Artificial Intelligence Accreditation Standard

Medical Software Industry Association Limited & Medical Technology Association of Australia

1 December 2025

MTAA Medical Technology Association of Australia

MSIA Medical Software Industry Association

MinterEllison.

MinterEllison Consulting.

Introduction

This is the Medical Software Industry Association (**MSIA**) and Medical Technology Association of Australia (**MTAA**) Artificial Intelligence Accreditation Standard, Version 1, 1 December 2025 (the **Standard**).

The Standard sets the requirements against which MTAA and MSIA members are assessed to become an Accredited Organisation. To be accredited, the organisation must:

- be a member of MSIA or MTAA; and
- provide evidence that they satisfy the MSIA and MTAA Artificial Intelligence Governance Code (the **Code**) as set out in this Standard.

Accredited Organisations can display the MSIA or MTAA logo *as appropriate* with the text "Accredited Signatory under the MSIA & MTAA AI Code", to demonstrate to the market that they meet the industry standard for safe and responsible governance of AI Systems as set out in the Code. The requirements in the Standard were developed by operationalising the provisions of the Code through a structured mapping to the ten guardrails of the Voluntary AI Safety Standard issued on 5 September 2024 by the Department of Industry, Science and Resources. The drafting process considered recognised frameworks, including the National Institute of Standards and Technology AI Risk Management Framework and ISO/IEC 42001, to enhance consistency with established governance and control practices.

Unless otherwise defined in the Standard, capitalised terms have the meaning given to them in the Code.

Accreditation Standard Criteria

1. Accountability

Code Criteria

The Participant Organisation will establish and maintain appropriate processes to support organisation-wide accountability and regulatory compliance in the use of AI Systems. This may include (as is appropriate in the organisational context):

- appointing an overall owner for AI use;
- developing a clear AI strategy;
- developing a documented organisational AI governance framework; and
- ensuring that personnel (particularly executives) possess the appropriate knowledge and competencies to uphold quality and compliance in the governance and use of AI Systems.

Internal processes will be documented to demonstrate accountability across the Participant Organisation.

The Participant Organisation will take steps to put in place oversight of AI Systems throughout their lifecycle.

1. Requirements

1.1 Assign organisational accountability and authority for AI to key roles within the Accredited Organisation that are competent and empowered. This will include maintaining the following across the AI lifecycle:

(a) explicit leadership commitment to AI accountability;

(b) documented roles and responsibilities for AI across senior stakeholders; and

(c) sufficient resource allocation to enable roles and responsibilities.

1.2 Establish and document an AI strategy aligned with organisational objectives and values, supported by appropriately detailed processes.

1.3 Assign and document accountable owners for AI Systems to oversee and intervene in the operation across of AI Systems across the AI lifecycle. This should include:

(a) identification of conditions that trigger human intervention, as well as supporting escalation paths and decision authority; and

(b) allocation of lifecycle responsibilities to the best suited teams, including oversight of third-party AI Systems.

1.4 Deliver appropriate training for accountable people and personnel under the AI strategy, including in relation to AI literacy. This requires the Accredited Organisation to:

(a) conduct a training needs analysis to understand training requirements across the organisation;

(b) deliver training that enables personnel to fulfil their roles and responsibilities under the AI strategy;

(c) maintain training and competency records; and

(d) update AI training as AI use evolves.

2. Risk Management

Code Criteria

The Participant Organisation will establish and maintain appropriate risk-management processes to identify, assess and address risks associated with AI Systems across their lifecycle, proportionate to their organisational context.

Specific risk-management strategies will be implemented to manage clinical risk. This may include, for example, a requirement that:

- AI Systems are only applied in clinical practice, where clinically suitable;
- before deployment, any Health Software that incorporates an AI System undergoes appropriate clinical validation and approval (for instance to confirm that clinical expertise is leveraged throughout the total product lifecycle, the Health Software incorporating an AI System uses datasets that are representative, and selected reference standards are fit-for-purpose); and
- after deployment, the AI System is subject to ongoing monitoring and review to ensure its performance and risk profile remain appropriate for a clinical context, and re-training risks are managed (where applicable).

If risks cannot be eliminated, reasonable steps will be taken to mitigate these risks.

To demonstrate compliance with risk management processes, the Participant Organisation may develop risk taxonomies, implement risk registers, develop and maintain quality management documentation, and attend to delineating responsibilities across the AI System supply chain.

2. Requirements

2.1 Set and document an organisation-level AI risk tolerance for the use of AI Systems, including defining criteria for acceptable and unacceptable AI risks. Based on this risk tolerance, identify unacceptable or prohibited AI Systems and use cases.

2.2 Create and document an AI System risk and impact assessment that covers internal and third-party AI Systems and sets clear triggers and timing for reassessment across the lifecycle.

2.3 Perform and document a risk assessment for each AI System. Assess and document risks with reference to specific intended and unintended uses for that AI System, along with key characteristics of the AI System. This should include:

(a) where people or groups may face significant potential harms, carry out and document an appropriate AI impact assessment and communicate identified risks and mitigations to relevant teams and third parties; and

(b) for AI Systems used in a Health Context, document clinical validation commensurate with risk, ensure deployment and use is only for clinically suitable scenarios, demonstrating safety and efficacy for the intended population.

2.4 Implement documented controls promptly to safeguard against identified risks and potential harms and verify their effectiveness through reassessment.

2.5 Repeat risk assessments and treatment plans periodically and whenever material changes or new risks arise, including in response to impact assessments.

3. Data Governance

Code Criteria

The Participant Organisation will establish and maintain appropriate data governance, privacy and cybersecurity measures across the AI System lifecycle to:

- comply with applicable privacy laws, including the *Privacy Act 1988* (Cth) and any applicable State or Territory legislation binding on the Participant Organisation;
- safeguard the provenance, security and quality of the data stored, including its accuracy and currency;
- protect against unauthorised disclosure, use, and access to data by AI Systems (including when incorporated in Health Software); and
- ensure the quality of data, including its accuracy, currency and management across the data lifecycle,

as appropriate, having regard to the unique characteristics of any AI System in use and the Participant Organisation's position in the AI System supply chain.

3. Requirements

3.1 Ensure existing organisational policies, standards and controls (including in relation to data governance, privacy, system management security and cybersecurity) address AI specific risks, including how the Australian Privacy Principles and Australian Signal Directorate Essential Eight (**Essential Eight**) are applied to the organisation's AI Systems.

3.2 Define and document appropriate AI data governance processes for AI Systems. This should include:

(a) data quality, provenance and preparation requirements;

(b) data sources;

(c) collection processes and types of data used for training, testing and operation;

(d) how the Australian Privacy Principles have been applied;

(e) how the Essential Eight has been applied; and

(f) data usage rights including intellectual property, indigenous data sovereignty, confidentiality and contractual rights.

3.3 Report to stakeholders about data and large language model (**LLM**) sources where appropriate for all AI Systems.

3.4 Consider and document data breach reporting requirements processes for AI Systems in alignment with applicable standards (such as the *Privacy Act 1988* (Cth)).

4. Testing, Monitoring and Controls

Code Criteria

The Participant Organisation will establish and maintain processes to test and evaluate AI Systems across the AI System lifecycle. The frequency and nature of testing and monitoring will be determined by the Participant Organisation, having regard to the nature and complexity of the AI System/s in use.

The Participant Organisation will implement proportionate controls to mitigate identified risks and will establish processes to facilitate transparency of AI Systems, enabling human oversight where appropriate, through a high-level understanding of AI System behaviour, and the ability to correct or amend outputs where necessary.

To support this, the Participant Organisation will ensure that workplace AI System use policies are developed and implemented to guide personnel on the safe and compliant use of AI Systems within the Participant Organisation.

To the extent the Participant Organisation develops Health Software incorporating AI Systems, that Participant Organisation acknowledges:

- Health Software incorporating AI Systems must be proven to an appropriate standard of evidence and deemed safe for the population in the Health Context in which they are intended to be applied. The level of evidence required to demonstrate the efficacy, accuracy and safety of Health Software incorporating an AI System should be commensurate with the level of risk connected to the use of that AI System; and
- the importance of post-market surveillance systems, including to manage any re-training risks.

4. Requirements

4.1 Create and operate proportionate organisation-wide processes and capability for testing, monitoring, continuous evaluation, improvement and reporting of AI Systems, with appropriate documentation. This should include:

(a) a process to map business targets to system performance with clear metrics for internal and third-party AI Systems; and

(b) a formal review and approval process for evidence that AI Systems meet their test requirements.

4.2 Define specific, objective and verifiable acceptance criteria for AI Systems that link to identified harms and record acceptance criteria in a registry. Communicate acceptance criteria to relevant teams, and review and update them when the AI System, risks or context change.

4.3 Develop and execute a test plan that covers all acceptance criteria, uses representative non-training data and benchmarks, and produces a complete test report. This should include:

(a) conducting adversarial testing such as red teaming;

(b) defining clear criteria that must be met before deployment; and

(c) for AI Systems intended for use in a Health Context, clinical validation to an appropriate standard of evidence, demonstrating safety and efficacy for the intended population.

4.4 Ensure workplace AI acceptable use policies (or directions) are developed, implemented and maintained to guide personnel about safe and compliant AI use within the organisational context, including prohibited use cases.

4.5 Implement continuous monitoring and evaluation to evidence that each AI System continues to meet its acceptance criteria. This should include:

(a) clear feedback channels;

(b) auditable logs and review processes that enable recourse and redress where required; and

(c) a formal review of whether the risk level warrants regular audits, documenting the requirement and plan.

4.6 Document the testing, monitoring and controls for each AI System prior to its implementation. This should include:

(a) competency, oversight, intervention and monitoring requirements;

(b) completed test reports; and

(c) authorisation by the accountable owner.

5. Inform End Users

Code Criteria

The Participant Organisation will ensure that end users can reasonably access relevant information about the AI Systems used and developed by the Participant Organisation, particularly where outputs may significantly or materially affect individuals' rights or interests.

5. Requirements

5.1 Ensure that relevant end users can easily access and understand key information about AI Systems used by the Accredited Organisation, including how these systems operate, the decisions they influence, and any potential impacts on individuals. This may include:

(a) indicating when AI is used in direct interactions, decision-making, or content generation;

(b) ensuring transparency around the use of third-party AI System that may impact end users;

(c) meeting relevant reporting obligations under applicable legislation (e.g. the *Online Safety Act 2021* (Cth)); and

(d) offering appropriate training to enable end users to safely interact with the Accredited Organisation's AI Systems.

6. Contestability

Code Criteria

The Participant Organisation will establish mechanisms that enable and support individual people directly, significantly and materially impacted by an AI System used by the Participant Organisation to challenge how that AI System is being used, and contest AI System decisions, outcomes, or interactions.

6. Requirements

6.1 Create and communicate a process that lets people directly, significantly or materially impacted by an Ai System to challenge how that AI System was used in relation to them. The process should specify:

(a) when an impacted individual can challenge an AI System;

(b) the process an impacted individual must follow to challenge an AI System; and

(c) how the Accredited Organisation will respond.

6.2 Assign an accountable person to oversee concerns, challenges and remediation requests.

6.3 Operate a documented review process to evaluate contests and requests for information across the Accredited Organisation.

7. Transparency

Code Criteria

To the extent the Participant Organisation develops or sells AI Systems (including Health Software incorporating an AI System), that Participant Organisation will ensure that each AI System is labelled with a version number, and that AI System is supplied to third parties (including users) with access to information regarding the particular AI System:

- in an accessible way; and
- to assist users to effectively address potential risks arising from the use of that AI System.

The Participant Organisation will ensure users can reasonably access relevant information about each AI System developed, or deployed by the Participant Organisation, for use in a Health Context, including, for example:

- the particular AI System's intended use and purpose and indications for use, benefits and risks, and its regulatory status (i.e. it is not a Medical Device);
- general information about the dataset on which the AI System was (and is) tested and trained, including the extent to which customer data has been used to train and/or improve that system;
- the role of human oversight and supervision required for the safe deployment of the AI System;
- limitations of the AI System, including any Health Contexts in which it should not be used, and the Participant Organisation must consider whether disclaimers are appropriate in the AI System user interface, ensuring to take reasonable steps to reduce risk of alert-fatigue;
- the type of AI approach or AI technology used (for example, rule-based systems, machine learning models, or generative methods); and
- how to address system failures.

7. Requirements

7.1 Where an Accredited Organisation develops an AI System:

(a) those deploying that AI System must be provided with access to sufficient information about the AI System, including:

(i) AI System capabilities and limitations;

(ii) technical details (such as model architecture, description of data, components and their characteristics);

(iii) relevant test methods, use cases and test results;

(iv) data management processes, including data quality, metadata, and provenance;

(v) known limitations, risks and mitigations and external audit findings;

(vi) data governance for training and testing data including data quality, bias, and provenance

(vii) privacy, security and cyber practices, including conformance to standards and best practice; and

(viii) details of known potential bias and high-level information about the actions taken to minimise negative effects.

7.2 Communicate to third-party AI System providers in enough detail to highlight and replicate issues without compromising privacy or security the following information:

(a) the expected use of the AI System;

(b) any unexpected or unwanted bias observed in use; and

(c) issues, faults and incidents that occur.

7.3 Agree and document in contract form AI System responsibilities and accountabilities with third-party AI System providers. This may include:

(a) monitoring and evaluation of AI System performance;

(b) issue identification, resolution and updates;

(c) human oversight and intervention triggers;

(d) a process for raising issues and contested outcomes that protects user and stakeholder privacy; and

(e) scheduled regular reviews based on timed intervals and key milestones or events.

7.4 For each AI System deployed in a Health Context, provide an accessible user-facing interface and documentation that is up-to-date and includes the following information:

(a) the version number of the Health Software used (if relevant);

(b) high-level information about the datasets used to train and test;

(c) the role of human oversight and how to request review;

(d) the AI System's limitations and any Health Context where it must not be used with targeted interface disclaimers that minimise alert-fatigue; and

(e) the type of AI approach in plain English, and how to address system failures including fallback steps and how to report issues.

8. Record Keeping

Code Criteria

To the extent it is within the Participant Organisation's control, the Participant Organisation will ensure that appropriate records are made and kept in relation to AI System use, deployment, development, design, manufacture, sponsorship, distribution or implementation by the Participant Organisation.

8. Requirements

8.1 Maintain an organisation-wide inventory of every AI System deployed that is reviewed regularly with consistent detail across entries. Each entry should include:

(a) accountable people;

(b) purpose and goals;

(c) scope and intended uses;

(d) expected contexts;

(e) what responsible use looks like for end users or affected stakeholders;

(f) mechanisms for human control and oversight;

(g) capabilities and limitations;

(h) technical details;

(i) datasets and provenance for training and testing;

(j) testing methodology and results;

(k) acceptance criteria and test results;

(l) identified risks and controls;

(m) risk management processes and mitigations;

(n) impact assessments and outcomes;

(o) audit requirements and outcomes; and

(p) review dates.

8.2 Document the end-to-end process for internal AI System design and development.

9. Stakeholder Engagement

Code Criteria

The Participant Organisation will, at its discretion, take reasonable steps to actively engage with stakeholders (which may include, for example, the Therapeutic Goods Administration, Royal Australian College of General Practitioners, Pharmacy Guild Australia, Royal Australasian College of Physicians, Australian Medical Association, Royal Australasian College of Surgeons, Royal Australian and New Zealand College of Anaesthetists, Royal Australian and New Zealand College of Radiologists, Australian Health Practitioner Regulation Agency, Department of Health, Disability and Ageing, Australian Digital Health Agency, Australian Alliance for Artificial Intelligence in Healthcare, Australian Patients Association, hospital peak bodies, local and government health organisations) throughout the AI System lifecycle, supporting the identification of potential harms and unintended consequences of AI System use, deployment, development, design, manufacture, sponsorship, distribution or implementation by the Participant Organisation and shaping the ethical and inclusive design of AI System solutions. The Participant Organisation will implement measures to detect and minimise unwanted bias, promote accessibility, and remove ethical prejudices, striving for continuous improvement and alignment with the General Ethical Principles, while supporting the Participant Organisation's broader organisational objectives.

9. Requirements

9.1 Identify and document the stakeholder groups that may be impacted by the Accredited Organisation's use of AI. Determine stakeholder needs that will be addressed by organisational AI policies and create processes for ongoing engagement that recognise and support marginalised groups and enable meaningful feedback.

9.2 Document the stakeholder groups for each AI System. This should include:

(a) where users interact with the AI System or its outputs;

(b) where personal data is processed;

(c) where the AI System makes or influences decisions;

(d) an evaluation of potential harms at interaction points; and

(e) an impact assessment, where harm or material organisational risk is indicated.

9.3 Evaluate and document each AI System's impacts on diversity, inclusion and fairness, including risks of unwanted bias or discriminatory outputs.

9.4 Document the accessibility obligations and the points in each AI Systems lifecycle that require meaningful human oversight to meet organisational, legal and ethical goals.

Document Version Control

Item	Detail
Version	1.0
Date Issued	1 December 2025
Status	Final
Next Review Due	1 July 2026 (or earlier as required)
Contact	**Emma Hossack** CEO | MSIA ceo@msia.com.au **Toby Hodgson** Digital Health Senior Manager | MTAA aicode@mtaa.org.au **Jason McQuillen** Partner | AI Advisory jason.mcquillen@minterellison.com **Shane Evans** Partner | Disputes, Competition & Insurance Shane.Evans@minterellison.com **Sam Burrett** Director | AI Advisory sam.burrett@minterellison.com