algorithms, and the logic behind its outputs.