Healthcare AI Governance Standard (HAIGS) 2026

Institute for AI Governance in Healthcare (IAIGH)

INSTITUTE FOR AI GOVERNANCE IN HEALTHCARE (IAIGH)

GOVERNANCE FOR INNOVATION, SAFETY, AND TRUST

Visit AiHealthcareGovernance.org for more information

ISBN:

Contents

Foreword

The Institute for AI Governance in Healthcare (IAIGH) is dedicated to the promotion and implementation of comprehensive governance practices in the deployment and use of AI in healthcare. This standard is developed to guide healthcare organizations in integrating AI technologies responsibly, prioritizing governance principles such as patient safety, privacy, trust, regulatory compliance, fairness, scalability, adaptability, and ethics. It aligns with international guidelines such as the WHO Guidance on Ethics & Governance of AI for Health and best practices from healthcare, technology, and regulatory sectors. This standard is adaptable to institutions of all sizes, allowing governance practices to be tailored to each organization's capacity while ensuring robust compliance across diverse healthcare settings. This standard is regionally adaptable and can be harmonized with national regulatory frameworks.

Introduction

0.1 General

This standard establishes requirements for a quality management system covering the deployment and maintenance of AI systems in patient care. It is intended for institutions directly responsible for patient outcomes, including hospitals, clinics, imaging centers, laboratories, teleradiology practices, and other organizations. The standard also serves healthcare providers, regulatory bodies, and other stakeholders involved in the lifecycle of AI systems in medical applications, and its requirements may be adopted by suppliers or external parties offering products to these organizations.

Several jurisdictions have regulatory requirements for the application of quality management systems by organizations with various roles in the supply chain for AI systems in healthcare. Consequently, this standard expects that the organization:

- Identifies its role(s) under applicable regulatory requirements.
- Identifies the regulatory requirements that apply to its activities under these roles.
- Incorporates these applicable regulatory requirements within its quality management system.

0.2 Clarification of Concepts

In this standard, the following terms or phrases are used in the context described below.

- When a requirement is qualified by the phrase "as appropriate", it is deemed to be appropriate unless the organization can justify otherwise.
- When the term "risk" is used, it pertains to safety or performance requirements of the AI system or meeting applicable regulatory requirements.
- When a requirement is required to be "documented", it is also required to be established, implemented, and maintained.

0.3 Process Approach

This standard is based on a process approach to quality management. Any activity that receives input and produces an output can be considered as a process. For an organization to function effectively, it needs to identify and manage numerous processes which may be linked directly or indirectly to each other.

When used within a quality management system, such an approach emphasizes the importance of:

- Understanding and meeting regulatory requirements.
- Considering processes in terms of risks and added value to the end user.
- Obtaining objective results of process performance and effectiveness.
- Continuous improvement of processes based on objective measurement.

0.4 Compatibility with Other Standards

While this standard is self-contained, it also facilitates alignment with relevant regulatory requirements for quality management systems in organizations integrating AI systems into patient care. HAIGS complements existing AI standards and regulatory guidance by offering a specialized healthcare governance layer that supports comprehensive and cohesive compliance. Its balanced approach merges practicality with depth, enabling healthcare institutions of any size or type to build robust governance structures within their available resources.

0.5 Glossary

- **AI System**: An artificial intelligence-based system, software, hardware, application, tool, or utility used in healthcare, including machine learning algorithms, decision support systems, and autonomous devices.

- **Artificial intelligence**: a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to

perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action.

Accountability: The responsibility of stakeholders to ensure that AI systems are deployed and used in compliance with this governance standard, including safety, privacy, and ethics.

- **Adaptability**: The ability of governance frameworks and AI systems to evolve and respond to new technological advancements, regulatory changes, and unforeseen governance challenges.
- **Bias Mitigation**: The process of identifying, addressing, and minimizing biases in AI systems to ensure equitable treatment of all patient groups.
- **Compliance**: Adherence to all applicable healthcare regulations, this governance standard, and legal requirements related to the deployment and use of AI systems.
- **Continuous Improvement:** The process of regularly reviewing and updating governance practices, policies, and AI system performance to reflect advancements in technology, research, and stakeholder feedback.
- **Data Representation**: Ensuring that datasets used to train AI systems are diverse and representative of the population they serve, preventing biased outcomes.
- **Fairness**: The commitment to ensuring that AI systems do not exacerbate health disparities and contribute to reducing inequities in healthcare. Fair and consistent outcomes audits and assessments are used to monitor and address these concerns.
- **Fair and consistent outcomes audit**: A structured process of reviewing AI systems to ensure they do not disproportionately affect any population group and that they promote fairness and consistent outcomes across patient demographics.
- **Ethics**: A set of principles guiding the responsible development and deployment of AI systems, prioritizing patient well-being, fairness, transparency, and accountability.
- **Governance**: The framework of policies, procedures, and oversight that ensures AI systems are implemented and used in accordance with safety, privacy, responsible use, and regulatory standards.
- **Incident Reporting**: A system for logging, reviewing, and resolving any governance-related incidents, such as breaches of safety, privacy, or responsible use standards, that occur during the use of AI systems.
- **Institutional Capacity**: The ability of a healthcare organization to allocate resources, expertise, and infrastructure to implement and maintain AI governance practices. Governance approaches are tailored to match each organization's size and capacity.
- **Outcome Monitoring**: The process of regularly reviewing the results of AI system outputs to ensure they align with governance principles, including safety, fairness, and regulatory compliance.
- **Patient Participation**: The involvement of patients in decisions about their care when AI systems are used, fostering shared decision-making and transparency in AI-related healthcare decisions.
- **Privacy**: The protection of patient data and information from unauthorized access, breaches, or misuse in compliance with applicable laws, such as HIPAA.
- **Risk Management**: A process for identifying, assessing, and mitigating risks associated with AI systems, including responsible use, safety, privacy, and compliance risks.

- **Scalability**: The ability of AI governance practices to be expanded or contracted based on an organization's size, capacity, and resources, ensuring that organizations of varying sizes can implement this governance standard effectively.
- **Stakeholder Engagement**: The process of involving key stakeholders, including patients, healthcare providers, and regulatory bodies, in the development, deployment, and monitoring of AI systems to ensure governance compliance and trust.
- **Transparency**: Openness in how AI systems function, make decisions, and are used in patient care. Transparency also involves clear communication with patients and other stakeholders about the system's capabilities, limitations, and governance practices.

1 Scope

This standard defines the governance requirements for the deployment and maintenance of AI systems in healthcare. It establishes a common framework for AI governance practices, focusing on transparency, accountability, patient safety, privacy, security, fairness, scalability, regulatory compliance, and adaptability. This standard is designed to be scalable and applicable to any healthcare organization, regardless of size or available resources.

2 Normative References

The following documents are indispensable for the application of this standard. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies:

- **WHO Guidance on Ethics & Governance of AI for Health**
  Establishes ethical principles and governance practices for implementing AI systems in healthcare.
- **HIPAA (Health Insurance Portability and Accountability Act)**
  Ensures compliance with privacy and security requirements for patient data within U.S. healthcare organizations.
- **ISO/IEC 42005** (Artificial Intelligence Impact Assessment) (Applicable where relevant)
  Provides a structured method for organizations to evaluate the potential consequences of their AI systems.
- **ISO/IEC 42001:2023** (Artificial Intelligence Management System) (Applicable where relevant)
  A robust cross-industry AI governance framework, complemented by HAIGS's healthcare-specific focus on patient safety, fairness, scalability, and practical implementation guidance.
- **ISO 31000:2018** (Risk Management – Guidelines) (Applicable where relevant)
  Offers a widely recognized framework for risk management, but organizations may adopt equivalent methodologies to achieve similar outcomes.

- **NIST AI Risk Management Framework** (Applicable where relevant)
  An alternative to ISO 31000, providing specific methodologies for managing risks in AI implementation.
- **ISO/IEC TR 24027:2021** (Bias in AI Systems and AI-Aided Decision Making) (Applicable where relevant)
  Provides structured guidance for mitigating and auditing bias, but organizations may use other tools or frameworks to address fairness in AI systems.
- **ISO 27001:2022** (Information Security Management Systems) (Applicable where relevant)
  Provides a comprehensive framework for data security governance; organizations may use equivalent national or internal standards to meet similar objectives.
- **ISO 9001:2015** (Quality Management Systems – Requirements) (Applicable where relevant)
  Provides a scalable quality management system framework, particularly useful for larger organizations.
- **ISO 22320:2018** (Emergency Management – Guidelines for Incident Management) (Applicable where relevant)
  Offers guidance for structuring incident reporting and response processes; other frameworks may suffice for scalable adoption.
- **EU AI Act** (Applicable where relevant)
  Relevant for organizations operating in or engaging with the EU regulatory framework; optional for non-EU contexts.
- **ISO/IEC 22989:2022** (Artificial Intelligence – Concepts and Terminology) (Applicable where relevant)
  Provides standardized terminology and concepts related to AI, useful for ensuring consistent understanding across governance frameworks.

See Appendix C – Normative References

3 Terms and Definitions

3.1 AI System - An artificial intelligence-based system used in healthcare, including machine learning algorithms, decision support systems, and autonomous devices.

3.2 Patient Safety - The prevention of harm to patients during the use of AI systems in healthcare.

3.3 Transparency - The clarity and openness regarding how AI systems function, make decisions, and are used in patient care.

3.4 Accountability - The responsibility of stakeholders to ensure the responsible deployment and use of AI systems.

3.5 Privacy -The protection of patient data and information from unauthorized access and breaches.

3.6 Fairness - The equitable treatment of all patient groups by AI systems, avoiding biases and discrimination.

3.7 Informed Consent - The process of ensuring that patients understand and agree to the use of AI systems in their care.

3.8 Fairness - The commitment to ensuring that AI systems do not exacerbate existing health disparities and actively contribute to reducing inequities in healthcare.

4 General Requirements

4.1 AI Governance

4.1.1 Establish Oversight - Develop a governance framework to oversee the use of AI systems. This includes creating a governance committee with representatives from various disciplines (e.g., legal experts, medical professionals, regulatory experts, and ethicists).

4.1.2 Define Roles and Responsibilities - The organization shall clearly define and document roles and responsibilities for AI oversight within the healthcare organization. This ensures accountability at all levels, from governance committees to operational staff, for the successful implementation and maintenance of AI governance practices.

4.1.2.1 Governance Roles

a) AI Governance Committee - The AI Governance Committee is responsible for overseeing the organization's compliance with this standard. This committee should include representatives from various disciplines (e.g., legal, medical, responsible use, regulatory) to ensure all aspects of governance are considered.

Responsibilities:

- Establish and maintain governance policies and procedures for AI systems.
- Ensure alignment with safety, privacy, fairness, and regulatory requirements.
- Regularly review governance practices, including audits and risk management outcomes.
- Approve any significant updates to AI systems or governance policies.

b) AI Governance Officer (or Compliance Officer) - The AI Governance Officer is responsible for the day-to-day oversight of AI systems and governance practices. This individual ensures that AI system implementations adhere to the governance framework.

Responsibilities:

- Implement governance policies and procedures as outlined by the AI Governance Committee.
- Conduct internal audits to ensure compliance with the governance standard.
- Manage incident reporting and follow up on corrective actions.
- Monitor AI system performance, ensuring it meets safety, privacy, and responsible use guidelines.
- Establish safeguards to detect and mitigate potential inaccuracies, such as AI hallucinations, and monitor for performance degradation, particularly in critical clinical settings. Corrective actions shall be taken when system accuracy, reliability, or clinical efficacy falls below defined acceptable thresholds.
- Liaise with external auditors for required periodic compliance validation.

c) Risk Owners - Risk Owners are responsible for identifying, managing, and mitigating risks related to AI systems. They are accountable for specific risks identified in the risk assessment process and must ensure that mitigation strategies are effectively implemented.

Responsibilities:

- Monitor assigned risks related to AI systems, including safety, privacy, and bias.
- Implement risk mitigation strategies and regularly report risk status to the AI Governance Officer.
- Ensure that risk management activities are documented and updated in risk registers.
- Collaborate with departments (e.g., IT, clinical operations) to address and mitigate risks.

d) IT/AI System Administrators - IT/AI System Administrators are responsible for the technical deployment, maintenance, troubleshooting and monitoring of AI systems, ensuring that they function in compliance with governance requirements.

Responsibilities:

- Ensure AI systems are deployed and configured according to governance guidelines (e.g., data security, privacy).
- Perform regular system updates and vulnerability assessments.
- Work with AI Governance Officers to audit AI systems for compliance and performance.
- Support fair and consistent outcomes audits by ensuring systems are trained on representative data and tested for bias.

e) Clinical Staff and AI Users - Clinical staff and other users of AI systems are responsible for ensuring that they use AI tools responsibly and in compliance with established governance practices. They are also critical for identifying any issues that arise during the practical use of AI systems.

Responsibilities:

- Use AI systems in accordance with training, safety, and privacy guidelines.
- Report any anomalies or incidents involving AI systems to the AI Governance Officer.
- Provide feedback on AI system performance, including patient safety and fair and consistent output considerations.
- Participate in training and continuous education on AI governance best practices.

4.1.2.2 Role Documentation

The organization shall document all roles and responsibilities related to AI governance in a clear and accessible manner. Each individual with AI governance responsibilities should have documented duties, expectations, and reporting lines.

4.1.3 Governance Policies and Procedures - Develop and implement policies and procedures that promote responsible governance in the deployment and use of AI systems, addressing safety, privacy, scalability, and ethics.

4.2 Scalability and Adaptability

4.2.1 Definition of Organizational Size - For the purposes of this standard, organizations are classified as follows:

	Smaller Organizations Healthcare organizations with limited resources, typically defined by one or more of the following criteria:	**Larger Organizations** Healthcare organizations with more substantial resources and operations, typically defined by one or more of the following criteria:
Workforce Size	Fewer than 100 full-time employees (FTEs)	More than 100 full-time employees (FTEs)
Budget and Revenue Profile	Limited budget for AI governance and technology (< $10M in annual revenue)	Significant budget allocation for AI governance and technology (> $10M in annual revenue)
AI Adoption Profile	Use of fewer than 5 AI systems across all operational areas	Use of more than 5 AI systems across multiple departments or regions

Enterprise Profile	An enterprise with up to two locations in a small geographic area.	An organization operating across multiple locations with more than two sites or dispersed over a wide geographic area.

Compare your organization's metrics in each row, then classify it according to the column in which your organization matches the majority of criteria. In the event of a tie, prioritize the metric with the greatest operational impact, typically workforce size or budget.

4.2.2 Scalable Governance - The organization shall implement governance practices scalable to its size and available resources, ensuring effective and appropriate governance implementation. Smaller organizations should adopt streamlined processes that match their capacity; however, "streamlined" does not mean inadequate. Even in simplified forms, the governance measures must be robust enough to ensure compliance with the Healthcare AI Governance Standard. Larger organizations should employ more comprehensive systems aligned with their broader resources. Regardless of size, all organizations are expected to leverage their full potential for governance and meet the Standard's requirements.

4.2.3 Adaptable Framework - The organization shall implement an AI governance framework that is adaptable to changes in AI technologies and evolving regulatory landscapes. This framework shall ensure the organization remains vigilant and responsive to emerging responsible use, technical, safety, and fairness risks as AI continues to rapidly evolve. It shall facilitate continuous improvement, ensuring that AI systems remain compliant with the latest regulations, standards, and best practices. Regular performance evaluations shall be conducted to maintain accuracy, reliability, efficacy, and equitable outcomes over time, with corrective actions triggered when performance, safety, compliance, or fainess is compromised.

4.3 Risk Management

4.3.1 Identify Risks - The organization shall implement a structured risk management process that includes:

a) Defining thresholds for acceptable levels of risk, risk assessment tools and techniques related to risk estimation, risk evaluation, risk control, evaluation of overall residual risk, and risk management review.

b) Conducting risk assessments at AI system onboarding, at least annually, or when significant changes to AI systems or external conditions occur. Any modification, retraining, or update to an AI system shall trigger a governance review proportional to the change impact.
c) Assigning risk owners to specific AI systems to ensure accountability for risk estimation, risk evaluation, risk control, evaluation of overall residual risk, and risk management review.

d) Assessing risks based on the potential impact on patient safety, privacy, and regulatory compliance, using a risk matrix to evaluate likelihood, severity and detectability including the context of level of autonomy of AI systems.
e) Documenting rationale and objective evidence of all identified risks, assessments, and mitigation strategies.
f) Identification of risks related to AI-generated outputs, including the potential for inaccurate, fabricated, or misleading outputs (commonly referred to as "hallucinations"). The organization must implement strategies to detect, mitigate, and prevent risks in a timely manner, especially in clinical decision-making environments. The detection of critical risks should occur as soon as possible after they arise, with mitigation and preventive actions taken promptly to minimize impact on patient safety and clinical workflows.

4.3.2 Mitigation Strategies – The organization shall:

a) Develop and implement strategies/controls to mitigate identified risks.
b) Establish post-deployment safeguards, validation protocols, and regular review processes to monitor and address potential risks associated with the use of third-party AI systems. These strategies shall include mechanisms for detecting, mitigating, and responding to inaccuracies, such as AI hallucinations or performance degradation over time, within the organization's operational context. The organization shall regularly evaluate the system's accuracy, reliability, and clinical efficacy, and take corrective actions when performance falls below acceptable thresholds.

4.3.3 Documentation and Reporting - Maintain detailed documentation of risk management activities and regularly report to top management on the effectiveness of risk mitigation measures.

4.4 Continuous Improvement

4.4.1 Regular Reviews - Regularly review and update processes in the context of responsible use practices and guidelines based on new research, technological advancements, and feedback from stakeholders.

4.4.2 Stakeholder Engagement - Identify and engage with relevant stakeholders, including patients, healthcare providers, and regulatory bodies, to gather feedback and improve responsible use practices.

4.4.3 Training and Education - Provide ongoing training and education to staff on responsible AI practices and emerging ethical issues. Continuous learning and improvement in governance practices are crucial to ensuring that AI technologies benefit all stakeholders in healthcare, regardless of the institution's size or resources.

4.5 Fair and Consistent Outcomes Audits and Governance

4.5.1 Purpose of Fair and Consistent Outcomes Audits - The organization shall conduct regular fair and consistent outcomes audits scaled to the institution's size to ensure AI systems do not exacerbate existing health disparities and actively contribute to reducing inequities in healthcare. AI inequities in healthcare occur when artificial intelligence systems, due to biases in data, algorithms, deployment practices, or erroneous conclusions drawn by machine learning models, perpetuate or amplify disparities in medical care. These inequities can affect individuals based on race, lifestyle, socio-economic background, specific health conditions, family medical histories, and genetic predispositions. For instance, predictive models might favor certain populations over others, leading to unequal treatment recommendations, misdiagnoses, or resource allocations, further exacerbating disparities in patient care. The audits should be scaled to the size, resources, and risk level of the institution, ensuring that the approach remains feasible and meaningful for all organizations.

4.5.2 Framework for Fair and Consistent Outcomes Audits - Establish a structured process for conducting fair and consistent outcomes audits, with flexibility based on the size and resources of the organization. The framework should include at a minimum:

- Tiered Data Collection: Patient demographic data categorized into targeted risk areas.
- Pragmatic Bias Identification: Use readily available statistical tools and techniques such as data analysis with descriptive statistics, group comparisons using hypothesis testing, outcome fairness metrics like demographic parity, and visualization tools to identify disproportionate impacts on different subgroups at each stage, from data collection to model deployment and monitoring.
- Proportional Impact Assessment: Tailor the scope of impact assessments to the organization's scale and resources.

4.5.3 Scalable Fair and Consistent Outcomes Metrics - Develop and apply metrics that are scalable to the organization's size and resource capacity. Suggested areas for AI systems fairness and consistent output metrics include, but are not limited to:

- Data Representation: Engage the AI system vendor to ensure the AI system is trained with diverse patient data, proportionate to the organization's scale.
- Outcome Monitoring: Implement basic outcome monitoring with more in-depth metrics introduced as resources grow.
- Bias Mitigation: Monitor improvements in reducing biases with a priority on key clinical areas.

4.5.4 Accountability and Reporting - The organization shall implement a reporting and accountability structure to ensure compliance with the governance framework. This structure must include regular internal reviews, audits, and reporting on the following key compliance areas:

- Privacy
- Risk management

- Data security
- Fairness and Consistent Outcomes
- Incident reporting

The organization shall document findings and corrective actions and engage external auditors as required to verify adherence to governance and regulatory requirements.

4.5.5 Stakeholder Involvement – The organization shall engage diverse stakeholders, proportionate to its size and resources, to support continuous improvement. Stakeholders may include patients, healthcare providers, internal staff, community representatives, AI vendors, and relevant regulatory or oversight bodies.

Stakeholder participation shall be a structured and documented process that promotes fairness, transparency, and accountability in the governance of AI systems. Engagement activities shall be planned at defined intervals and scaled appropriately to organizational capacity.

Feedback obtained through these engagements shall be recorded, evaluated, and incorporated into governance updates, demonstrating a traceable link between stakeholder input and resulting decisions or corrective actions. The organization shall retain objective evidence of stakeholder engagement activities (such as meeting records, surveys, or consultation summaries) to confirm that patient and community perspectives are actively reflected in the responsible use of AI within healthcare operations.

Examples of Stakeholder involvement:

Organization Type	**Stakeholders Involved**	**Engagement Methods**	**Documentation and Follow-Up**
Smaller Organizations *(e.g., community clinic or single-site hospital)*	**Patients, clinical staff, local health representatives, and community members directly affected by AI-supported services.**	**• Quarterly feedback sessions or short focus groups.** **• Periodic surveys or comment forms to gather input on AI performance, clarity of communication, and patient trust.** **• Informal discussions during governance review meetings to capture user observations and community perspectives.**	**• Feedback recorded in a shared log or spreadsheet.** **• Summary report reviewed by leadership during quarterly governance meetings.** **• Documented actions showing how feedback informed policy or process updates.**
Larger Organizations	**Patients, clinicians, regulatory liaisons, AI**	**• Formal advisory boards and structured**	**• Detailed meeting minutes and**

(e.g., regional or national healthcare network)	**vendors, academic or research partners, and community advisory representatives.**	**stakeholder committees.** **• Annual public consultations, patient advisory panels, and community engagement events.** **• Digital feedback portals for continuous input on fairness, transparency, and system performance.**	**stakeholder reports reviewed by the AI Governance Committee.** **• Integration of stakeholder findings into management reviews and continuous improvement plans.** **• Published summaries or annual reports demonstrating transparency and accountability to the community.**

4.5.6 Continuous Improvement in Fairness - Integrate fair and consistent outcomes audits into the broader risk management and governance processes, scaling the complexity of these audits based on organizational capacity. Use practical and achievable methods for continuous improvement, allowing all institutions to adapt as their capabilities grow.

4.6 Data Privacy and Security

4.6.1 Data Protection Requirements - The organization shall ensure that all AI systems comply with applicable data protection laws and regulations, including but not limited to local, national, and international laws governing patient privacy and healthcare data security (e.g., HIPAA).

- Implement robust data protection measures, including encryption for sensitive data both in transit and at rest.
- Ensure that access to patient data is restricted to authorized personnel, using role-based access control (RBAC) and multi-factor authentication (MFA).
- Establish a clear process for patient consent related to the use of their data in AI systems.

4.6.2 Incident Response and Breach Management - The organization shall maintain a formal

incident response plan to handle data privacy and security breaches. The plan should include, but is not limited to:

- Procedures for detecting, reporting, and investigating security incidents involving AI systems.
- Notification processes for affected individuals and authorities in case of a data breach.
- Regular drills and updates to ensure the incident response plan remains effective.

4.6.3 Data Minimization and Retention - The organization shall minimize the collection and retention of personal data to only what is defined as necessary for the functioning of the AI system. This includes, but is not limited to:

- Implementing policies to regularly review and purge outdated or unnecessary data.
- Ensuring that data retention periods are aligned with regulatory requirements and organizational needs.

4.6.4 Security Audits and Vulnerability Management - The organization shall conduct regular security audits of AI systems to ensure compliance with data protection policies and to identify potential vulnerabilities.

- Penetration testing and vulnerability assessments shall be carried out at least annually or when significant changes are made to AI systems.
- Vulnerability management processes should be in place to address security weaknesses identified during audits or through threat intelligence.

4.6.5 Training and Awareness - All personnel with access to AI systems and patient data must receive regular training on data privacy and security best practices. This includes but is not limited to:

- Annual training on data protection laws, AI system security, and incident response protocols.
- Awareness campaigns to ensure employees understand the importance of maintaining data confidentiality and security.

5 Deployment Process

5.1 User Training

5.1.1 Comprehensive, Role-Specific Training Programs - The organization shall provide formal, role-specific training for all personnel involved in the use or oversight of AI systems or who interact with data processed by AI systems. This includes:

- **AI Application Training**: Training on the organization-specific implementation and functionality of the AI system, including expected output, end-user operation, incident reporting procedures, and contingency workflows if the application is unavailable, deemed unsafe, found to be non-equitable, or non-compliant with applicable standards and regulations the organization adheres to. This training should equip users with the knowledge to effectively and safely operate AI systems in their roles.

- **Healthcare AI Governance Awareness Training**: All personnel who interact with AI systems or data processed by AI systems shall complete Healthcare AI Governance Awareness Training during onboarding and at least once annually thereafter. This training shall provide a comprehensive understanding of the organization's AI governance framework, emphasizing the responsible use of AI, ensuring safety and fairness, and maintaining full compliance with relevant standards and regulations. Training materials shall be provided by, or approved by, the Institute for AI Governance in Healthcare (IAIGH).

- **Lead Implementor Training**: The AI Governance Officer (or Compliance Officer) is required to complete Healthcare AI Governance Standard Lead Implementor Training. Training materials shall be provided by or approved by IAIGH.

- **Internal Auditor Training**: Personnel conducting internal audits shall complete Internal Auditor Training to ensure they are equipped to audit the implementation of the Healthcare AI Governance Standard effectively. The training materials shall be provided by or approved by IAIGH.

5.1.2 Ongoing Education - Offer ongoing education and support to users, ensuring they remain informed about system updates and new AI governance challenges. The education should also address evolving governance considerations such as performance, fairness, scalability, and trust.

5.2 Monitoring and Evaluation

5.2.1 Continuous Monitoring - Establish mechanisms for ongoing monitoring of AI system performance and governance compliance, including responsible use, safety, and privacy standards. Regularly review system outputs to identify and address any governance issues.

5.2.2 Governance Metrics - The organization shall define, establish and monitor metrics for assessment of governance to evaluate the performance, compliance, safety and impact of AI systems. These metrics shall be tracked and reported at least once annually to top management, or more frequently based on the organization's size, resources, and risk profile. The following governance areas shall be included, but is not limited to:

a. Privacy and Data Protection: The number and risk severity of privacy and data protection incidents during the review period.
b. AI System Performance: AI system accuracy and reliability trends, reviewed in accordance with risk level and operational needs.

c. Fair and Consistent Outcomes Audits: Incidents of bias or inconsistency in AI outcomes, identified through periodic fair and consistent outcomes audits conducted at intervals proportionate to the organization's risk and resources.
d. User Feedback: Quantitative and qualitative user feedback on the transparency, trustworthiness, and overall user experience of AI systems, collected through engagement processes.
e. Operational Dependence: Measure the percentage of care workflows dependent on AI systems to guide resource allocation.
f. Remediation Timeliness: Measure time between incident identification and closure.

5.2.3 Incident Reporting and Response Timelines - The organization shall implement a structured process for reporting, responding to, and resolving governance-related incidents involving AI systems. All incidents shall be categorized by severity, with a risk=based approach used for establishing timeliness of incident triaging, incident containment, correction and corrective actions, reporting to relevant regulatory authorities and communication to the public.

5.2.4 Legal, Regulatory, and Contractual Requirements Register - The organization shall maintain a register of all applicable legal, regulatory, and contractual requirements, including any relevant laws, standards, regulations, and stakeholder agreements to which it must adhere. (e.g. HIPAA). This register must be reviewed and updated at least annually, or more frequently if there are significant changes in the external environment. The review should ensure that the organization remains compliant with current requirements and that these obligations are effectively integrated into its AI governance framework.

5.2.4.1 Incident Severity Classification - Incidents shall be classified based on a risk-based approach into one of the following severity levels, based on the potential impact on patient safety, privacy, system performance, and compliance:

Critical: Incidents that pose a life-threatening, immediate threat to patient safety, involve a significant data breach, or cause AI system failure leading to harmful outcomes. Incidents with a reasonable probability of serious adverse health consequences or death.

Examples: Misdiagnosis due to AI failure, unauthorized access to patient data, or AI system shutdown during critical patient care. Additionally, incidents involving inaccurate or misleading AI outputs (hallucinations) that impact patient care should be classified as critical incidents. Immediate steps must be taken to investigate the issue, communicate with clinical teams, and ensure the integrity of future outputs.

High: Incidents that could impact patient care or privacy but are not immediately life-threatening or involve data breaches without malicious use. Incidents where adverse health consequences are temporary or medically reversible, and serious outcomes are unlikely.

Examples: Incorrect AI-based treatment recommendations, or system performance issues that delay care.

Moderate: Incidents that cause minor disruptions in AI system performance or governance practices but do not directly impact patient safety or privacy.

Examples: Minor AI system inaccuracies or delays in non-critical processes.

Low: Incidents with minimal impact on patient care, system performance, or governance practices. Incidents where adverse health consequences are not expected.

Examples: User interface issues or non-essential AI system errors that are easily corrected.

5.2.4.2 Response Timelines to Complaints by Severity - For each severity level, a reasonable response timeline should be defined in a risk management plan. The response timeline should include acceptance of complaints, initial response, investigation and full resolution timeframes, in line with industry standards for healthcare systems.

	Critical Incidents	**High-Severity Incidents**	**Moderate-Severity Incidents**	**Low-Severity Incidents**
Initial Response	Immediate, within 1 hour of detection.	Within 4 hours of detection.	Within 1 business day of detection.	Within 2 business days of detection.
Actions	Triage the issue, notify key stakeholders (e.g., IT, clinical teams, compliance officers), and initiate a full investigation.	Conduct an initial investigation, mitigate immediate risks, and communicate with relevant departments (e.g., legal, IT, clinical staff).	Investigate the issue, determine whether it could escalate to a higher severity, and inform relevant staff.	Log the issue and determine if any immediate action is needed.
Full Resolution	Within 24 hours.	Within 72 hours.	Within 5 business days.	Within 10 business days.
Actions	Resolve the issue, implement corrective actions, and provide a full incident report to the governance committee. Post-incident analysis should follow to prevent recurrence.	Correct the issue, implement mitigation strategies, and document the incident for review by the governance board.	Resolve the issue, document findings, and update the governance committee on corrective actions.	Resolve the issue, document the resolution, and note any minor governance updates or adjustments.

5.2.3.3 Post-Incident Review - After an incident is resolved, a Post-Incident Review shall be conducted for all critical and high-severity incidents to assess the effectiveness of the response and identify opportunities for improvement as part of preventive action.

Timeline for Post-Incident Review:

Critical incidents: Within 3 business days of resolution.

High-severity incidents: Within 7 business days of resolution.

Moderate-severity incidents: Within 10 business days of resolution.

Low-severity incidents: Within 20 business days of resolution.

Key Review Areas:

- Cause of the incident and contributing factors.
- Timeliness and effectiveness of the response.
- Adequacy of corrective actions and measures to prevent recurrence.
- Impact on patient safety, privacy, and AI system performance.

5.2.3.4 Incident Reporting Documentation - The organization shall document all reported incidents, including:

- Incident ID
- Severity classification
- Date and time of detection
- Initial response time
- Full resolution time
- Corrective actions taken
- Post-incident review findings (for critical and high-severity incidents)
- Lessons learned and governance updates (if applicable)

This documentation shall be reviewed during audits and used as part of the continuous improvement process to enhance AI governance.

5.2.3.5 Compliance Monitoring and Reporting - The organization shall track and report on compliance with incident response timelines to ensure accountability and continuous improvement. The organization should define acceptable compliance metrics, such as aiming for 95% compliance with the defined response timelines across all severity levels. The governance committee should review incident response time performance on a quarterly basis and address any areas of non-compliance to enhance governance practices.

5.2.4 Continuous Output Monitoring for Accuracy - The organization shall establish monitoring processes for AI outputs, with a specific focus on identifying and mitigating inaccurate or misleading outputs (hallucinations). Monitoring should include timely flagging of abnormal outputs and scheduled evaluations of AI accuracy and consistency across clinical settings.

5.2.5 Monitoring Degradation in Efficacy - AI systems should be regularly evaluated for potential performance degradation, such as model drift, over time. This includes monitoring for decreases in system accuracy, clinical relevance, and efficacy. Procedures should be in place to recalibrate or update the system to maintain optimal clinical performance as part of post-deployment activities.

5.3 Regulatory Compliance

5.3.1 Compliance with Regulations - The organization shall ensure that AI systems used in healthcare fully comply with applicable regulations, governance standards, and legal requirements. Compliance measures shall be regularly reviewed and updated to address changes in regulatory frameworks and to proactively manage emerging issues related to AI governance.

5.3.2 Documentation and Audits - The organization shall maintain detailed documentation of governance compliance activities, including records of decisions, audit findings, training sessions, and risk assessments. These records shall be kept up-to-date and made available for regular internal reviews and external audits to ensure all aspects of AI governance, including safety, privacy, fairness, and regulatory standards, are adequately monitored and enforced.

As part of the internal audit process, the organization shall also review its Legal, Regulatory, and Contractual Requirements Register to ensure compliance with all applicable laws, standards, regulations, and stakeholder agreements.

5.3.3 Sampling for AI System Audits - To ensure the AI system's performance and fair and consistent outcomes audits are both effective and manageable, organizations shall adopt a structured approach to selecting a representative sample of clinical cases influenced by the AI system. This sampling process is designed to provide meaningful insights into the AI system's impact on patient outcomes and care, without requiring the review of every clinical interaction.

Sampling Requirements:

Randomized Sampling: Organizations shall define and select a manageable number of clinical results where the AI system was used, ensuring the sample includes a variety of patient demographics and care contexts (e.g., inpatient, outpatient, emergency).

Stratified Sampling: For audits requiring more focused data, the sample may be divided into subgroups based on factors such as age, gender, and general health conditions. Random selections from each subgroup shall ensure the sample is representative of the patient population served.

High-Impact Areas: Organizations should prioritize sampling from cases that have the highest potential impact on patient outcomes, such as critical diagnoses or complex care scenarios where the AI system's recommendations had significant influence.

Time-Based Sampling: Organizations should sample clinical cases at regular intervals over the audit period, ensuring that the data reflects performance over time rather than a single snapshot.

Minimum Sample Size:

- Smaller organizations shall sample a minimum of 25 clinical cases, ensuring variety in the cases selected to represent different demographics and clinical scenarios.

- Larger organizations shall sample a minimum of 50 clinical cases per audit cycle, focusing on specific AI-influenced cases that reflect key performance areas across the organization.

The data collected from these samples shall be used during governance reviews and fair and consistent outcomes audits, allowing the organization to track performance, fairness, and any discrepancies in clinical outcomes influenced by the AI system.

6 Patient-Centered Considerations

6.1 Transparency to Patients

6.1.1 Clear Communication to Patients - The organization shall ensure that patients are informed of AI system usage through:

a) Documented consent forms that explain the role, benefits, and limitations of AI systems in their care.
b) Periodic surveys or feedback mechanisms to gauge patient understanding and satisfaction with AI system use.
c) Healthcare organizations shall maintain patient education materials that explain AI-supported care pathways in accessible, non-technical language.

6.1.2 Accessible Information - Ensure that information about AI system decisions affecting patients' health is easily accessible, understandable and interpretable. Use language and formats that are understandable to patients across demographics and geographies, ensuring transparency in how AI systems align with governance practices, including privacy, trust, and regulatory compliance.

6.2 Patient Participation and Trust

6.2.1 Patient Involvement - The organization shall promote patient trust and understanding by communicating clearly and consistently how AI systems are used in their care. Information shall be provided in plain, accessible language describing the AI system's role, intended purpose, and governance safeguards that ensure fairness, accuracy, and accountability.

Patients shall be given meaningful opportunities to provide feedback on their experience with AI-supported care through structured, documented channels such as surveys, feedback forms, or participation in community or patient advisory discussions appropriate to the organization's size and capacity.

This engagement shall be used to confirm that AI systems are applied responsibly, remain aligned with clinical integrity, and reflect patient expectations. Records of patient feedback and

resulting actions shall be maintained as objective evidence of compliance with HAIGS requirements for transparency and responsible use of AI in healthcare.

6.2.2 Building Trust - Build patient trust by consistently applying governance principles, including safety, privacy, and responsible use. Address patient concerns promptly and demonstrate the reliability, fairness, transparency and accountability of AI systems.

7 Continuous Improvement and Research

7.1 AI Governance Oversight Boards

7.1.1 Establish a Governance Review Board - Establish a governance review board to oversee AI projects and ensure compliance with all governance standards. This board should have diverse representation from various stakeholders, including legal, medical, responsible use, and regulatory experts.

7.1.2 Regular Reviews and Audits - The organization shall conduct internal reviews and audits at planned intervals to ensure ongoing compliance with this standard. The internal audit program shall be planned, established, implemented, and maintained to include the frequency, methods, responsibilities, planning requirements, and reporting necessary to ensure effective governance. The internal audit scope and criteria shall cover the organization's governance framework, including safety, privacy, ethics, fairness, and regulatory compliance.

The organization shall conduct an internal audit at least annually to assess whether the governance practices conform to the requirements of this standard and are effectively implemented and maintained. The results of these internal audits, including findings, nonconformities, and corrective actions, shall be documented and reported to relevant management for review and decision-making. The results of the internal audits shall inform management reviews and support continual improvement efforts, ensuring that governance practices remain effective and aligned with the evolving requirements of this standard.

7.1.3 External Audit Requirements - The organization shall undergo an external audit conducted by the Institute for AI Governance in Healthcare (IAIGH) or any certification body authorized by IAIGH to verify compliance with the Healthcare AI Governance Standard. The external audit will assess the organization’s adherence to the risk management, fairness, and compliance requirements outlined in this standard. These audits will be conducted over a structured three-year cycle to ensure continued compliance with this standard.

The audit cycle shall include:

- Initial Certification Audit (Year 1)
  This audit will be carried out in two stages:
  - Stage 1: A preliminary audit will assess the organization’s AI governance framework documentation, ensuring that policies, procedures, and controls are in place and align

with the requirements of this standard. This stage will also evaluate the organization's readiness for the full audit.
    - Stage 2: A more detailed audit will verify the implementation of the AI governance framework. Auditors will examine how effectively the organization has applied its governance practices related to safety, privacy, ethics, fairness, and regulatory compliance. This audit will confirm that the framework is operational and capable of achieving ongoing compliance.

- Maintenance Audit (Year 2)
  In the second year, a maintenance audit will evaluate the organization's efforts to maintain and improve its governance framework. The audit will focus on continuous improvement, verifying that any nonconformities from the initial audit have been addressed and that the organization remains compliant with the standard.

- Re-Certification Audit (Year 3)
  A full re-certification audit will be conducted in the third year to verify ongoing compliance with the standard. The re-certification audit will assess the organization's sustained adherence to the AI governance framework and confirm that the governance practices remain effective and up to date.

The organization shall maintain documented evidence of all external audit results, including any nonconformities identified and the corrective actions taken to resolve them.

7.1.4 Continuous Improvement Process - The continuous improvement process ensures that insights from governance reviews, audits, and stakeholder feedback are integrated into the organization’s AI governance practices. This includes the following steps:

1. Monitoring and Evaluation: The organization shall continuously monitor AI system performance, governance metrics, and audit findings to identify areas for improvement. Specific areas for monitoring include:

- Governance metrics (e.g., privacy incidents, AI system accuracy, and bias).
- Incident reports and risk management updates.
- Feedback from stakeholders, including patients and staff.

2. Implementation of Corrective Actions: Following reviews and audits, corrective actions shall be identified and implemented. These actions should focus on closing governance gaps and improving AI system performance.

3. Documentation of Improvements: The organization shall maintain detailed records of governance improvements, including updates to policies, corrective actions taken, and their outcomes. Continuous improvement plans should be updated after every major audit or review.

4. Stakeholder Engagement in Improvement: Stakeholder feedback, both internal and external, shall inform continuous improvements. Regular consultations and feedback mechanisms (e.g., surveys, workshops) should be used to gather input on governance practices.

7.1.5 Technological and Regulatory Adaptation - To stay current with evolving AI technologies and regulatory changes, the organization shall ensure that:

1. Technological Monitoring: The organization shall monitor technological advancements in AI and assess their impact on existing governance practices.

2. Regulatory Compliance: Regular updates to governance frameworks shall be made to ensure alignment with new or updated regulations (e.g., HIPAA). The governance board shall be responsible for adapting practices as necessary.

3. System Updates and Validation: AI systems shall be regularly updated and validated, with changes documented and reviewed during audits to ensure ongoing compliance with safety, privacy, and responsible use standards. In the event of not validating AI systems, adequate rationale must be provided.

7.2 Collaboration and Sharing

7.2.1 Promote Collaboration - Promote collaboration between institutions to share best practices and advancements in AI governance. Foster a culture of learning and continuous improvement to advance adoption of the governance standard across the healthcare sector.

7.2.2 Open Data and Research - Encourage open sharing of data and findings to advance the field responsibly. Ensure that data-sharing practices align with governance principles, particularly those related to patient privacy and consent, as well as regulatory and responsible use compliance.

7.2.3 External Feedback and Public Reporting - The organization shall engage external stakeholders, including patient advocacy groups and healthcare regulators, to review AI governance practices at least annually.

- Publicly available reports on AI governance performance, including metrics on safety, privacy, fairness, and compliance, shall be published annually to enhance transparency and build public trust.

8 Fair and Consistent Outcomes-Focused Guidelines

8.1 Fair and Consistent Outcomes Audits

8.1.1 Purpose of Fair and Consistent Outcomes Audits - Conduct regular fair and consistent outcomes audits to ensure that AI systems do not disproportionately affect any population group. The audits should be integrated into the overall governance framework and aligned with the organization's risk management and continuous improvement processes.

8.1.2 Scalable Approach - The scale and frequency of fair and consistent outcomes audits shall be tailored to the size and resources of the organization. Fair and consistent outcomes audits are essential for ensuring that AI systems are implemented and managed in a manner that promotes fairness and equitable outcomes. The organization shall determine an appropriate frequency for conducting these audits, ensuring that they are thorough enough to address risks while remaining manageable within the organization's capacity.

8.1.3 Bias Detection and Mitigation - Fair and consistent outcomes audits should include procedures to detect and address biases in AI systems. Organizations should develop strategies to mitigate identified biases, ensuring fairness in outcomes for all patient demographics.

8.2 Representative Data Practices

8.2.1 Representative Datasets - Ensure that AI systems are trained on diverse and representative datasets. This includes collecting data that reflects the full range of patient demographics, such as age, gender, race, and socioeconomic background.

8.2.2 Data Collection and Usage - Data collection processes shall be designed to capture the necessary diversity to ensure that AI systems are fair and inclusive, while respecting privacy and regulatory requirements. The organization is responsible for implementing data collection practices that reflect the diversity of the populations they serve, ensuring compliance with all relevant data privacy laws and standards.

8.2.3 Continuous Review of Data Practices - Regularly review data collection and usage practices to ensure they remain aligned with the goals of responsible use and fairness. Adjustments to data collection may be needed as AI systems evolve or as new governance challenges arise.

8.3 Stakeholder Engagement

8.3.1 Purpose of Stakeholder Engagement - Stakeholder engagement is critical to ensure that AI governance practices are transparent, accountable, and aligned with the needs of the communities they serve. Engaging diverse stakeholders fosters trust, improves system outcomes, and ensures that governance frameworks remain adaptable and inclusive. The organization shall actively engage internal and external stakeholders to gather input on AI system design, performance, ethics, privacy, and consistent output.
8.3.2 Key Stakeholder Groups - The organization shall identify and engage the following key stakeholder groups, ensuring a diverse range of perspectives:

1. Internal Stakeholders:

- Clinical and Medical Staff: Provide feedback on AI system performance in patient care, safety concerns, and usability.
- IT and AI Development Teams: Contribute technical insights on system performance, data security, and scalability.
- Management and Governance Boards: Ensure alignment with organizational goals and compliance with regulatory requirements.
- Legal and Compliance Teams: Provide input on legal compliance, privacy issues, and risk management.

2. External Stakeholders:

- Patients and Patient Advocacy Groups: Gather feedback on the patient experience with AI systems, with a focus on fairness, transparency, and trust.
- Regulatory Bodies and Healthcare Authorities: Ensure compliance with evolving healthcare regulations and standards.
- AI Developers and Vendors: Collaborate with external AI system developers to address technical issues and fairness assurance.
- Community Representatives: Engage marginalized or underrepresented groups to ensure AI systems are equitable and inclusive in healthcare delivery.

8.3.3 Stakeholder Engagement Strategies - To effectively engage these stakeholder groups, the organization shall adopt the following strategies:

1. Regular Stakeholder Meetings:
Hold structured stakeholder meetings (e.g., quarterly or bi-annually) to review AI governance practices, performance, and feedback. These meetings should include representatives from all key stakeholder groups, providing an opportunity for diverse perspectives to be heard.

2. Feedback Mechanisms:
Implement formal mechanisms for stakeholders to provide ongoing feedback on AI system performance, governance practices, and output fairness and consistency. These mechanisms may include:

- Surveys and Questionnaires: Distributed to patients, staff, and external stakeholders to gather insights on AI system usability, transparency, and trust.
- Focus Groups and Roundtables: Target specific issues, such as fair and consistent AI outcomes or patient data privacy, providing a platform for in-depth discussions with stakeholders.
- Open Consultation Forums: Public or community meetings where stakeholders can express concerns or ideas about AI system governance and performance.
- Digital Feedback Channels: Anonymous reporting tools or online portals for stakeholders to submit feedback in real-time.

3. Collaborative Decision-Making:

Incorporate stakeholder feedback into the decision-making process. For major changes to AI systems or governance policies, involve key stakeholders (e.g., clinical staff, patient advocates) in evaluating options and assessing potential risks and benefits.

4. Fair and Consistent Outcomes Audits with Stakeholder Input:
Conduct regular fair and consistent outcomes audits with the participation of external stakeholders, especially marginalized or vulnerable communities, to assess how AI systems are performing across different demographic groups. These audits should inform adjustments to AI governance practices and system updates.

8.3.4 Stakeholder Communication and Reporting - Transparent and open communication with stakeholders is essential for maintaining trust and accountability. The organization shall:
1. Provide Regular Updates:
Communicate AI system performance, governance outcomes, and fair and consistent outcomes audit findings to all stakeholder groups. This can include:

- Quarterly or Annual Reports: Summarizing key metrics (e.g., AI system performance, data privacy, fair and consistent outcomes) and governance updates.
- Public Reports for External Stakeholders: Ensuring transparency in how AI systems impact patient care, data handling, and responsible use considerations.

2. Publish Corrective Actions:
When stakeholder feedback leads to changes in AI systems or governance practices, publicly document the corrective actions taken and the outcomes of these changes. This demonstrates accountability and responsiveness to stakeholder concerns.

3. Tailored Communication for Different Audiences:
Adapt communication styles and materials to suit different stakeholder groups. For example, patient-facing reports should focus on how AI systems are used in their care and address transparency and trust, while technical stakeholders may require more detailed reports on system performance and compliance.

8.3.5 Tracking Stakeholder Feedback and Engagement - The organization shall maintain a structured system for tracking stakeholder feedback and engagement efforts, ensuring that input is documented, evaluated, and acted upon. Feedback tracking systems should use digital tools to record stakeholder input, categorize it by theme (e.g., fair and consistent outcomes concerns, usability issues), and track follow-up actions. For each significant piece of feedback, a responsible party should be assigned, deadlines for addressing concerns set, and the progress of implementing changes or corrective actions tracked. The organization shall also develop metrics to assess the effectiveness of stakeholder participation efforts, including engagement frequency, stakeholder satisfaction, and the completion of follow-up actions.

An annual review of stakeholder participation practices shall be conducted to identify opportunities for improvement and adjust strategies as needed to ensure active involvement of all key groups in the governance process.

8.4 Fair and Consistent Outcomes Metrics

Organizations shall develop specific metrics to measure fair and consistent outcomes, with a focus on reducing bias, ensuring fairness, and enhancing transparency and accountability in AI governance.

8.4.1 Development of Fair and Consistent Outcomes Metrics - In addition to existing metrics, the following are examples of fair and consistent outcomes metrics that organizations can use to measure progress in Transparency and Accountability:

1. Transparency of AI System Decisions

- Metric: Percentage of patients who report understanding how AI systems are used in their care (e.g., via surveys or feedback forms).
- Purpose: To assess how well the organization communicates the role of AI in healthcare decisions to patients, ensuring they understand the system's capabilities and limitations.
- Target: Achieve a minimum of 90% of patients reporting a clear understanding of AI-assisted decisions.

2. Transparency in Data Usage

- Metric: Frequency of updates and public reports on data collection, usage, and privacy measures related to AI systems.
- Purpose: To track how often the organization provides transparency reports on AI system data usage, ensuring patient privacy and responsible use data practices.
- Target: Publish data transparency reports at least annually, outlining how data is collected, stored, and used by AI systems.

3. Public Accountability for Fairness and Consistent Outcomes

- Metric: Number of public reports on AI fairness and consistent outcomes and corrective actions taken to address bias.
- Purpose: To assess the organization’s commitment to publicly sharing its progress in improving AI fairness and reducing bias, thereby enhancing accountability.
- Target: Publish regular (e.g., annual) fair and consistent outcomes audit reports that include identified biases, actions taken to mitigate them, and the resulting improvements.

4. Stakeholder Involvement in Accountability

- Metric: Frequency and scope of stakeholder participation (e.g., patient advisory boards, public consultations) focused on AI governance and fair and consistent outcomes.
- Purpose: To track how often and how broadly the organization engages internal and external stakeholders in discussions about AI fairness, transparency, and accountability.

- Target: Conduct stakeholder consultations at least quarterly, with a focus on gathering feedback on AI system performance and fair and consistent outcomes.

5. Compliance with Public Reporting Requirements

- Metric: Compliance rate with regulatory and voluntary public reporting requirements on AI system fairness and governance performance.
- Purpose: To measure how well the organization complies with legal and self-imposed public reporting standards related to AI governance and fair and consistent outcomes.
- Target: Maintain 100% compliance with all regulatory and voluntary public reporting guidelines for AI governance.

8.4.2 Regular Review and Reporting - In addition to reviewing fair and consistent outcomes, organizations shall also regularly review and report on Transparency and Accountability metrics. These reviews should focus on how well the organization is communicating to patients, regulators, and stakeholders AI usage and governance practices that ensure safe, fair and consistent outcomes.

- Internal Reviews: Regularly evaluate how transparent AI governance practices are and how effectively the organization holds itself accountable for ensuring fairness and consistency in AI outcomes.
- Public Reporting: Larger organizations should issue public-facing reports on transparency and accountability, including how AI systems are used and how fair and consistent outcomes are ensured.

8.4.3 Integration with Stakeholder Feedback - Metrics related to transparency and governance effectiveness shall be integrated with feedback from internal and external stakeholders. Input from patients, healthcare staff, and regulatory bodies should be utilized to improve communication about AI system usage, fairness, and data practices. The organization shall ensure that stakeholder feedback contributes to ongoing design enhancements in transparency and compliance with the Healthcare AI Governance Standard.

8.5 Fair and Consistent Outcomes Impact Assessments

8.5.1 Timing of Assessments - Conduct fair and consistent outcomes impact assessments at critical stages of the AI system lifecycle, such as system design, deployment, and major updates. These assessments should focus on identifying potential fairness concerns early and mitigating them before they become embedded in the system.

8.5.2 Documentation and Follow-up - Document the findings of each fair and consistent outcomes impact assessment and create follow-up action plans to address any identified concerns. Ensure that mitigation strategies are effectively implemented and monitored over time.

8.5.3 Integration into Governance - Incorporate fair and consistent outcomes impact assessments into the broader AI governance and risk management framework. The assessments should not be isolated processes but part of a continuous improvement cycle to enhance fairness and consistency in AI systems.

Appendix A - Example Governance Applications for Organizations of Different Sizes

This section provides examples of how the Healthcare AI Governance Standard can be applied in practice by healthcare organizations with varying capacities. Whether an organization is large with abundant resources or smaller with limited resources, the following examples demonstrate how the governance framework can be tailored to suit the institutional capacity while maintaining compliance with the standard.

1. Risk Management

	Smaller Organization Example A rural healthcare clinic with limited resources implements an AI-based decision support system. To comply with risk management requirements:	**Larger Organization Example** A major urban hospital with a dedicated AI governance team deploys a suite of AI-powered diagnostic tools across multiple departments. To comply with the standard:
Risk Identification	Identifies key risks, such as patient safety, AI system reliability, and data privacy, using a simple risk matrix. The clinic collaborates with external AI vendors to ensure that risks associated with system updates and performance are monitored continuously.	Performs comprehensive risk assessments across departments, incorporating healthcare regulations such as HIPAA and state laws.
Legal, Regulatory, and Contractual Obligations	The clinic maintains a register of legal, regulatory, and contractual obligations, ensuring compliance with applicable healthcare standards and laws, such as HIPAA. This register is reviewed annually as part of the internal audit process.	The hospital maintains a detailed register of legal, regulatory, and contractual obligations, ensuring compliance with national standards and laws. This register is reviewed annually and updated as needed during internal audits to ensure continued compliance with the evolving legal landscape.
Mitigation Strategies	Develops basic mitigation strategies, including regularly checking the AI system for accuracy and ensuring staff understand when the AI may not be appropriate for use.	Creates detailed, department-specific risk mitigation plans that are updated regularly based on new risks and healthcare regulatory changes.

Documentation	Uses simple tools (e.g., spreadsheets or templates) to log risk assessments, the register of obligations, and mitigation measures.	Maintains thorough records in a governance platform, including the register of obligations, ensuring that all risks, compliance activities, and system changes are continuously tracked.
Review Frequency	The risks and the register are reviewed annually or following any significant changes to regulations or the AI system itself.	Conducts monthly reviews and audits using timely monitoring tools, ensuring AI systems adhere to healthcare governance standards and regulations.

2. User Training and Ongoing Education

Smaller Organization Example:

The provider implements a structured training program using materials provided or approved by the Institute for AI Governance in Healthcare (IAIGH). All personnel operating AI systems complete AI Application Training, and all personnel interacting with AI systems or AI output data complete Healthcare AI Governance Awareness Training during onboarding and annually. The AI Governance Officer completes Lead Implementor Training, and audit personnel complete Internal Auditor Training to meet the standard's requirements.

Larger Organization Example:

In a larger organization with broader AI adoption, the same training requirements apply: AI Application Training for all personnel operating AI systems, and Healthcare AI Governance Awareness Training for all personnel interacting with AI systems or data during onboarding and annually. The AI Governance Officer completes Lead Implementor Training, and audit personnel complete Internal Auditor Training. While more staff and systems may require training in larger organizations, the content remains consistent.

3. Fair and Consistent Outcomes Audits and Bias Mitigation

- **Smaller Organization Example:**

  A regional hospital serving a largely homogenous patient population introduces an AI tool for patient risk assessment. To comply with fair and consistent outcomes audit requirements:

- **Fair and Consistent Outcomes Audits**: Conducts annual fair and consistent outcomes audits, focusing on potential disparities in maternity care and chronic disease management. The hospital

uses demographic data it already collects, ensuring the AI tool does not introduce bias into these critical care areas.

- **Bias Mitigation**: Regularly checks the AI system for bias using vendor-provided fairness tools. The hospital ensures the AI system is trained on a representative dataset whenever possible.
- **Documentation**: Uses an internal database to record audit findings and documents any corrective actions taken to improve equitable care delivery.
- **Larger Organization Example:**

A national healthcare system with diverse patient demographics deploys multiple AI tools across diagnostics and treatment. To comply with fair and consistent outcomes audit requirements:

- **Fair and Consistent Outcomes Audits**: Conducts in-depth audits across all AI systems, analyzing data related to race, gender, and socioeconomic status. The healthcare system uses advanced statistical tools to detect biases and identify inequities in areas such as cardiology, oncology, and pediatrics.
- **Bias Mitigation**: Collaborates with AI vendors and in-house developers to update algorithms regularly, ensuring they are trained on diverse and representative datasets. Systems are updated continuously to address new biases as they emerge.
- **Documentation**: Maintains detailed records of fair and consistent outcomes audits, bias detection, and mitigation efforts. Publishes an annual report detailing audit findings, fair and consistent outcomes metrics, and improvements made to address healthcare disparities.

4. Stakeholder Engagement

Smaller Organization Example:

A community health center introduces a new AI tool for patient scheduling. To meet stakeholder participation requirements:

- **Engagement Methods**: Engages stakeholders (patients, staff) through simple surveys and feedback forms to gather their input on the AI tool's use.
- **Community Involvement**: Holds quarterly patient focus groups to discuss AI usage and make adjustments based on patient needs and concerns.
- **Documentation**: Keeps track of stakeholder feedback using an internal report that is reviewed by clinic management.

Larger Organization Example:

A large healthcare network with multiple hospitals and clinics deploys AI systems across various services. To meet stakeholder participation requirements:

- **Engagement Methods**: Establishes formal stakeholder committees, including patient advocates, medical professionals, and external experts, to provide continuous feedback on AI usage.
- **Community Involvement**: Hosts annual forums and public consultations to involve patients, healthcare providers, and regulatory bodies in discussions about AI impacts.

- **Documentation**: Develops detailed records of engagement activities, ensuring that feedback is incorporated into governance strategies and system updates.

5. Incident Reporting and Compliance

Smaller Organization Example:

A local clinic implements an AI-supported diagnostic tool for triage. To comply with incident reporting requirements:

- **Incident Reporting**: Implements a simple reporting system for AI-related incidents using standard forms and basic tracking software. When the AI system fails to flag a high-risk patient in emergency triage, the clinic logs the issue, informs staff, and works with the AI vendor to correct the system.
- **Compliance**: The clinic collaborates with the AI vendor for regular system updates and compliance with local healthcare regulations. Quarterly compliance checks are conducted, with particular attention to emergency response capabilities.

Larger Organization Example:

A large, multi-state healthcare organization uses AI in high-stakes diagnostic areas, such as oncology and emergency care. To comply with incident reporting requirements:

- **Incident Reporting**: Deploys an advanced, real-time reporting platform to track AI-related incidents. The system logs any AI malfunctions (e.g., misdiagnosis in oncology or failure in triage systems) and ensures immediate response from the clinical teams.
- **Compliance**: The organization's dedicated compliance team conducts frequent audits of AI systems to ensure adherence to national and international healthcare regulations. The team also updates systems and practices regularly based on regulatory changes and incident findings.

6. Patient-Centered Considerations

Smaller Organization Example:

A small outpatient clinic uses AI tools for appointment scheduling and triage. To comply with patient-centered considerations:

- **Clear Communication**: Provides patients with a one-page handout explaining how the AI system helps schedule their care, including its limitations and privacy protections.
- **Patient Involvement**: Organizations shall inform patients, in plain language, of how AI systems are used in their care, including their intended role, benefits, and limitations. Patients shall be given clear information about the use of AI in their treatment. Organizations are not required to allow patients to opt-out of AI employed in their care. Transparency and trust shall be prioritized over exclusion.
- **Building Trust and Documentation**: Clinic staff are trained to explain the role of AI during patient interactions, particularly addressing privacy concerns. Staff document any opt-out requests (granted or denied) or patient concerns, which are reviewed quarterly to ensure the AI system aligns with patient needs and builds trust.

- **Larger Organization Example:**
- A large hospital system using AI for diagnostics and patient management integrates the following patient-centered approaches:
- **Clear Communication**: Develops a detailed AI information portal for patients, including brochures and digital notifications. Patients are informed about the AI system's role in diagnosis, treatment planning, and how their data is used.
- **Patient Involvement**: Hosts workshops where patients can provide feedback on AI tools and participate in shared decision-making processes regarding AI-based treatment options.
- **Building Trust and Documentation**: Patient interactions involving AI are logged into the hospital's system, with feedback automatically forwarded to the AI governance board. Trends in patient feedback are documented and used in system performance reviews and governance audits, ensuring AI systems maintain high levels of trust and transparency.

7. Continuous Improvement and Research

Small Organization Example: A small regional hospital deploys an AI-supported diagnostic tool. To comply with continuous improvement requirements and ensure effective implementation of the standard:

- Governance Review: The hospital conducts a biannual review of the AI system's performance, using clinician feedback and a spreadsheet-based tool to track patient outcomes. The spreadsheet includes minimal but essential data to ensure AI system effectiveness and fair and consistent outcomes, such as:
    - Patient demographics: Age, gender, general health conditions.
    - Treatment outcomes: Diagnosis accuracy, length of hospital stay, recovery outcomes, and readmission rates.
    - AI system interactions: How often the AI tool was used for diagnosis or treatment, and whether it influenced clinical decisions.
    - Discrepancy flags: Any differences in outcomes or delays in treatment based on the AI system's recommendations.

  This data helps the hospital identify patterns or anomalies in patient care that may signal the AI system is not performing as expected.

- Fair and Consistent Outcomes Audits: The hospital conducts annual fair and consistent outcomes audits, using the same dataset in the spreadsheet to ensure that outcomes do not differ significantly across patient demographics. The goal is to detect any unintended variances in care that might suggest inequities in how the AI system supports clinical decisions. This is done by comparing the treatment outcomes and AI system interactions across different demographic groups (e.g., age, gender) without linking it to specific minority conditions.

- Legal, Regulatory, and Contractual Obligations: The hospital maintains a register of legal, regulatory, and contractual obligations, which is reviewed annually to ensure compliance

with HIPAA and other relevant healthcare regulations. This register is also part of the hospital's internal audit process.

- Monitoring Changes: If the hospital detects differences in treatment outcomes or AI performance through the governance reviews or fair and consistent outcomes audits, the findings are logged and reviewed. Corrective actions are taken to ensure the AI system delivers equitable and accurate results for all patients.

- Collaboration and Best Practices: The hospital engages in regional healthcare networks to share knowledge and best practices regarding AI governance and system improvements. This allows the hospital to remain up-to-date with the latest trends in AI usage without needing extensive internal resources.

Larger Organization Example:

A major healthcare system with research capabilities implements a range of AI systems. To comply with continuous improvement requirements:

- **Governance Review**: Establishes an AI governance review board, conducting monthly system reviews with a focus on both compliance and system enhancements based on patient and clinician feedback.
- **Collaboration**: Engages in multi-institutional collaborations, conducting joint research projects and publishing findings on AI governance and system improvements.
- **Open Research and Documentation**: Detailed logs of governance review meetings, including data on AI system performance, clinician and patient feedback, and collaboration outcomes, are stored in the organization's governance system. These records are reviewed during external audits and form the basis for ongoing system improvements. The organization also publishes a public annual report summarizing continuous improvement efforts and research contributions, demonstrating compliance with the governance standard.

Additional examples of how Smaller and Larger organizations might comply with specific sections of the standard to achieve compliance.

4.1.2.1 Governance Roles

a) AI Governance Committee

- For smaller organizations:

In smaller organizations with limited resources, this committee may consist of a small group of cross-functional leaders (e.g., CEO, compliance officer, medical director) who perform multiple governance functions.

- For larger organizations:

In larger organizations, the AI Governance Committee should include dedicated AI governance officers, legal experts, privacy officers, and department heads, who specialize in their respective areas of governance.

b) AI Governance Officer (or Compliance Officer)

- For smaller organizations:

A part-time compliance officer or another senior leader may take on this role, performing AI governance duties alongside other responsibilities.

- For larger organizations:

In larger organizations, this role may be filled by a full-time AI Governance Officer who focuses solely on managing governance practices and compliance.

c) Risk Owners

- For smaller organizations:

Risk owners may include heads of departments or senior staff who manage risks as part of their broader roles, focusing on the most critical risks identified.

- For larger organizations:

Larger organizations may assign dedicated risk managers or department heads to oversee specific risk categories (e.g., data security, clinical safety), with more frequent risk assessments and detailed reporting.

d) IT/AI System Administrators

- For smaller organizations:

The IT manager or a third-party service provider may handle AI system administration duties, with support from external vendors or consultants.

- For larger organizations:

Larger organizations should have a dedicated AI System Administrator or team responsible for ongoing AI system monitoring, optimization, and compliance checks.

e) Clinical Staff and AI Users

- For smaller organizations:

In smaller organizations, clinical staff may receive basic training on AI governance and rely on external support for technical issues and incident reporting.

- For larger organizations:

Larger organizations should ensure that clinical staff undergo more comprehensive training tailored to the specific AI systems they interact with, with regular updates and involvement in feedback loops.

4.1.2.2 Role Documentation

- For smaller organizations:

Smaller organizations may rely on simple, clear documentation of governance roles using existing templates and forms. They may consolidate roles where necessary due to resource constraints.

- For larger organizations:

Larger organizations should have detailed role descriptions, responsibility matrices, and reporting hierarchies that clearly define the functions and accountabilities of each governance stakeholder.

4.4.2 Framework for Fair and Consistent Outcomes Audits

- For smaller institutions or those with limited resources, simplified tools and approaches may be used to ensure equitable outcomes.

- Tiered Data Collection

- Smaller organizations may focus on basic categories or targeted risk areas. Leverage existing data sources where possible to reduce the burden of new data collection.
- Larger organizations can collect comprehensive patient demographic data.

- Pragmatic Bias Identification

- Smaller institutions can focus on high-priority areas of care where disparities are most likely.
- Larger organizations would expand the depth and range of bias detection beyond just the high-priority areas of care where disparities are most likely.

- Proportional Impact Assessment

- Smaller institutions can perform at minimum annual reviews.
- Larger organizations should conduct more frequent, in-depth analyses.

4.4.3 Scalable Fair and Consistent Outcomes Metrics

- Smaller institutions may focus on a few key metrics that are most relevant to their patient population and risk areas
- Larger organizations can develop more comprehensive sets of metrics.

4.4.4 Accountability and Reporting

- Smaller organizations with limited resources can comply by using simplified reporting templates provided within the governance framework. Internal reviews should be conducted by existing staff, covering key compliance areas such as privacy, risk management, data security, fairness, and incident reporting. External consultants and/or compliance management and tracking platforms can be engaged as required when internal resources are insufficient for detailed audits or regulatory verification.

- Larger organizations should conduct comprehensive audits across all required governance areas, including privacy, data security, risk management, fairness, and incident reporting. Dedicated compliance teams should manage these processes, and external consultants and/or compliance management and tracking platforms should be engaged as required to ensure full compliance with both governance policies and external regulatory standards.

4.4.5 Stakeholder Involvement

- Smaller organizations can meet this requirement by engaging key stakeholders through structured outreach methods such as focused feedback sessions or targeted consultations with patient and provider groups. These interactions should be documented and reviewed as part of regular governance assessments to ensure they contribute to compliance with the Healthcare AI Governance Standard. Organizations may also establish informal advisory groups to gather insights on patient needs, AI system performance, and regulatory expectations.

- Larger organizations should establish formal stakeholder participation processes, such as creating advisory boards or regularly consulting with broader stakeholder groups, including patient organizations, regulatory bodies, and healthcare professionals. These engagements should be systematically documented and reviewed, with clear evidence of how stakeholder input informs policy decisions, governance practices, and the organization's adherence to the Healthcare AI Governance Standard.

4.5.2 Scalable Governance

- Smaller organizations can use streamlined processes such as predefined templates and basic documentation tools (e.g., spreadsheets) to manage internal audits, governance tracking, and compliance. Incident reporting and reviews may be performed quarterly or as needed. External audits must be conducted at the required intervals to ensure adherence to the governance standard.

- Larger organizations should establish comprehensive governance systems, including dedicated AI governance teams, real-time monitoring tools, and more frequent reviews. Advanced tools should be utilized to monitor AI system performance, fairness assurance, and governance effectiveness. External audits must be conducted at the required intervals to ensure adherence to the governance standard.

4.5.3 Adaptable Framework

- Smaller organizations may adopt a flexible governance review cycle, updating policies annually or when major changes in AI technologies, performance, or regulations arise. To stay current with evolving AI risks and best practices, smaller organizations can subscribe to industry newsletters, participate in healthcare AI consortiums, and attend virtual workshops or webinars that provide updates on the latest advancements. In addition, they may designate a staff member to track emerging trends and regulatory changes, ensuring that governance policies remain responsive to new responsible use, technical, safety, and fairness risks without the need for extensive resources.

- Larger organizations should continuously update their governance framework, incorporating regular feedback from internal audits, external stakeholders, and the latest developments in AI technologies and regulatory requirements. They should leverage their resources by subscribing to industry newsletters, attending AI conferences and seminars, and ensuring key personnel participate in workshops and training sessions focused on AI advancements and associated risks. Larger organizations should also establish dedicated roles or committees to monitor

developments in AI, ensuring policies are regularly updated to reflect the latest best practices, responsible use and safety considerations, and regulatory shifts. The governance framework should be adaptable and scalable to ensure compliance across complex and diverse operational environments, with the capacity to respond swiftly to emerging challenges, including new technical, safety, and fairness risks.

5.2.3.5 Compliance Monitoring and Reporting

- Smaller organizations with limited resources may adopt simplified tracking tools, such as spreadsheets or incident logging software, and focus on meeting critical and high-severity incident timelines. For more complex incidents that require specialized expertise, smaller organizations can rely on external vendors or consultants to ensure timely and effective incident resolution.

- Larger organizations should have dedicated incident response teams and automated tracking systems to manage the response process efficiently. These organizations should establish formal procedures for conducting post-incident reviews, ensuring that lessons learned are integrated into future governance policies to improve overall compliance and incident response times.

7.1.2 Regular Reviews and Audits

- Smaller organizations with limited resources may use predefined templates and checklists provided by the governance framework to streamline their internal audit process. Simplified documentation practices can be applied, with a focus on key governance areas such as safety, privacy, and regulatory compliance, to ensure efficient use of resources while maintaining audit effectiveness.

- Larger organizations should implement more comprehensive audit processes, involving dedicated audit teams and more detailed documentation practices. These organizations may require more frequent internal audits or additional scope to cover complex governance structures and multiple compliance areas, ensuring thorough reviews of safety, privacy, ethics, fairness, and regulatory adherence.

8.1 Fair and Consistent Outcomes Audits
8.1.2 Scalable Approach

- Smaller organizations may conduct focused fair and consistent outcomes audits annually, concentrating on specific high-risk areas such as access to care or patient demographics. These audits can utilize streamlined methodologies to evaluate fair and consistent outcomes concerns without overextending limited resources.

- Larger organizations should perform more frequent and in-depth fair and consistent outcomes audits, covering a broader range of governance areas. These audits may involve detailed analyses of multiple fair and consistent outcomes dimensions, such as race, gender, and socioeconomic status, ensuring comprehensive assessments of AI system impact on diverse patient populations.

8.2 Representative Data Practices
8.2.2 Data Collection and Usage

- Smaller organizations may leverage public datasets or collaborate with external partners to access diverse data that meets fair and consistent outcomes standards. These partnerships can help mitigate resource constraints while ensuring sufficient data diversity for AI system development and governance.

- Larger institutions can prioritize the development of internal data collection systems, allowing for more comprehensive and controlled data gathering processes. These systems should be designed to collect and maintain diverse data from their patient populations, ensuring that fairness is addressed in a detailed and systematic manner.

8.3.5 Tracking Stakeholder Feedback and Engagement

- Smaller organizations can use simplified feedback mechanisms, such as online surveys and occasional focus groups, to gather input from patients and staff. Stakeholder meetings should be held at least annually, and all feedback should be documented in accessible formats, such as spreadsheets.

- Larger organizations should implement more formal engagement methods, such as establishing dedicated stakeholder advisory committees, hosting regular roundtables, and publishing public reports. Digital feedback tracking systems can be used to capture and respond to stakeholder input in real-time, with regular reports shared with external stakeholders.

8.4.3 Integration with Stakeholder Feedback

- Smaller organizations should focus on transparency regarding AI system decisions and stakeholder involvement to ensure that patients and staff clearly understand how AI systems are used. Regular internal reviews of transparency practices should be conducted, with simplified reporting mechanisms, such as patient-facing communications, implemented to maintain clarity.

- Larger organizations should adopt a broader set of metrics, including public transparency about how they are ensuring fairness and consistent outcomes, compliance with public reporting standards, and clear communication of data usage. Formal public reporting on AI fairness and governance efforts should be conducted regularly, integrating stakeholder feedback to ensure comprehensive oversight.

These examples illustrate how the Healthcare AI Governance Standard can be applied flexibly across organizations with different resource levels. Smaller organizations may focus on simplified approaches, leveraging external tools and collaborations, while larger institutions can implement more robust, in-house governance systems. Both approaches ensure compliance with the standard’s core principles while being adaptable to the organization's capacity.

Appendix B – Templates

The templates below provide a comprehensive and easy-to-use framework for risk management, incident reporting, and audits across all governance activities within the standard. They are designed to be scalable, ensuring that both smaller and larger organizations can implement them with minimal complexity while maintaining compliance with the Healthcare AI Governance Standard (HAIGS).

Template 1: Risk Assessment Matrix

This matrix helps organizations assess risks related to AI systems, including patient safety, privacy, fairness, and regulatory compliance. Usage of AAMI 34971:2023 can be referred to.
Instructions:

1. **Risk**: Identify the specific risk
2. **Likelihood**: Assess how likely the risk is to occur.
3. **Impact**: Determine the potential impact on the organization or patient safety.
4. **Risk Level**: Combine likelihood and impact to establish an overall risk level.
5. **Mitigation Strategy**: Outline the steps or measures to reduce the risk.
6. **Risk Owner**: Assign a responsible person for managing the risk.
7. **Review Date**: Set a date for reviewing the risk.
8. **Status**: Track the status of the risk (e.g., ongoing or resolved).

Risk	Likelihood (Low, Medium, High)	Impact (Low, Medium, High)	Risk Level (Low, Medium, High)	Mitigation Strategy	Risk Owner	Review Date	Status (Ongoing, Resolved)
Data breach due to system vulnerability	High	High	High	Implement encryption and conduct regular vulnerability assessments	IT Security	01/02/2026	Ongoing

AI algorithm bias affecting patient outcomes	Medium	High	High	Implement fair and consistent outcomes audits and fairness assurance procedures	AI Governanc e	01/03/2026	Ongoing
Non-compliance with regulations	Low	Medium	Medium	Ensure regular compliance checks and employee training	Legal	01/04/2026	Resolved
Patient safety risk due to AI misdiagnosis	Medium	High	High	Conduct AI system validation and implement safeguards for critical decisions	Clinical Team	01/05/2026	Ongoing

Template 2: Incident Reporting Form

This form is used to log governance-related incidents, including data breaches, patient safety issues, or AI system failures.

Instructions:

1. **Incident ID**: Assign a unique identifier for each incident.
2. **Date of Incident**: Record the date the incident occurred.
3. **Reported By**: Enter the name of the person reporting the incident.
4. **AI System Affected**: Specify the AI system involved.
5. **Incident Description**: Provide a brief but detailed account of the incident.
6. **Immediate Action Taken**: Note what immediate steps were taken to contain or resolve the issue.
7. **Investigation Findings**: Document the findings of any investigation into the cause of the incident.
8. **Corrective Action(s)**: Outline the actions taken to prevent recurrence.
9. **Completion Date**: Record the date the corrective actions were completed.
10. **Responsible Party**: Identify who is responsible for managing and resolving the incident.

Incident ID	Date of Incident	Reported By	AI System Affected	Incident Description	Immediate Action Taken	Investigation Findings	Corrective Action(s)	Completion Date	Responsible Party
INC-2026-001	02/10/2026	Jane Doe	AI Diagnostic Tool	Data breach identified in patient records due to incorrect access controls.	Revoked access, notified IT Security.	Breach caused by misconfigured access privileges.	Updated access controls, conducted employee training on data handling.	02/15/2026	IT Security
INC-2026-002	03/01/2026	John Smith	AI Scheduling Tool	AI system assigned incorrect appointment slots for high-priority patients.	Manual intervention to correct scheduling errors.	System logic issue detected in priority assignment algorithm.	Updated algorithm, conducted post-update testing.	03/10/2026	AI Development Team
INC-2026-003	03/15/2026	Sarah Lee	AI Risk Assessment	AI incorrectly flagged patient for high-risk due to missing demographic data.	Investigated demographic data collection errors, flagged for review.	Data entry issue; demographic fields were not consistently filled in by clinical staff.	Implemented mandatory demographic fields in patient intake system.	03/20/2026	Clinical Operations

Template 3: Audit Checklist

This checklist ensures all elements of the Healthcare AI Governance Standard (HAIGS) are reviewed and evaluated during internal audits.

Instructions:

1. **Audit Area**: Define the key areas to be audited based on the standard.

2. **Audit Criteria**: List specific criteria for compliance.
3. **Compliant**: Mark “Yes” or “No” based on the findings.
4. **Evidence Provided**: Record any evidence that supports compliance (e.g., documents, reports).
5. **Findings/Recommendations**: Note any findings or recommendations based on the audit.
6. **Action Required**: Identify whether corrective actions are needed.
7. **Responsible Party**: Assign responsibility for addressing any actions.
8. **Due Date**: Set deadlines for completing corrective actions.

Audit Area	Audit Criteria	Compliant (Yes/No)	Evidence Provided	Findings/Recommendations	Action Required	Responsible Party	Due Date
AI Governance Framework	Is a formal AI governance framework established and implemented?	Yes	Governance policy documents, governance committee minutes.			Governance Committee	
Risk Management	Are risk assessments conducted annually or when significant changes occur?	Yes	Risk assessment reports, risk management matrix.			Risk Management Team	
Data Privacy and Security	Are data protection measures in place (e.g., encryption, access controls)?	No	Lack of encryption in certain data storage systems.	Implement encryption in all patient data storage locations.	Yes	IT Security Team	04/01/2026
Fair and Consistent Outcomes Audits	Are fair and consistent outcomes audits being conducted to identify biases in AI system outcomes?	Yes	Fair and Consistent Outcomes audit reports, demographic analysis reports.			Fair and Consistent Outcomes Audit Team	
Incident Reporting and Management	Is there an incident reporting system in place, and are	Yes	Incident reports, corrective action logs.			Compliance Officer	

	incidents documented and resolved appropriately ?						
Training and Competency	Are all staff members trained on AI governance, data privacy, and security?	No	Incomplete training records for some staff members.	Ensure all staff complete mandatory training on data privacy and AI system usage.	Yes	Training Department	04/15/2026
AI System Validation	Are AI systems regularly tested and validated for accuracy and performance?	Yes	Validation reports, testing logs.			AI Development Team	
External Audit	Is there a plan in place for external audits at the required intervals?	Yes	External audit schedule, contracts with audit firm.			Governance Committee	

AI System Performance and Fair and Consistent Outcomes Audit Spreadsheet Design Template

1. **Date**: The date of the patient interaction with the AI system.
2. **Patient ID**: An anonymized identifier to maintain privacy.
3. **Age Group**: Grouping patients into age categories (e.g., 18-34, 35-50) to track fairness and consistent outcomes across demographics.
4. **Gender**: Identifying gender for fair and consistent outcomes audits.
5. **General Health Conditions**: Tracking common conditions (e.g., hypertension, diabetes) to ensure that the AI system treats patients equitably, regardless of health status.
6. **Diagnosis Outcome**: Whether the diagnosis or recommendation by the AI system was accurate or inaccurate.
7. **AI Used (Yes/No)**: Whether the AI system was used in the diagnosis or treatment decision.
8. **AI Influence on Decision (Yes/No)**: Whether the AI system influenced the clinician's final decision.
9. **Length of Stay**: The number of days the patient stayed in the hospital, if applicable.
10. **Recovery Outcome**: Whether the patient fully recovered or experienced complications.

11. **Readmission (Yes/No)**: Whether the patient was readmitted within a specified timeframe (e.g., 30 days).
12. **Discrepancy Flag (Yes/No)**: Flagging any discrepancies in treatment, such as unusual outcomes or delays, to identify potential AI system issues.
13. **Notes/Actions**: Any follow-up actions or notes on specific cases, such as corrective actions taken if discrepancies were found.

This template allows for easy tracking and auditing of both AI system performance and fair and consistent outcomes without requiring extensive resources, making it practical for smaller organizations to implement.

- Governance Review: The data in this template can be reviewed to track the AI system's overall performance and effectiveness. This helps the organization ensure that the AI is consistently accurate and reliable.
- Fair and Consistent Outcomes Audit: The same data can be analyzed annually to ensure that the AI system is not introducing inequities into the care process. By comparing outcomes across age groups, genders, and health conditions, the organization can ensure that the system is treating all patients fairly.

Appendix C – Normative References

This annex provides additional guidance on the normative references listed in Section 2, including their applicability and whether they are required or optional for compliance with this standard.

Reference	Type	Applicability
WHO Guidance on Ethics & Governance of AI for Health	Required	This document outlines global ethical principles and governance practices for AI in healthcare. For HAIGS adopters, it provides foundational insights into how to approach ethical considerations, such as transparency, accountability, and fairness, in implementing AI systems for patient care. Use this guidance to inform high-level governance policies and engage stakeholders in ethical AI practices.
HIPAA (Health Insurance Portability and Accountability Act)	Required	HIPAA ensures the protection of patient data privacy and security. Adopting HAIGS requires aligning your organization's governance frameworks with HIPAA requirements, particularly for AI systems processing or accessing protected health information (PHI). Review your AI implementation processes to ensure compliance with HIPAA's Security Rule and Privacy Rule.
ISO/IEC 42005 (AI system impact assessment guidance).	Applicable where relevant	ISO/IEC 42005 is the international standard for AI system impact assessment, providing a structured method for organizations to evaluate the potential consequences of their AI systems on individuals and society. It guides organizations in identifying and analyzing both intended and unintended impacts, integrating this process with their broader AI risk management and management systems.
ISO/IEC 42001:2023 (Artificial Intelligence Management System – Requirements)	Applicable where relevant	ISO 42001 provides a universal framework for AI governance, applicable across industries and focused on accountability, transparency, and risk management. HAIGS complements ISO 42001 by addressing healthcare-specific nuances, including patient safety, equitable outcomes, and governance scalability for diverse healthcare organizations. HAIGS also delivers tailored tools and guidance to help healthcare organizations implement AI systems effectively within clinical and regulatory contexts.
ISO 31000:2018 (Risk Management – Guidelines)	Applicable where relevant	This standard provides principles for identifying and managing risks. Organizations adopting HAIGS can use it to develop scalable risk management processes that align with their size and complexity. Consider ISO 31000 for structuring risk assessments for AI systems and defining risk tolerance levels.

NIST AI Risk Management Framework	Applicable where relevant	An alternative to ISO 31000, providing specific methodologies for managing risks in AI implementation.
ISO/IEC TR 24027:2021 (Bias in AI Systems and AI-Aided Decision Making)	Applicable where relevant	This document offers guidance on identifying and mitigating bias in AI systems. Use it to establish governance processes for monitoring AI outputs and ensuring fairness in patient outcomes. It's particularly useful for HAIGS adopters seeking to address demographic biases in healthcare AI.
ISO 27001:2022 (Information Security Management Systems)	Required	ISO 27001 offers a comprehensive framework for data security governance. For HAIGS, this standard can help organizations secure sensitive AI-related data and integrate robust access control measures. If national or internal standards are already in place, ensure they cover similar objectives to meet HAIGS requirements.
ISO 9001:2015 (Quality Management Systems – Requirements)	Applicable where relevant	This standard provides a framework for quality management that is scalable to organizations of all sizes. Use it to formalize governance processes and improve oversight of AI systems in patient care. It's especially valuable for larger organizations managing multiple AI implementations.
ISO 22320:2018 (Emergency Management – Guidelines for Incident Management)	Applicable where relevant	This standard guides the development of structured incident management processes. HAIGS adopters can use it to establish clear protocols for reporting and addressing incidents related to AI system failures, including patient safety risks or data breaches.
EU AI Act	Applicable where relevant	Relevant for organizations operating in or engaging with the EU regulatory framework; optional for non-EU contexts.
ISO/IEC 22989:2022 (Artificial Intelligence – Concepts and Terminology)	Applicable where relevant	Adopting ISO/IEC 22989 helps ensure terminology consistency when complying with other AI-related standards, such as the EU AI Act or ISO 42001. This alignment reduces ambiguity and enhances interoperability between governance practices and compliance efforts. By harmonizing terminology, organizations can more efficiently integrate HAIGS governance with broader international requirements, reducing duplication of effort in documentation and training.