Oneview / the connected care experience company

AI Governance Policy

Version	**3.1**
Date of Version	**07 Mar 2025**
Created By	**Declan Bright**
Approved By	**James Fitter**
Confidentiality Level	**TLP:WHITE**

Change History

Date	Version	Created By	Description of Change
08 Dec 2023	0.1	Declan Bright	Initial version
14 Dec 2023	0.2	Declan Bright	Updates based on team feedback
14 Dec 2023	1.0	James Fitter	Reviewed and approved
25 Apr 2024	1.1	Declan Bright	Added impact assessment section
02 Aug 2024	2.0	Declan Bright	Added AI management objectives
06 Aug 2024	2.0	James Fitter	Reviewed and approved
31 Jan 2025	3.0	Declan Bright	Updates to R&Rs and policy sections
07 Feb 2025	3.0	James Fitter	Reviewed and approved
07 Mar 2025	3.1	Declan Bright	New document template

Table of Contents

Purpose

The purpose of this policy is to outline Oneview Healthcare's commitment to the ethical, secure, responsible development and deployment of artificial intelligence (AI) systems within the company and within our products. This policy, combined with related governance policies, is designed to guide the integration of AI technologies into Oneview's operations while ensuring the protection of data, individuals' rights, and overall AI system integrity.

All users of AI enabled systems must use those systems in a manner that aligns with the company's values, adheres to legal and regulatory standards, and promotes the safety and well-being of our staff and customers.

Scope

This policy applies to all employees, contractors, partners, suppliers and customers of Oneview Healthcare who use or interact with AI systems, including but not limited to; Generative AI, LLMs (Large Language Models), ML (Machine Learning) and any tools, services & applications with integrated AI capabilities.

This policy applies to all AI systems developed, acquired, or used by Oneview, and supplements other company policies to encompass the entire AI system lifecycle, from design and development to deployment, monitoring, and retirement.

Roles & Responsibilities

This policy recognises the importance of involving and addressing the concerns of various stakeholders throughout the AI lifecycle.

The key stakeholders include, but are not limited to:

- Organisational Leadership: Responsible for setting the strategic direction for AI governance, allocating resources, and ensuring compliance.
- AI Governance Group: Responsible for assessing and guiding the ethical implications of AI projects, ensuring alignment with ethical principles.
- AI Development Teams: Comprising data scientists, architects & engineers responsible for designing, building, and maintaining AI systems within the SDLC.
- Legal and Compliance Teams: Responsible for ensuring that AI systems comply with relevant laws, regulations, and industry standards.
- Data Privacy Officers: Responsible for safeguarding individuals' privacy rights and ensuring compliance with data protection laws.
- Security Teams: Responsible for assessing and addressing the security risks associated with AI systems.
- Regulatory Authorities: Relevant governmental agencies that oversee AI-related activities, whose guidance and compliance requirements must be adhered to.
- Users and Customers: Individuals and organisations that interact with AI systems, whose interests, experiences, trust and well-being must be considered, when deploying AI systems that impact the broader community and society at large.

Policy

Authorised Use

AI tools, services and platforms for use within Oneview and in our products must be evaluated and approved by the AI Governance Group before use. This includes reviewing the tool's security & data privacy features, terms of service, and privacy policy. It is prohibited for company information to be input into 3rd party services that utilise the information for AI model training purposes, without explicit permission from the company. AI tools, services and platforms may only be used for business purposes approved by the AI Governance Group. Such purposes include code generation, product feature development, marketing content & document generation, market research, or other legitimate activities. Approved tools/services are listed in the *AI Service Usage Guide*.

Responsible AI Use

Users of AI systems must use the systems responsibly and ethically, avoiding any actions that could cause harm to others, violate data privacy, or facilitate malicious activities. Generated content must be reviewed by a human before distribution. Generated content must not be used or distributed if it is misleading, harmful, offensive, or discriminatory.

Bias and Fairness

Users of AI systems must be cognizant of the risks and are encouraged to actively identify and mitigate biases in AI systems. Users must ensure that outputs from AI systems are fair, inclusive, and do not discriminate against any individuals or groups.

Explainability

Oneview will make every effort to ensure that its AI systems, models or agents are explainable as to how they generate output or take actions.

Feedback

Oneview will provide a means of receiving feedback on the adverse impacts of AI systems from users. Feedback will be evaluated to inform the continual improvement of AI systems.

Human-AI Collaboration

Users of AI systems must be cognizant of the limitations of AI systems and always use their judgment when interpreting and acting on AI-generated content or recommendations. In most cases, AI systems should only be used as a tool to augment human decision-making, not replace it.

Human Oversight

Oneview must identify and document AI system features and capabilities that require human oversight, in relation to operational and societal contexts, trustworthy characteristics, and applicable risks.

Intellectual Property Rights

Users of AI systems must respect and protect intellectual property rights, both internally and externally. Unauthorised use of copyrighted material or creation of content that infringes on the intellectual property of others is strictly prohibited.

Laws and Regulations

Oneview will abide by, and comply with, any AI-related laws and regulations that may be applicable to it, including data protection, privacy, and intellectual property laws.
Personnel and AI stakeholders will be made aware of these laws and regulations, and their impact on AI-related design, development, and deployment activities.

Security & Data Privacy

Employees, partners and suppliers must adhere to the company's security and data privacy policies when using or implementing AI systems. Access to enterprise AI tools, platforms, or related systems must be restricted to authorised personnel only. When using free or non-enterprise AI systems or websites; personal data, sensitive data or company intellectual property must not be entered as prompts or source data. When using enterprise AI systems, personal or sensitive data must be anonymised and stored securely.

Training and Education

Users of AI systems who use the systems in their work must receive appropriate training on how to use them responsibly and effectively. This training must cover topics such as ethical considerations, potential risks, requirements for human oversight, security best practices, and regulatory compliance requirements.

Transparency and Accountability

Users and developers of AI systems must be transparent about the use of AI in their work, ensuring that stakeholders are aware of the technology's involvement in the creation of unique content or decision-making processes.
Developers of AI systems are responsible for the outcomes generated by AI systems and must be able to explain and justify those outcomes.

Third-Party Services

When utilising third-party AI services or platforms, users must ensure, to the extent possible, that the providers adhere to the same ethical standards and legal requirements as outlined in this policy.

Implementation & Monitoring

AI Governance Group

The AIGG (AKA ov.ai.gov) is a multidisciplinary AI risk management team comprised of individuals from across the business to ensure that AI systems are developed, deployed and used responsibly, while considering security, privacy, ethical, societal, legal & regulatory concerns. The AIGG defines roles and responsibilities for designated committees critical to the oversight of Oneview Healthcare's AI initiatives.

Designated AI Officer

The company has appointed a designated AI Officer who is accountable for overseeing the implementation of this policy, providing guidance and support to employees, and ensuring compliance with relevant laws and regulations.

AI Management System

To support this policy, Oneview maintains an Artificial Intelligence Management System (AIMS). The high-level objectives of Oneview's AIMS are defined below.

AI Management Objectives

These high-level AI management objectives are aligned with Oneview's key business objectives and strategy, to use technology responsibly, while developing and delivering innovative solutions for our customers.

1. Personnel Safety, Culture and Awareness

Oneview Healthcare PLC shall maintain AI policies and processes to drive and promote a responsible AI culture. This includes Oneview's Responsible AI Awareness training program backed by processes and incentives along with continuous improvement to align with global best practices.

2. Risk & Impact Management

Oneview Healthcare PLC shall assess impacts and risks of AI to enable informed business decisions. This includes a set of internal AI policies and procedures that support risk management; to understand organisational AI risks; methods to assess risks, vulnerabilities and impacts; the implementation of controls to mitigate risk; and an assurance process to monitor and manage risk.

3. Technology & Services Management

Oneview Healthcare PLC shall identify any AI technology or services that are part of the critical infrastructure and appropriately manage the impact and risk. AI technology controls shall be selected and implemented based on a risk-based process. The controls shall be kept current, managed, protect against non-compliant behaviour and ensure the technology is resistant to disruption and abuse.

4. Incident Response

Oneview Healthcare PLC shall maintain procedures to appropriately handle AI safety incidents and minimise negative impacts on people, sensitive assets and critical information systems.

Employees must report any suspected or confirmed violations of this policy or any potential ethical, legal, or regulatory concerns related to use of AI to the AI Officer, IT Operations or through the company's whistle-blowing officer.

Periodic AI System Reviews

The AI Governance Group will conduct on-going reviews of AI system use within the company to ensure adherence to this policy, identify any emerging risks, and recommend updates to policies and procedures as necessary.

Enforcement

Violations of this policy may result in disciplinary action for employees, up to and including termination of employment in accordance with Oneview Healthcare's disciplinary policies and procedures, and in the case of others engaged in Oneview Healthcare PLC, may result in legal redress.

Exceptions

Any exceptions to this policy must be reviewed and approved by the AI Governance Group, prior to implementation.

Alignment with Other Policies & Procedures

AI initiatives much be implemented in line with existing ISMS & PIMS policies, procedures and controls, including: Business Continuity, Change Management, Human Resources, Incident Management, Risk Management, Software Development Life Cycle and Supplier Management.

Contact & Reporting

Issues related to or feedback on adverse impacts of the AI systems should be reported to the AI Governance Group via email: aigovernance@oneviewhealthcare.com
The AIGG will review the feedback to determine the appropriate action and response.

Policy Review

This policy will be reviewed annually or as needed, based on the evolution of AI technology and the regulatory landscape. Any changes to the policy will be communicated to the relevant stakeholders.