Availity's Responsible Artificial Intelligence Principles

Summary

At Availity, we are optimistic about the potential of Artificial Intelligence (AI) for enhancing the products and services we offer to our clients. Equally, we recognize the challenges with training and maintaining AI systems. We must proactively ensure and operationalize AI use safeguards, fairness, security, privacy, transparency, accountability, and learning.

In our voluntary commitment to these principles, we are continuously developing our AI policy through broad and collaborative contribution, buy-in, and advocacy across Availity business units and promoting the adoption of well-reasoned practices. We are guided by internationally recognized standards and applied lessons learned from industry leaders.

Availity knows that this undertaking will lead to more trustworthy AI systems that benefit our customers.

Defining AI Systems

An AI system is an engineered or machine-based system that can, for a given set of objectives, generate outputs such as predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy.

Guiding Principles

Safety first:

We will continue to apply industry leading safety standards and security practices to reduce risks of harm – to our clients, users, and individuals they serve. Specifically, we seek to establish proper safeguards to appropriately and reasonably minimize potentials for inappropriate influence and bias. We will use the appropriate tools for each use case, considering and employing, when possible, rules-based approaches over black box, statistical AI/ML, methods to maximize the control and explainability of the results.

Avoid creating or reinforcing unfair bias:

AI systems can reflect or reinforce biases intrinsic in the input dataset or solution design. We seek to avoid unjust impacts on people and to utilize data that are representative of those the model will service. When evaluating a solution for a given use case, we will endeavor to consider relevant ethical implications, including impacts related to diversity, equity, and inclusion, and any protected characteristics covered under Availity's Code of Conduct and Ethics. While identifying such biases are not always simple, we aim to reduce any known biases. We also strive to design our AI systems with fair and equitable objectives and monitor the outputs accordingly.

Security, privacy, and confidentiality:

Availity will endeavor to identify and seek to mitigate security risks of its AI systems to ensure responsible delivery of products and services. We adhere to HIPAA Security and Privacy Rule policies and will respect data use rights agreements, adopt architectures with privacy safeguards, and provide appropriate transparency and control over the use of data.

Lead with accountability, transparency & observability:

AI systems can be complex and may feel like a "black box." We believe that transparency in the development process and observability of system outputs are key to ensuring accountability and building trust. We will endeavor to document what

AV258-1223 © Availity, LLC, all rights reserved. | Confidential and proprietary. Updated 12/18/2023

data was used in developing the system and the metrics by which the AI was evaluated (model provenance), appropriately explain how the data was used to produce the systems' recommendations (model observability), and continuously assess the AI for proper functioning within the context and use case for which it was designed (model monitoring).

Research, learn and iterate:

We are committed to building our AI systems on the foundation of scientific rigor and integrity. We will work to continuously improve our solutions, applying a systematic risk management approach through monitoring and analyzing AI system behavior throughout its lifecycle, including gathering feedback from end-users, applying human-in-the-loop audits, and adjusting or retraining systems to ensure fairness, context appropriateness, and security. Availity will monitor emerging trends, collaborate with fellow leading AI developers as needed, and continue to evaluate AI use safeguards, fairness, security, privacy, transparency, and accountability issues.

Best Practices

In our pursuit to uphold our ethical standards and values, we have established these Best Practices to define and emphasize the voluntary commitment we are making to the collective values and principles we hold dear as conscientious AI creators.

Policy Controls

Availity will utilize an appropriate level of the AI Risk Management Framework based on National Institute of Standards and Technology (NIST) and Government Accountability Office (GAO) recognized standards and control recommendations to all bespoke AI products in Production within the Availity digital ecosystem. We will tactically apply the applicable NIST Artificial Intelligence Risk Management Framework (AI RMF 1.0) Core Profiles: Governor, Map, Measure, and Manage. Our goal is to thoughtfully consider and apply the relevant AI RMF Core Level 1 categories and subcategories before considering advanced levels. The process is iterative, and we will use our best judgment to logically apply AI RMF Core categories and subcategories to relevant projects based on context, available resources, and capabilities.

Right Tool and Scope

When appropriate, rules-based approaches will be employed over black box, "statistical" AI/ML methods. We will design and document clear and specific AI use cases, contexts, and scope of operation so that deviations in functionality and bias can be more readily identified.

Responsible, Appropriate, and Transparent Use of Data

- We will provide appropriate descriptions of AI based solutions to end users via Product resource documentation that includes:
    - where within the product the AI component is being applied;
    - what data was used in the training of the models; and
    - the user populations that can access the AI driven functionality.
- Data used in creating the AI model is appropriate.
- We will limit data use to minimum necessary to meet business/product requirements.
- All code and models will be developed and stored in source-controlled systems.
- Model training, testing, and validation data will be maintained in the state it was applied, in its entirety, and stored for retention periods that meet appropriate data governance and compliance policy requirements.
- We will use commercially reasonable practices to assess and document the compatibility with and impact of the model

on any privacy or data usage contract considerations, respect contractual obligations to our clients and customers regarding data use, de-identification, and aggregation (e.g., we will investigate whether any contractual limitations result in data samples that are no longer complete or representative).

- We will secure data appropriately.

Data and Algorithm Performance and Bias

- We will consider and develop reasonable and appropriate plans for each AI system to increase the accuracy of training and reduce bias across the entire product lifecycle, including, as applicable:
    - data sample profiling and balance (completeness, representativeness, and breadth) based on model-, use-, and/or outcome- (or downstream-) dependent attributes;
    - annotation/annotator diversity and experience;
    - processes to mitigate human error (e.g., expert consensus-based and/or multi-annotation ground truth averaging, and/or random and iterative validation audits);
    - when reasonable and appropriate, testing against available independent validation sets;
    - monitoring for drift, and
    - plans and timelines for remediating bias if found.
- We will define metrics to measure functioning, including minimum acceptable thresholds and documented remediation plans.
- We will continuously monitor performance using feedback loops and human-in-the-loop audits to ensure operations are within performance expectations.
- Any bias that materially affects user experience will be appropriately documented and remediated.

Accountability

Establish an AI steering committee. This AI steering committee will review business use cases and the AI systems proposed to address them to ensure accountability. Each AI system will be reviewed with the goal of appropriately meeting stated objectives in a transparent way through a delineated set of algorithms and/or processes, before the AI system is released to production.

Iterative Improvement

A risk management inventory and metrics system will be used to periodically assess AI systems in development and in production. This risk management process will endeavor to identify risks associated with the development and use of AI are prioritized and mitigated, transferred, avoided, or approved, as appropriate, with Availity's risk tolerance given the use case the AI system proposed to address.

Revision History

Date	Updated By	Description	Approved By
12/18/2023	Kaelee Waldrop, Sr. Compliance & Privacy Analyst	Added finalized version from Legal to OneTrust.	Scott Herbst, Chief Legal Officer and SVP Compliance & Regulatory Affairs Sara Brown, Sr. Compliance & Privacy Manager

*The most current versions of Compliance & Privacy policies & standards can be found in OneTrust.